Tape 1, Side 1

topical subject here or whatever you want to call it. There was an absolute dearth of cryptologic material of any utility in 1930 when Friedman had started training the group that had been formed after Yardley's organization was closed down and one of the pressing jobs which had to be done was to prepare a body of material that could be used for training not only the small group which had been assembled but broadly across military intelligence and signal corps personnel, both officer and enlisted, and this lack of material was had to be overcome before any training program could be set up which would embrace more than just one small class like the unit that Friedman was bringing up by hand with his own instruction and that was the group ~~that~~ of Kullback, Sinkov, Rowlett, Hurt, Clark and the small group in the civilians in the Signal Intelligence Service. There was no training material available from the navy or (State Department or the Bureau) or any place else in the government. The few things that had been published ~~that~~ were the [Hagelin] I'm sorry it was ~~the~~ a [Swedish writer]

DOS FBI

(Valaki) [~~(Gildan)~~ (Gylden) Gylden. ~~Gildan.~~] He had published a book. There was one by Gebeirs(?), Kasisky Givierge (?), ? and a few of that type, totally worthless for training purposes is about all that was available. So Friedman being sort of considered the storehouse of knowledge on cryptanalysis, cryptography and cryptology was about the only person who could fill this gap so one of his priority objectives was the preparation of a series of books starting out with the military cryptography, Special Text No. 165 if you want to be able to identify it, which he had prepared and was ready to go to the printers by April 1930. The reason I am so precise in my recollection is that I was given about the umpteenth copy, carbon copy, as the text which I would study when I reported for duty in April and I think I learned ~~my~~ more cryptanalysis

from deciphering the manuscript than I did from the text itself because it was such a poor copy and one of our jobs and Abe finally inherited this was to prepare examples for these texts. Now Friedman had four or five ~~sessions~~ sections in mind as his approach to this problem. One of these was to divide cryptography into two parts, elementary military cryptography and advanced military cryptography and then his concept of cryptanalysis was elementary and advanced and then followed with a bunch of special texts ~~that~~ like we would find in the solution of the mechanical/electrical cryptograph, the Hebrew machine, and have a bunch of technical papers which would then serve as ~~the~~ text books and calculus and group theory and other things in mathematics to people who wanted to specialize, so he began producing and of course this was not an easy job and it took several months he began producing the text which have now come out as military cryptography and I believe you'll find an elementary and advance and you'll find maybe two or three in cryptanalysis and he sort of built these up in nice neat packages which could be produced and printed you see without having to hold up the whole series until the final paper was written because there was a great deal of urgency ~~to~~ in get ting this training program underway in the military services and also I think Friedman quite accurately recognized that if he didn't do it that it probably would never be done until some of the rest of us could be spared and he was afraid that the pressure of both producing US cryptographic materials and to produce intelligence by cryptanalysis on the messages which we'd intercepted ~~from~~ to foreign governments ~~with~~ would grow into such an important operation that none of us could be spared for it and so while he was training us he I think burned the candle at both ends producing the text at least outlining and putting the words around the text and I think finally the latest ones Calimahos collaborated pretty made ~~good~~ big contributions to them because Friedman got so preoccupied with other things and probably

honestly burned out by doing these things because it's not an exciting thing to do a textbook on cryptanalysis if you've got some live material waiting for your attention. Now I believe this is a reasonable summary of what happened in the preparation of the text on cryptography and cryptanalysis and I think it lays the groundwork for us understanding to understand the so called Black Books or technical papers which were published about that time. Friedman because of the pressure of producing the comprehensive work on cryptography and cryptanalysis which was a great big chore in itself, went ahead without waiting to any longer than he had to to begin publishing the technical papers and here again in tribute to Friedman's foresight ~~we~~ he had budgeted a certain amount of money to be spent ~~on~~ for printing and binding and the production of technical papers on cryptology. Now as soon as he found something that would qualify for a technical paper he would get a manuscript prepared that could be sent to the Government Printing Office and he went first to the papers that he had produced. The most significant of these is the Heb~~ron~~ern solution, the technical paper that is entitled "Analysis of the Mechanico-Electrical Cryptograph~~s~~" and the reason there is a Part I to that is because that's basically his analysis of the Heb~~ron~~ern machine which was presented to him by the navy department back in the middle 20s. Later on, Part II arose out of the second version of the Heb~~ron~~ern machine which I believe as I recollect here without looking at the book was a result of work which was done after 1930 and we the three of us I leave Hurt out of this because he was suffering pretty badly ~~badly~~ from tuberculosis at that time and of course was burdened with the work on the Japanese. Hurt worked very little with us on the research problems and so Part II was later on published as a follow-up of a cipher machine based on the Heb~~ron~~ern and I think that is probably the best example of an authentic pre-1930 publication. I mean the manuscript that Friedman put into publication after 1930

that we could find. Now there were certain other of these papers. The solution for the double transposition cipher and oh . . . .

Some of the other more important technical papers that were produced as a part of the literature program and I think probably the most important that came out of the work of the three of us Kully, Sinkov and myself was the general solution of the ADFGVX cipher system. The philosophy and the concept that we discovered in dealing with the ADFGVX cipher laid the groundwork for our solution of the Japanese transposed codes, the J19 series and that group, and also gave us the first opportunity for the application of computer type~~s~~ modern day computer type~~s~~ attacks on cryptanalysis and I think this needs this paper~~s~~ needs considerable separate treatment on its own merits because the ADFGVX cipher system, although a WWI type of system, led us into a domain of the wilderness that we might never have otherwise explored and maybe it would have been some years later than was actually the case that the application of computery to cryptanalysis would have been achieved. Others of which I felt were very good papers of the state of the art at that time was The General Solution for the Double Transposition Cipher which I believe is authored by Dr. Kullback and the permutation tables involving the featured non-transposability which is by Dr. Sinkov and statistical methods in cryptanalysis also by Kullback. These represent positive contributions, significant milestones in the development of cryptanalysis as we saw it in the early 30s and this was a very very fruitful period because for two reasons. One Friedman had really stimulated our interest in doing research, finding new techniques for solution of systems which were known and devising ~~uses~~ new systems which were an improvement and he'd build a fire under us and it got a very good response

from all of us in that field and second there was no competition so it was a very good year for young cryptanalysts to go into publication because what we had learned and we had learned lots of things that were useful but we never there was just so much work to be done we ~~never put~~ couldn't write them all down and these papers are rather thin because we were forced to put the bare bones of the information down rather than by to take some small items and expand them by elaborating on them and putting a lot of words ~~in~~ and so they are very pithy, they are right to the point and they are very useful I think as measures of whats accomplished in those years. Now some of the other papers were published for example the report of the code compilation section of general headquarters american expeditionary forces Dec 17 to Nov 18. Since we couldn't produce enough technical papers in volume as represented by the efforts of Friedman and those of us who were in his small group to eat up the budget which had been the money which had been budgeted for these things Friedman went back into the files and picked out useful historical documents and the title of the paper I mentioned represents one he'd selected. Another one, encipherment of the german diplomatic code No. 7500, money was available and this in Friedman's mind was something that ought to be documented in the history of cryptography and so he chose ~~this~~ it. The Zimmerman telegram of January 16, 1917 and its cryptographic background was a paper produced by Mendelsohn and Friedman in collaboration. Mendelsohn did a tour of military duty, a couple of them, and produced this paper as part of his military assignment while he, as a reserve officer, he satisfied his requirements for active duty and its a very good paper. I think it puts into pretty good

context what Barbara ~~Gickman~~ Tuchman (?) publishes in her story of the Zimmerman telegram but I can't resist my own impulse to say what I think about it. I think that both Friedman and Mendelsohn were completely taken in by Admiral Hall and his group and the intentions of the British. I think that by golly the British were reading the American codes and they were very nervous about ~~this~~ disclosing their cryptanalytic techniques to the US because they didn't want to dry up this valuable source of insight into American intelligence. That is I think probably the way it happened. The British were so reluctant and made such a deal about revealing the fact that they read the Zimmerman telegram and I think some of the speculation in the paper by Friedman and Mendelsohn doesn't take that into account and couldn't have because at that time the Americans weren't aware of the competence how really how good the British were in cryptanalysis. The other papers I think can be readily identified and put in the sort of categories of useful historical docu-

documents that is old reports which were published simply because the funds were available and we felt we had to use these funds because they might be cut back next year and we certainly anticipated that the documentation of what had been developed either as a training program or in terms of a technical papers was important to future cryptanalysis. I might mention one other paper and then I believe we've dealt enough with these and this is the paper on the solution of cryptograms produced by the IT&T cipher machine. This was the result of a challenge by Parker Hitt of Friedman to break the machine that he had been instrumental in producing as for IT&T and it was a very straightforward attack that we applied to it and Friedman was looking ahead in this case and he could see that the automatic encipherment, the teletype signal, was going to be one of the big problems for the future of cryptography and cryptanalysis and so he was very anxious for us to write up the solution which we had achieved on the IT&T so that there would be at least some basis in the

cryptanalytic literature for dealing with that type of a system. Both from the standpoint of cryptography, protecting our own systems, and from the standpoint of a possible attack on foreign cipher machines using the teletype stream as the basis for cipher treatment. Is that what you want?

A: Yeah.

Q: The first question I had on my list was the one that you commented briefly on there about ~~reporting~~ recorded material and the question being did you receive any recorded material during the 30s and WWII and if so what form was it in, tape, wire, dictaphone? Sir the reason that I asked this originally was that I became aware of the fact that they were using dictaphones in the WWI period, in 1919 and so forth, to record intercept and I was particularly interested in what was being used in this later period and what then was being forwarded back one way or another?

Coates

A Shall I pitch in? Yes there was some recorded material received after 1930 and during WWII but the role played by the recorded material somewhat traces the

development of the recording art in that timeframe and let me tell you some examples about some examples that I know about, This and we are now talking about intercept material. We've got to go back and realize that there was no intercept service available before the early 30s. The signal intercept service in the army and I'm talking about the army now, did not begin to produce until sometime after April 1, 1930 and I would judge that as a loose recollection that the first information, the first intercept material, we got was sometime within the next three to nine months and it was the first meager takings of the second signal service company. Nathaniel Lee Baldwin, Capt Baldwin, was the officer in charge of the organization of the intercept service and they had arranged for one of these to be up at Fort Monmouth. I believe this was station one, That was where the school was and they were going to select their operators from the cream of the communications operators The normal telegraph operators, radio telegraph operators, in the signal corps because they had already learned Morse code, they had learned the magic of intercept, well taking the signal off the air and putting it on paper.

and so all they had to do was to learn the quirks of these special quirks of the networks that they were covering. The navy had gone much further than the signal corps in developing intercept service and I believe they had a full grown one, a very good one in being by 1930 but I know very little about that because we did not learn of this until sometime a couple of years later when there was the beginnings of some sort of collaboration in the intercept field that I began to observe. There may have been more before I noticed it but that's when I began to observe it. Now the first recordings that we received were from a special installation in the Presidio, California in the San Francisco and the reason we got these is because General Mauborgne later Chief Signal Officer who at that time was a colonel was the signal officer for the 9th Corps area with his headquarters in the Presidio and he was very anxious to begin coverage of the transoceanic circuits between

San Francisco and Tokyo to pick up Japanese diplomatic messages which was the number one priority in the SIS as our intelligence target and I believe it was about 1930 well it was a couple of years after 1930 anyhow that we began to receive in the in the signal intelligence service some undulator tapes that had been recorded by ~~Mobern~~ Maubourgne in, believe it or not, his quarters where he'd set up a radio receiver, communications receiver, and tuned it in on the commercial circuits between San Francisco and Tokyo. He knew the frequency. He'd spotted it. He had it all pretty well lined up and since they came up, these circuits came up, while he was on duty he'd also rigged up a sort of homemade do-it-yourselfer time clock on ~~this~~ the thing which essentially was, as I believe he described it, as an alarm clock with a clothespin. Somehow or other the alarm clock pulled a little piece of insulating material up between a weakened clothespin and closed the contacts and you must remember we didn't in those days have timing lights switches like we now have that you can buy for 5 bucks. It was a laboratory job to build a timer because I don't

think the synchron~~is (?)~~ous clock motor had been marketed at that time so it was a very primitive sort of setup that ~~Mobern~~ Mauborgne had but he did produce the tapes. These tapes came in in packages by registered mail with a government franking, and ~~we~~ were received in the signal intelligence ~~[illegible]~~ unit. Friedman brought them in and gave them to Abe Kully and myself, and Johnny Hurt to do something with. Well they were undulator tapes in Morse code and I think this is interesting. It really doesn't come in as part of the question but it shows the state, it shows something about our development. I was the only one who had any inkling of what a Morse code was like being a little bit of a radio buff when I was in college and before that and so I had maybe a little more knowledge of what to expect on these tapes and I was able then to take the tape~~s~~ and look at the Morse signals which was inscribed on it and translate it into letters and of course there was the question of putting it down in copy so we could work on it. Well Kully and I formed a team. I would take the tape, read it vocally. Kully would take the back, take the paper

which consisted of the backs of mimeographed weather reports because we were so hard up for funds in those days in the signal corps that we couldn't buy stationary and there was some kind of commitment which required the signal corps issue every day a weather report in a certain number of copies and they had to do this to satisfy the budget requirements At least that's what the Chief Signal Officer experts told them so when the rest of us were without paper, the meteorological section had paper and then we took their what they didn't distribute you see and used it as for our paper and of course it was ideal from the standpoint of handwritten copy of the intercept. So I would read the tape and Kully would transcribe it and then Abe, we were beginning to get organized in the Japanese section at this time, Abe would you know sort it out by categories, and index it and this was the division of effort. It was this went on for two or three years until he actually had trained the intercept operators to do this transcription work in the station. Of course it was a makeshift

kind of a thing for ~~Mobern~~ Mauborgne to send in these tapes. Now to get down to the real meat of your question and get away from this sort of incidental experimental development which is interesting because it does demonstrate how we had to deal with the problem. In due course the intercept operators would record the signal on undulator tape because that was the way the commercial companies were recording it and it was probably the most efficient and the most prudent way of doing it because to go to some other medium, remember magnetic tape hadn't been invented, the wire recorders were most unpredictable and poor quality and poor quality control on the wire and very little was known about the theory of recording and the other fancy things like reproduction quality and fidelity. So The undulator tape was just up and down and if you got a good fat signal and it ~~was~~ went through a good strong amplifier there was no mistaking what it was unless you got a burst of static and then since the commercial companies collated their messages you could always clean up the static on the second transmission and also if it was too bad they would retransmit at a

later date so if you kept on the circuit you could get good clean cop~~ies.~~ They had to have clean copy because they were selling it. We had to have clean copy because we were trying to solve it. Their requirement was money and ours was maybe didn't show through as loudly and talk as firmly as money did. When we got into tape-magnetic kind of tape or wire recorders-some experimental work was done by the laboratories, signal corps laborator~~ies~~y, on wire recording and it was not at all satisfactory and at that time if you'll just look into your records I'm sure you will confirm what I'm going to say is that there was the dictaphone was pretty good for office work but for the long continued recording sessions required by the intercept operators ~~just~~ well it could be used did require special equipment, hard to obtain and did require special training which sometimes it was hard to achieve and since the undulator tape was doing such a magnificent job there was no point in going to something else until it could definitely be proved the other medium was better and we didn't achieve that latter in the timeframe up until I would say

the beginning of the war. Now I have ~~there~~ contact with the intercept station at about the time the war started because there was just too much to do and there were too few of us to work in the well the development of the old signal intelligence service we just well that's my excuse for not knowing anything about what happened in WWII. Did I answer that question?

Q Yes I think very well. _____ _____ _____ _____ _____ _____

Coates

_____ You said there was no intercept service prior to April 1, 1930. How was Yardley getting all his material?

Goodman

A Pickups from cable office. That's a good point. I should have mentioned that. You can confirm this by Yardley's book. He sort of slides over it but if you read it carefully you will . . .

Q Do you know whether or not the MID had directed any of the ~~naval~~ signal corps people to maintain ~~some of~~ the stations that were in existence earlier say the post war period 1921, 22 _____ or some of the other ones. (Is _____ a city or Fort Sam) Fort Sam Houston ~~[illegible]~~ They were still operating after WWI and we don't know how long they continued.

A. I don't know how to answer that but I can speculate on what might have happened

because unless there is a threat the military services tend to go dormant. This is sort of Rowlett's rule of thumb. What can you pick up from the places you mentioned? Fort Sam? Fort Sam was one of the stations that was planned for the signal intelligence service. It didn't take us long to discover that this was a very useless place to have an intercept station because (1) it was right sort of in the middle of Texas which is a pretty good state and (2) for close-in listening like the Japanese military or German military what can you do down there?

Q How about Mexico?

A: Mexican? Mexico was no threat in the timeframe of 1930 to 35, If it was it was so relatively small as compared with the three major threats Japan being number one Germany being number two and Italy number three and then France possibly four. Britain was not considered a threat for some strange reason. I don't find it philosophically explainable that in terms of what I remember at that time and what I learned later but Britain was just not considered a threat at all. Probably as an outgrowth of the Alliance which was developed in WWI but Spain, the Spanish of course was not much as a military but was useful for diplomatic intelligence.

South American countries somewhere below [Spain.] Cuba, of course, was of interest because of its proximity to the east coast of the US. its possibility of being taken by some foreign power in a coup like the Bay of Pigs turned out not to be so I think this kind of puts them in perspective. Now go back to my speculation about this question. It was just so futile and so little real work could be done at these intercept stations and the requirement was so disguised. The requirement was there but there was no mechanism you see to make the requirement to implement the requirement to ask that certain well you've got to give an intercept operator direction or he's no good as an intercept operator just tunes like when we do when turn our CBs on. He listens, He finds something interesting and thats where he stays but if you're going to have a thriving good production intercept station you've got to give them a proper target and you've got to give them instructions and you've got to give them circuits and other things because the intercept station cannot thrive without direction and I don't think there was any direction and any

requirement and they just did what everybody would do under the circumstances.

They just did what was necessary and let it go the rest of it go because even if there

was an impulse like

End of Tape 1, Side 1 560

Tape 1, Side 2

Q Goodman Was there any continuity that you can recall to intercept activities from the WWI era through to the establishment of the SIS in 1930?

A. I can speak only from 1930, April 1, 1930 on and what I bumped into quite by accident regarding what was done in the period prior to April 1 1930. The there wasn't quite a capability for intercept developed in WWI, frontline intercept. Most of this was picked up from the French and most of it was done in the field commanders domain and just like in every other major conflict where the field commander is pretty much like MacArthur was as we think about it in the Philippines where he develops his own military structure. When the need for that military structure disappears then all the components are pretty much done away with. Now since the intercept which was viable in WWI was mainly field intercept, and in the years following WWI up until 1930 there was no field requirement, You can quite naturally expect and it would be my assumption that it just dried up on the

vine because there was no need for it. But now this didn't mean that certain people within the military establishment lost their realization of the importance of an intercept capability both in terms of ~~the~~ a natural war and in terms of preparation for future wars. It was I think this realization coupled with the realization that there would be a need for intelligence of the type of the Zimmerman telegram, if you will, which was pretty well publicized (that lead the State Department to continue ~~the~~ Yardley's organization) and since Yardley's organization was fed by pickups from the cable offices there was no need for the conventional radio intercept operator and radio intercept station that we visualized as we looked at the problem ~~at~~ in today's dimensions. Yardley could produce intelligence from the cable copies, and since there was no war there was really no need to do military intercept. your [cable intercept was the diplomatic intercept] and if you could get it from the [cable companies] for almost free why waste the money and the effort and attract attention by the activity? It was good from the secrecy standpoint and all these factors tended to work against the development of a productive intercept

service in the timeframe up to 1930. Now when the Yardley's organization was dissolved in 1929 the concept of taking the 10 grand that had been contributed by G2 to the State Department funding for Yardley's installation up in New York City well that 10 grand was used to hire a few people, Kullback, Sinkov and myself and Hurt and Larry Clark and that just about added up to ~~their~~ her salary because at $2,000 a year ~~per~~ for a junior cryptanalyst and $1440 for another job you had about $600 left over which could go into the general signal corps kitty and that came out as the dimensions ~~that~~ of the civilian staff of the signal intelligence service. But now since the military was going to provide the people for the intercept service, that came out of ~~or~~ a different sort of funding-manpower arrangement and there was hardly any point in developing the civilian component without mounting the intercept activity at approximately the same time because they recognized I think the ~~Moberns~~ Mauborgnes and the others who were behind this movement to develop the signal intelligence service, they realized there would be a training time lag in there.

By the time they got the cryptanalyst trained they would need the intercept and they would need also by that time to train the intercept and organize it and they visualized one each of the departments major intercept station that would be the Philippines, the Hawaiian department and the Panama Canal department looking down to South America. Of course Hawaii didn't look very good at any place because the Philippines in terms of the state of the art at that time was the primary place for intercepting communications from Japan and China and the chief advantages of the Presidio and Fort Monmouth was found in the their availibility to pick up transoceanic commercial circuits from New York to Europe and from San Francisco to the east. Now in terms of the kind of information that was intercepted, military activity was nil and so they were almost limited exclusively to picking up diplomatic communications. Now this wasn't true for the navy because there is always naval activity. Ships go out. They sail the ocean. They sail around the world. The navy always has an opportunity to intercept Japanese, German or Italian or whatever navy in

the timeframe of the 30s which you would never enjoy if you were trying to intercept military traffic and at that time you must remember also that our capabilities of the major nations still somewhat in its early stages and in some cases could not be identified as being separate from the army or navy because if I was in the U.S. Army or the U.S. Navy that land capability was so far as air was concerned was part of the army and the sea was part of the navy. I think this last is important because people lose sight of the fact that in that time period there was practically no reason there was no Vietnam, no Korea. Nothing like that going on. We were pretty much an isolated country and we could see only what was right around us.

Q: The second question I have here then I think you're almost ~~right~~ into ~~was~~ is do you know of any pre-war intercept in the Philippines or China?

A: Now do you mean pre-WWII intercept?

Q: Pre-WWII. Yes.

A: Yes. The navy up sometime before 1930 and I can't put a date on this as I recollect it ~~this~~ now had developed a competence for intercepting Japanese naval and other land-based, certain other certain land-based, transmissions in Asia. For example, there was a net a Japanese net called the Far Eastern Diplomatic Net that had a base station

in Tokyo and then several outlying stations within Asia and they were covering this net completely. The operators were very good the cream of the navy communications operators and they had done enough work on the Japanese so that they understood exactly what the Japanese were doing and they copied them as good as any I can recollect having seen. Of course now I'm basing my observations on what I learned in 1933 and 34 because we didn't know about this navy activity until some years after 1930. What year I don't remember now. Now we had for example developed quite a capability for interception in the Philippines before Pearl Harbor and one of the most interesting and I think heartbreaking things that you could listen to was this recording of the last message from Corregidor because the message is from an intercept operator. That's about all they had to send back in those days. Actually I think I might inject this reminiscence in the answer to your question. Actually in the Philippines the intercept station was located in one of the most impregnable points in the area and when the Japs took the Philippines the intercept

station was one of the last positions that was overrun by the Japanese and the intercept operator the intercept operators were intercepting Japanese messages, field messages. It was the first time we'd seen them this close up and had been sending them in from about the time the Japs landed until the fall of Corregidor and what they were doing was taking the better intercepts which we had specified from Washington, enciphering them with the M134T1, sending them out over the radio circuits, we picked them up in San Francisco, sent them by landline to Washington where we decoded them and then we had the actual intercept messages. Now there was a considerable volume of these things coming in and they were extremely valuable because they gave us the first real sample of the Japanese military front line tactical communications systems and radio activity. Now as part of the human interest aspect of this thing we thought this were we putting too much of a burden on these folks so we made the query and this was the answer and I will remember this answer very vividly as long as I live - roughly - "There is very little that

DOCID: 4223202

we can do except it seems to us this is a positive action against the Japanese. We are happy to do it. We would be happy if we were killed, to die doing it because there is nothing else for us to do except surrender and we don't want to surrender." Now this oh there were usually there was a little bit of a commentary at the end of the transmission on what the intercept operators and the chief of the intercept service and some of the signal corps officers thought because this was separate and apart from the command communications to Manila and I remember one of the last ones that we received talked about the imminence of the fall of the station, what actions they were going to take to destroy the classified equipment which was very important to us you see. We didn't want cipher devices and other things like that and other classified equipment to fall into the hands of the Japs so we sort of bugged the people out there and uselessly I'm sure but you do it nevertheless as a prudent thing and they explained what they did and went into some detail about living conditions. So we had an active and mature intercept service operating out of the Philippines at the time the Japs struck Pearl Harbor and this had been

developed from about 1932 ~~to~~ through the years up to Pearl Harbor and it was one of the priority intercept activities of the signal intelligence service because it was the only hope we had of picking up mainland China and mainland Asia and certainly from Japan itself a military traffic because we weren't able to get it from anyplace else.

Q: I wondered to some extent about the Navy that sent their boats up the various rivers into China - whether they were taking advantage of their close-in position to do any intercept activity?

Contes

A: I couldn't answer that except by speculation. Knowing the navy I'm sure they did and I think it was the right way to do it. I don't say that in a derogatory sense but I say it that if you're going to you have to have a pretty good idea of what each portion of the radio spectrum used by the enemy is being employed for, employed for and unfortunately ~~for the~~ in radio some of that is very close in and the timeframe of those days certainly it was indicated we'd go close in. Now these were intercepts. They were primary items of intelligence. Not secondary like we find in the, well we

had _COMINT and we had RADINT. We had what the Air Force tried to do whenever they found out they could do communications intelligence and I'm talking now about ~~the~~ Butcher's fiasco. That kind of stuff is in my opinion and for what its worth in this context not worth going after because you have to do to much to it and there's to make it useful and when you have made it useful its it has to be confirmed by many other sources many of which are much better intelligence criteria than the stuff itself.

Q: Since we're talking about actual intercept activities the last question that I put on here was one concerning targetting on [Russia] particularly in the 30s but also periods back during actual period of WWII. I suspect that we probably did intercept activity against [Russia] and but I haven't gotten into any type of work on it. I wondered if anyone was in fact with your group maybe working on the [Russian problem?]

Coates

A: We did some work on [Russian] in the 30s. There was a congressional committee investigating ~~the Amtorg~~ AMTORG activities up in New York City and they turned to the navy with a bunch of intercepts and this I guess would be 32 or 33 and asked

the navy cryptanalysts to try to decode the messages and give them to the contents to the congressional committee. Lawrence Safford and Joe Wenger, I think Joe Wenger was, you'll run across his name so I won't identify him or Safford anymore in this context than I've done. Joe Wenger was very young in those days and an ensign and this is the first time I think he'd bumped into the army. Safford had been known to us because he was in charge of the code section over there, so Safford and Wenger brought this package of material and saw Friedman to see if we might do anything with it and I think we worked, we worked pretty long on it. We broke into the meaning of the first groups, the indicator groups, they had a sort of a syllabary that told what to do with the rest of the message but we were never successful in breaking the messages themselves. It wasn't too much I'd say about a stack about two inches high which they'd filched out of the offices of the Monterey Trading Corporation and the reason they'd done this because at that time we had not recognized Russia and I think in terms of what was done against the

Russians, remember that Russia's back was broken in WWI and it was a state of chaos to the outside world. Everything that happened in Russia was not understood. The communications were'nt, didn't mean much. The American intelligence had very little concept of the Russian situation but they could see the Japanese navy and they could see the German navy and they could see the Italian navy and they could talk to the Japanese and the German and the Italian diplomats and these were the big targets and nobody ~~ever~~ had noticed Russia really in that simplified context. Now when did we become concerned about Russia? Of course when we woke up to what was happening when Hitler starting acting up in Germany then interest was developed and we started to put some Russian priority into effect and we required Russian messages but we didn't organize the ~~real of the~~ Russian section because still the real fighting, the real enemy, was not Russia but (it was Germany), Japan and Italy in that order because the order changed after Hitler had become as active but we were still working hard on Japan because we figured that Japan

would be it was inevitable I mean there was no question in our minds and the people I talked to that war with Japan was inevitable and this was clear about a year before Pearl Harbor and of course nobody knew until Pearl Harbor itself where the strike was going to be and I think we were all surprised that the Japanese had the temerity to do it the way they did. The real realization, though, to the importance of Russia did not come until just before the end of WWII when Japan sent a series of messages, I believe it was in May of the year, that they wanted their Ambassador in Moscow to go down and call on Stalin and get him to intercede with the Allies for an honorable peace for Japan. The only caveat over and above unconditional surrender was that the integrity of the Imperial household be maintained and when Potsdam took place and well in the first place Stalin never did see the Japanese Ambassador on this question. I think he talked to one of the his deputies in the foreign office and then when Potsdam took place and the Russians didn't mention this we knew those of us in the business we knew who the next enemy

was. Now another activity had taken place and I don't know whether this shows up in the reports or history or not so dont be surprised if you don't find it right quick but the lend-lease traffic out of the Pentagon up to Ladd Field in Alaska which then went on over to Russia through Siberian landlines. There was a link from the Pentagon, Russian teletype installation there, which terminated in one of the buildings over at Arlington Hall Station, A Building, and every message that went back and forth across that line was copied, recorded, and we had a Russian section working in B3 several months before the end of the war, and may I tell another story because I don't think you'll find this and I don't know I may get in trouble and you all may get in trouble in this one too but Carter Clarke was the head of the army security agency and Carter Clarke was one of the most dedicated men to intelligence I ever knew. He wasn't always a he never did the conventional thing. He was a very unconventional man and he was also a man of considerable moral courage and he would spit in your face and laugh at you. I mean

that was his temperament. Now we had organized this activity, the Russian section, and we were working on this Ladd Field traffic because it was you know sort of "for free" intercept and beautiful copy about as good a copy as you could hope. It wasn't really intercept copy. It was communications copy you see as opposed to the kind you pull out of the air and transcribe. Now we had had considerable success with the German one time pads at this time. We were read we would read everything the Japs sent in the diplomatic traffic and we were right up on top of the Japanese military. There were two fellows up in the White House who were very close to Mrs. Roosevelt. Shall I mention their names? David K. Niles and Curry. Remember Lauchlin Currie?, and for some reason Mrs. Roosevelt got the word that we were working on Russian traffic and G2 got the order that any work on Russian traffic was to be stopped. Carter Clarke who was our boss came down to my office. He came to see me not my boss but he came to see me and he said "Tell me what you're doing on the Russian", and I told him and Dink Hayes was also there. Dink was pretty close to Clarke and

this was Col Hayes, Col Harold G. Hayes and Clarke turned to Hayes and said "You haven't told me that you're doing anything on Russian, have you Dink?" and Hayes said "No sir, I haven't" and he says "You keep on doing what you told me." No. He says "You stop doing what you told me you were doing on Russian and Rowlett you keep on doing what you told me you're outfits doing on Russia." and that was the end of the conversation. Did we stop? We did not. We kept working and we went to work harder and harder because it was pretty well established that Mrs. Roosevelt was meddling in things she had no business to be meddling in you see and there was a very rare opportunity for somebody in the bosom of Arlington Hall to get this close to the White House so I remember it very distinctly and Clarke had it straight from the Secretary of War's office because he had been called up and put on the mat for this and I'm quite sure that Curry and Niles and Hiss as a group had, seeing what was happening to the Japanese and the German and the Italian, and had presumed that we would do the same on Russia.

and had taken steps on their own initiative to cool the effort. Now this is Rowlett's speculation. Did you record that? (laugh) OK. I don't think I told you that story. You've got some more questions, sir?

Q: I have several more but I have an appointment and I'm ~~are going to~~ have to go in a little bit.

A: OK lets do a raincheck.

Q: (Rowlett) We're on tape. Do you want to read the question or do you want me to read it and then deal with it?

Q: (Valerie) Well how did you apply what you learned from Friedman's orange manual and from open sources?

A: To Give you a smart answer. We didn't. If you mean the by the orange manual the little booklet that Friedman had prepared I think it was published in the Levenworth series and it covered the information that he'd put together to conduct a course in cryptology at I think I don't know whether it was Levenworth up at Cape May which later became Fort Monmouth and if that's the document you mean the use its usefulness was somewhat as follows: Since it was very little instructional material available at that time;I mentioned earlier the elementary military

cryptography that Friedman gave me to read actually what happened I came on the first of April and Friedman was hoping to have all four of us together before he started us on our formal training and since I came first, then Sinkov came about ten days later and Kully came about twenty days after the first there was a waiting period for me and then later Sinkov until Kullback came in and so he used his orange manual as a filler to keep me occupied and later to keep Abe occupied until he found out what we could do and gainfully occupy us with other activities while Kully caught up with us. Now the orange manual was an interesting thing because the problems in it were sort of our first introduction to cryptanalysis. To put it into perspective, when I came to Washington and Major Crawford received me in his office, Friedman wasn't there and he said "Yes, he says, "We're going to teach you to be a cryptanalyst." I asked Major Crawford, "What is a cryptanalyst"? and he said "You wait until Friedman comes and he will explain to you" and I waited and when Friedman came I asked him what a cryptanalyst was and Friedman said "Well have you

read ~~the post gold book~~ Poe's Gold Bug and I said "Yes" and he said "Well the man that solved the Gold ~~book~~ Bug cipher was called a cryptanalyst and that's ~~the~~ a cryptogram that he solved and we're going to train~~ing~~ you to be a cryptanalyst and a cryptographer and I nodded like I understood and I really didn't and so I was still puzzled when he gave me this orange manual because it was titled "Elements of Cryptanalysis," and I ~~felt~~ thought then I would find out exactly what a cryptanalyst was but when I got in there I was as much puzzled when I got through with it as I was when he handed it to me and I still didn't know what a cryptanalyst was so I guess how I applied and how Abe and Kully applied this was that Abe and I used it as a filler until Kully caught up with us and it wasn't much use because the problems were so simple and the concepts were so primitive that it just didn't stimulate us any way and while we did learn a little bit about solving monoalphabets and polyalphabets this was indeed nothing in the broader scope of well it didn't match what we were introduced to later on to in terms of the Heb~~ron~~ern machine and the IT&T machine and

the Swedish cipher machines the strips well not so much the strip as the circular cipher device, cipher device type M94, and actually I don't think Friedman's orange manual as you call it here was any more sophisticated than Parker Hitt's book on the solution of the ~~paper~~ cipher. Now open source of material? I'll talk a little bit about that. Again personalizing this since I was supposed to be an expert in German when I came in, Friedman had collected a bunch of books in foreign, by foreign writers. There was nothing written by an American that was worth a consideration except his draft of 165 in the orange manual and Hitt's manual and so he picked out two books and gave me almost the first day I was in, probably to find out how much German I knew and one of them was ~~Kreisky~~ Kreiski, which was a little thin greenback book about 1/4 inch thick and 5x8 in dimensions and another big thick hard cover book by Andreas Figl ~~Adrus~~ ~~General~~ ~~Thiegel~~ Spiegel? about I think cipher systems or well I forget the title of it but its Spiegel's book on ciphers and I was supposed to read these and that was my introduction. Now the open source of material was mainly a description of cryptography, the

DOCID: 4223202

cipher systems and Kirkpatrick in particular had a bunch of examples of some very very unsophisticated systems, substitution, grilles, route transpositions, things like that, more to confuse the encipherer than to deny the information to anybody with an apptitude for puzzle solving and they were terribly written. My German wasn't very good. I could make sense out of scientific German ~~journals~~. The vocabulary was awful -- ~~The~~ words I had never bumped into, and I finally wound up by taking examples and working out the examples from the information that I could decipher out of the German text and then recov~~er~~ering the German text sort of by intuitive cryptoanalysis and I can remember ~~it~~ this distressed me so much I would, in my dreams at night in that first few weeks which was a very stressful period of going from being to a country boy to trying to be a city boy, I could remember seeing those pages and some of it would be in English and then there would be a long German word and the rest would be English and I couldn't find my dictionary. So to summarize this long reminiscence the

orange manual and open source of material was hardly worth anything except Friedman's

manual did introduce us to his vocabulary. Other material

Valaki Q: You didn't read _____ then? Kerchhoffs

A: I don't remember. I think I may have but I don't remember and if I did it was

so much worse than _____ and _____ that I probably rejected

it.

Valaki Q: I think probably you didn't.

Q: What was the date of orange manual? (Hank, 1923)(All present agreed)

A: Incidentally a mint copy of that is worth about $23.

Valaki Q: Is that so?

(Hank) Hey don't try to sell it. (laughter)

A: I don't think there are many of ~~those~~ them. ~~There's probably~~ They destroyed about 150 of them once.

I salvaged two. I've got a mint copy but I'm certainly not going to throw it

away.

(Hank) Hold on to it.

Virginia) Yeah, ~~throw it this way if you're going to~~ throw it away.

End of Tape 1

Tape 2, Side 1

Valaki: Q: I'd like to ask something about the green papers. You remarked something earlier about speculating what you could do and when you started working, especially on the machine ciphers. Did you get terribly impatient with the imitations of whatever you were working on, the little IBM machines once ~~once you started with~~ and think ahead.

A: Oh not particularly. Cipher machines in those days were well first place of course the thing we had to computer was one of these old Friedman comptometers, if you remember that, and slide rules and these were sort of not very useful and also not very impressive in terms of what you could use to assist you in the techniques of cryptanalysis after we'd learned them from Friedman. What we did find, however, ~~what~~ was that by taking the cipher machine, for example the machine I call the Damm machine because it was invented by a Swede by the name of Damm. I forget the number of it. I'll think of it later. What we did was to convert that to a pencil and paper analog. We took the cryptographic principles and we worked

out how we could duplicate the machine and its cryptography and its cryptographic process in both enciphering and deciphering with the simpler concepts that you could put on paper like sliding strips or in the case of the Swedish machine it would be a fractionating square and the effect of the pin wheels and, you know, laid out in terms of the sort of a diagram on a large sheet of crosssection paper and once we'd achieved that, we had reduced ~~the~~ it to concepts that we could deal with ~~it~~ in terms of our cryptanalytic training and our other backgrounds, particularly mathematical backgrounds, and what~~ever~~ little understanding we ~~have~~ had of electromechanical devices. Now the way we dealt with the machines then was reducing them essentially ~~the~~ to hand systems and solving ~~the~~ them as hand systems and I think I've just answered your question in that last sentence.

Q: Yes. I ~~would~~ was thinking that mostly ~~that~~ about computer applications of the machines systems, ~~were there~~ whether ... You could see that some time in the future it would be nice to have a very large computer or something that would dupe particular

Valaki?

things. Were you even thinking of generalizing the computer or building analogues? ~~analyze?~~

A: Let me speak at length on that. Nobody that I knew of in the army or ~~the~~ navy except Billy Friedman had any concept of, lets use the word loosely, mechanizing the cryptanalytic process and this was only a glint in Friedman's eye and Friedman had had only very limited contact with accounting machines like Hollerith and IBM at that time in the technological state of development there were these two competing systems. Hollerith was much more static and less, well, it was very useless because you use mechanical linkages to set up your accounting process. IBM fortunately used combination relays with plug-board which gave you a much much wider range of programming potential than the simple-minded mechanical linkage system of Hollerith. Friedman had occasion to make some studies on the IBM system and he was intrigued by it but unfortunately for him at that time there was a depression on and there wasn't any money and so

he was denied any opportunity of testing the IBM against the cryptanalytic processes and he couldn't do this commercially because of the attitude of secrecy which surrounded our whole activity. Now keep in mind that the Secretary of State, Mr. Stimson, had ordered the dissolution of Yardley's unit and that the people in the Signal Corps and in G2 had actually gone to the trouble of putting our unit in the Signal Corps because they were going to justify it in terms of being an essential activity for our code production program for which our Chief Signal Officer was responsible, and their justification for teaching us, training us, as cryptanalysts was that you had to be a cryptanalyst before you could be a proper cryptographer and if you knew the weaknesses of the cryptographic systems you could therefore produce a better system and when Friedman would start making his requests for IBM equipment they would, he would be reminded by all those concerned and rightfully so that we were lucky to have what we had and let's don't go making waves until ~~we get some~~ there's more money and we're out of the depression. Fortunately to

sort of wind up this comment about IBM the quartermaster had an installation and Friedman found out that this was about to be closed down and so he made arrangements to use it part-time at night and we went over and actually employed these devices for the compilation of type codes, division field codes, the training edition and we turned out four or five codes in what normally would have, well, we did it was about a 5 or 10 to 1 ratio. We did five codes I think in less time, about half the time, it would have taken to prepare one code and got a manuscript that was totally acceptable by the Government Printing Office where we had ~~the~~ our codes printed just from one operation. We had five manuscripts that, I believe it was five, somewhere in that neighborhood. Now also at that time there was no idea, no idea, of computery as we can look back on it and think about it today. The limited work that had been done in England by Babbage, ~~Babbit~~ which is pretty well set forth in his story of calculating machines was unknown to us. The closest that we came to computery and I use my own term here rather than somebody else's

term is in a visit we had that was I think arranged because Kully had read about the work being done up at the University of Pennsylvania University of Pittsburgh I believe. Well it was done in Pittsburgh, but the school it was slips my mind now and we had this fellow come down and talk to us about what he had learned about these special devices that would do some of these more onerous calculations very rapidly and when he got through talking about it we were overwhelmed with the astronomical problems that he was solving and we saw very little benefit to the kind of simple-minded cryptanalytic problems we'd had. Now there were a couple of other things that might be mentioned here in terms of your question. The navy had made a contract with Vannevar Bush and this was the scientist up at MIT to built a sort of comparator so that he could drag one cipher text against another cipher text to find whether they were in phase, that is the same key. This was an index of coincidence machine called the IC machine. ~~Bische (?)~~ Bush once told us on one of the rare occasions that we had to talk to him

that he was not very well pleased with his work on this machine because it fell far short of what he thought could be done but he never did tell us what he thought could be done. He just went away sort of leaving us waiting for him to explain further and he just never chose to so to talk down to you a minute there was nothing that lead us to believe that there were magic machines that could do the kind of things that had to be done by cryptanalysts. The labor saving machines to shorten the time and to achieve results satisfactory results in the time required for dealing with a very complex system. Nothing to lead us to imagine that this would be possible. As a matter of fact the information that we received particularly from ~~Bischel's~~ Bush's experience with the IC machine and what we had learned from this professor from Pittsburgh lead us to conclude quite the contrary. It was not until we were confronted with the J19 problem that we had reduced any of these things to practice. Now I'm jumping around in time here. Your question was directed at the early days and I guess the simplest answer to

it is that in those days we had no concept of computery. It was a glint in Friedman's eye that maybe we could be helped by ~~the~~ accounting machines, particularly IBM, not Hollerith because it was so inflexible and that some day in the future we might find something that would be useful to us but we were so busy learning to be cryptanalysts and had very little skill and talents in developing computery ~~and~~ so we were lead into the investigation of the more sophisticated possiblities that might have occurred to us in computery and I think there is a good story that can be told about J19 and how it really opened the door into the application of computery and really the development and invention of computery ~~is~~ as a cryptanalytic aid and then spillover later into the public domain.

Q: At what point did you become acquainted with the systems of the first World War, besides the ADFGVX cipher, or even that one? The reason I mention that is because the French used ~~in a traffic~~ an enciphered ~~cipher~~ code which even today is pretty good for the purpose.

Valaki

A: Well, there was no point in time when we became aware of these things. I guess

if you try to identify a time when we learned something about WWI systems is when Friedman took us down to the vault, 2742 Munitions Building, where Yardley's records had been stored and this was sometime in the middle of the summertime 1932 and our first job was to sort of organize these files and select from them, particlarly the ADFGVX, because now here again is where Friedman had a glint in his eye that the rest of us probably weren't ready to appreciate. He thought that the special solution had been developed by Painvin and others, by the French cryptanalysts, was not the right proper answer of the problem. He thought that the general solution so that you could read almost any message that was enciphered in this ADFGVX cipher, he thought that this was possible and so one of our first research projects was to develop such a solution. So in organizing these files we ran into a variety of things. Most of them very little traffic because evidently Yardley did not see fit to carry over beyond the Black Chamber era some of this WWI traffic but for some reason a whole mass of

all intercepts of the German ADFGVX messages had been retained and these were pretty much intact and any other systems were sort of incidental to this. They either didn't know what to do with them or they got misidentified and assigned to the German military traffic files so there was very little practical real material to for us to study except the ADFGVX.

Q: Valaki Does that mean that in the files there were no German dip traffic left over from the first World War?

A: No Maam. It just means that I don't remember it.

Q: Valaki Oh OK.

A: There probably was some but I don't imagine there was because Yardley's group were interested in maintaining continuity of intelligence production and not in doing research on old systems in the sense of promoting their cryptanalytic capability. This was for Friedman to introduce later on and for which he should receive full credit.

Q: Goodman Did you get a chance to go through the whole of Yardley holdings in the vault _____?

A: Not only did we get the chance but we were required to because part of our job was to catalog and index and classify that stuff so we could sort the desirable stuff from the ADFGVX, the Japanese of course we wanted to do some review of that and then we wanted to review the other traffic, The Italian, the German, the French, the South American countries' traffic so we could develop a hard core of information on each of these hopefully in due course maybe in the next decade or so to actively and aggressively attack them and produce intelligence from them.

Q: Was it all cable traffic?

A: It was all cable well let me make a statement as correct as I can. I know that the current traffic was cable. There may have been other stuff which we would have overlooked and which time would have erased from my memory ~~but~~ I just don't remember.

Q: But the great majority of it was?

A: I remember distinctly there was a large amount of cable traffic and I can recall no other traffic other than the ADFGVX and maybe some associated miscellaneous

traffic that looked like it was radio intercept.

Q: That was left over from the first World War? Well the Yardley period. The ADFGVX. When did that go out? I haven't seen it ~~said~~ seen it end anywhere.

A: You haven't seen what?

Q: Its end. Because I know in 1919 for the peace conference Yardley reported back that they were reading only two German systems and one of them was the ADFGVX.

A: And they were reading it only under favorable circumstances of having messages with repeated (beginnings and endings) beginnings and endings.

Q: That was the special solution from the French wasn't it?

A: Yes the so-called ask Ambassador Childs about this.

Q: Yes, I've....

A: He'll have a good story on this and I'd like to read it if I ever get back. But now go back and let me tell you what I remember about the ADFGVX. I believe that when Germany lost the war that the ADFGVX died as a cipher, an active cipher. Now the GErman forces when they re re were reconstituted may have adopted something like the ADFGVX but it was a field cipher as I recall and it would be most unlikely that it would be used after the end of hostilities.

Q: Well I know that it was used in December in 1918 when it was recorded in Childs

notes. They were still reading it. They were still using it to withdraw in fact there was some pretty good economic intelligence in it.

A: Well I won't fight with your date...

Q: I happened to find it you know just by chance and it sort of has puzzled me and also Yardley's report in 1919 I think it was in March or February saying this is one of the two German ciphers we're reading. ~~Rather particular~~ Sounds peculiar but I was just wondering whether ....

A: My recollection is limited to our work with ADFGVX traffic that is reported on in the technical paper.

Q: Where did that traffic ... It just happened to be in Yardley's ...

A: No Maam. I think it was came about this way and this is sort of guessing rather than factual knowledge. I know I've heard Friedman say that when he was attached to the French cryptanalytic activities in Europe that what they were seeking was a general solution to the ADFGVX, that he had become convinced in his own mind that such a thing was possible and that this could be attained through statistical approaches but that there had not either been the opportunity or the skills

the mathematical skills available to test this out and I think it was a result of his interest and his conviction that you could have a general solution of the ADFGVX which would be much better than ~~Panvan's~~ Painvin's solution that caused that traffic to be saved and I think he saved the select traffic, some of it obviously was fine traffic because this is what we worked on. We picked the day with the greatest number of messages and we identified the ones with the odd keys and the even keys because we developed this statistical group and then we were able to finally zero in on one day's traffic and break the key and for that day or for that period and then we just spread this and went ahead and did enough other days so we could prove that it wasn't an accident, That we had indeed achieved a general solution.

Goodman

Q: The three of you got it? The general solution?

A: Yes. Abe and Kully and myself were the ones who did the work under Friedman's general direction. Well I think well the thing that came out of it, We'd been working on double transposition. We discovered some pretty significant new principles not earthshaking but we'd made advances in working on double transposition in particular. Also we had done had developed a very good understanding

of statistics and how statistics can be applied particularly in alphabet matching and also we had realized that there was a difference in taking the digraph for example there was a difference in the expected frequencies of the initial letter of the digraph and the final letter and also ~~statist~~ fact attend this we had recognized the positional frequency characteristic of a code group, whether it be literal or numerical , could be significant in some cases. Well for example take a simple case. Some codes would, particularly dictionary codes, would go off maybe through 3000 and so you'd be limited to three digits in the first position and then you would find that the frequency of the second and the third and the fourth and fifth digit in this five-letter code group each would have its own significant frequency characteristic. Five might be the most frequent for the second position and some other letter for the third position and so on. So you can sort of have your have your statistical penetration of a base for statistical penetration laid by virtue of this fact. Well the magic

of the ADFGVX solution was that the fractionating square was devised and frequent letters all from the same column that one letter would stand out and you could find just by looking at the message. You wouldn't have to make a frequency distribution. Well taking this sort of obvious principle and refining it into mathematical, taking advantage of the mathematics we knew about in those days, we would find the tools. It was very effective in breaking into the ADFGVX messages. Now it just happened that the ADFGVX was a good vehicle for us to develop this on because the same thing, the same principles, applied later on to the Japanese system which we worked out and again to repeat myself laid the basis for the first computerization of cryptanalysis because and that's another story. I think that is about the size of it on the ADFGVX. Friedman had a glint in his eye. He used us to establish that the glint in his eye was a real inspiration and a vision and then having used the ADFGVX as a vehicle for proving that he had made the correct assumption. Later on we did expand these principles into a

broader application with even more fantastic results than ~~even~~ Friedman had imagined when he first thought about it.

Goodman Q: ~~Are~~ you suggest~~ing~~ed that, earlier on in your remarks on this, that Mr. Friedman was assigned to the French.

A: That's part of his record.

G. Q: (Do you know you have stated that position?) wjr

A: I don't think he obtained it. I think he.....

G. Q: Or decided upon it maybe would be a better.....

A: Well, it was inspired by it.

G. Q: Inspired by it.

A: That's the way I would like to say it. This was an inspiration of Friedman's. This inspiration may have been stimulated by his conversations with ~~editors~~ others but I think Friedman was convinced that this ought to be explored and his conviction was so strong that he actively arranged for it to happen. I said it right, now. I said it correctly.

G. Q: Let me ask you another question then about the business of the Yardley collection once again. This may seem redundant but I think we ought to have it for the record. There was no intercept material traffic whatever which you recall as having come from for example army radio intercept activities in 1921 onward period.

A: I can recall nothing of that nature but I can recall volumes of cable drop

traffic.

G. Q: Cable drop traffic but nothing _____?

A: I recall nothing. This just means that my recollection, I'm tapping it, and it means nothing more than what I've said. I didn't recognize it if it was there. It could have been there.

Valaki Q: Can we go back to the ADFGVX, Mostly as ~~as~~ the source or the selling point of the development of new techniques. What particular techniques can you advise can be traced to work on the ADFGVX cipher?

A: Two major ones. One is the utilization of positional frequen~~cies~~y characteristics, so that ~~XXXXXXXXXXXXXX~~ you can take advantage of them in your cryptanalytic attack and that's essentially it. Of course, again depending on the system you'll have to devise how this ~~will~~ would be applied. And second it simplifies the cryptanalytic process to the point of where it could be developed into a type of program that lead to some of the primitive computer procedures, The adaptation for example of the IBM machine and the publication of the GEEWHIZER which I think even by today's standards ~~were~~ was a pretty sophisticated device and I will repeat my earlier conversations with Hank here, the thing had a memory, primitive as it was. It could

draw a.. it could do the IC task that the ~~Bishe~~ Bush machine was designed for. It would give you a statistical evaluation of each one of the ~~texts~~ tests automatically and finally it would discriminate and tell you which were the more likely ones. In other words you set a level and if you got above that level, the total got above that level, it when you looked at so you didn't have to look at a bunch of ones that weren't very likely. In terms of statistics if you drew ~~a~~ the probability curve it would clip off the upper end of the probability curve and reject everything below the optimum positive level that you set. Finally I think it represents an effective application of something invented by Albert Small and that was the use of logarithms in lieu of the absolute values or the observed values of the statistical values which got away from the problem of multiplying and simply by adding logs you see you got the effect of the ~~problem~~ product of the probabilities which I think was one of the cleverest things I ~~ever~~ have encountered in my whole business in cryptanalysis. Small just came up out of the blue with that and it was

beautiful. Everybody else had missed it.

Valaki

Q: May I ask also ~~about to mention~~ as long as you mentioned the IC about your introduction to the IC? Did you ever see the Riverbank publication?

A: Oh yes.

Q: _____ early in the game?

A: Yes. Those are part of the fillers that Friedman gave us while Kully was getting ready, catching up, with Abe and myself, Friedman. See I was there first so I was the one who was always out of a job and he couldn't find enough things to do in those first couple of months to keep me busy while Abe caught up and then Abe and I sort of paired off and we did some simple things like proofreading manuscripts for him and other things but he just didn't have enough that he could trust us with so that we could he could keep us fully occupied and I remember hounding him one day about I was out of anything to do so he said I will bring you something in the morning and he gave me some ~~trigger Jack nik work~~ trivial job, make work until the day was over. Next morning he came in with three Riverbank publications and handed one to me and one to Abe and one to Kully and these were the ones well I think one of them

was the transposition solution ~~tion~~ route ciphers. He didn't ~~got~~ give us the one on Wheatstone, ~~I preached on~~, the star ciphers, because he saving those for special examples in our later training period but the more trival ones he handed us first. One on secret inks he gave and these were make work but honestly outside of the one on the Wheatstone cipher, I think it included the star cipher too. I'm a little hazy on this. The rest of them ~~are~~ were pretty trival and I think Friedman knew it because he was pushing so hard to get the technical papers published.

Valaki

Q: Well what surprises me is that ~~when~~ once Friedman got the IC that he didn't sort of apply it to everything he had. You know it seems like such a terrific thing to do that I don't know why he just didn't take up traffic and try the ~~idea~~ IC on everything and then after ~~capitus~~.

A: Maybe I could explain that if you will define what you mean when you say IC.

J. Q: Well I'm not quite sure what at which point after you came in which point was developed because the I.C. and the Kappa test ~~capitus~~ both which are ~~whether~~ ~~which~~ what any other statistical test ~~text~~ but this is under your slide ~~applied~~ one piece of text against another piece of text and count the occurrences and then measure the number of occurrences against the expected at random. That is as for plaintext of ~~whether~~ whatever we use languages.

A: Well this.... I think I can act a little more intelligently in response to your question because your definition of the IC ~~text~~ test is exactly what ~~Bishe~~ Bush had in mind when he developed his machine. You counted the coincidences and made a record of them and recorded the number of coincidences for each position of match if I can call it that, and then you explored it, these totals if you will, to see which one looked like it might be the right one. Now the ~~capitus~~ Kappa test turned out to be a pretty trival test because as a practicing ~~and~~ cryptanalyst you could look at them and tell better than you could figure them out. If you got into the ~~capitus~~ Kappa test at all it was sort to validate your judgment after you made the inspection of the results so we we also were handicapped by something that I think became a very practical consideration in our work and that is your ~~capitus~~ Kappa test has to be reduced to a sort of standard base. It was a lot of it was a problem in arithmatic you see to take messages of different length and ~~messages~~ matches of different quantities and reduce them to all the same base because you could look

at the curve and you could tell and sort of make a mental judgment a lot easier than the ~~capitus~~ could be made, so we didn't we weren't too formal a little bit maybe loose in our displinary ~~codes~~ approach but actually it was just like solving a crossword puzzle. _____ worth a lot more than the mathematics because the mathematics will give you a general idea but the real test is ~~the~~ ~~degree~~ does it read? Now we were great believers in making tests ~~to~~ that read, you see, and not to satisfy the mathematical criteria that we established. Now the ~~xxxxxxxx~~ IC ~~xxx~~ test ~~was~~ is only one of ~~the~~ a great many statistical tests. We well I think it doesn't take too much to appreciate what you can do ~~xxxxxxxxxxxxxxxxxxxxxxxxxx~~ simply by siding one message against the other but the real test is when you get into more sophisticated things ~~xxx~~ as ~~intensified~~ exemplified in Friedman's ~~book~~ work on the Heb~~ron~~ern machine ~~so he used~~ where he uses the basic, well, the interval test, I call~~ed~~ it _____ certain ~~matters~~ letters appear~~ed~~ more frequently ~~and~~ or more likely to appear ~~garbled~~ doubled at different intervals, for example, E you find more E at 2 and 3 intervals 4 ~~about~~ well, maybe 3-4- and 5 interval than

you will ~~another~~ some letter, and new that is another form of statistics. A Third form is in what is generally well it is pretty basic to the ADFGVX [illegible]. That's practical characteristic. And as Japanese ~~why~~ where you can go to town with all sorts of frequency counts because the double letters in Japanese like double O and double U, and since the vowels comprise about half the text you get a terrific statistical representation. You cannot look at this as a simple IC test but a variety of classes of tests that you can apply in a refined form depending on the cipher system that you are dealing with and you sort of ~~connect~~ select that statistical test which will allow you to penetrate to some degree the mystery that's produced by the encipher~~ing~~ment process, and I think we were more concerned ~~in~~ with developing a variety of tests than concentrating on how sharp we could make the IC test. ~~Well~~ What other tests were there that could be applied to our problems and we just passed them through easier solution.

Valaki

Q: How did you develop [illegible] ~~your~~ people who developed the [illegible]

for enciphered code, additive enciphered code?

A: No. We I _____. Kully may have had some ~~too.~~ clue, If any of us did

it would have been Kully but I didn't realize what a difference table was

until after we started collaboration with the British. Now I speak of this in terms

of the pragmatic application of the difference principle~~s~~, in terms of different

stages and things like that. We were fully on board though ~~with~~ as to the statistical

implications of it except we had so many beautiful machine ciphers to work on,

at least in what I was conscious of. Maybe Kully would tell you different. Abe

would tell you different but from where I sat it was all machines and there were

so many of these and our techniques were so powerful that we didn't concern

ourselves, and had no reason to concern ourselves, with the and I ~~would~~ will sit

here today and say with the trivial aspects of the difference table because the

difference table is a sort of a technique, a way of doing things, it's not a sophisticated

thing in itself. It's a tool. It's a shortcut. It's a sort of a golden trick that you use it employ rather than being a sophisticated approach. Now, Some of my friends who are additive solvers will get sore at me because I put it in this context but I think Friedman's work on the Heb~~ron~~ern machine was much much more significant than the difference table technique. Incidentally that difference table is nothing more than an indication of IC. It's another kind of a tests and it's a quick way of establishing the IC. If you think about it I believe you will believe it.

Valaki Q: I see that you're thinking of it theoretically rather than practically.

A: Both. Practically the difference table is a fine thing if you've got a bunch of people that you don't have much time for training and who have a particular problem with a good statistic~~s~~ underlying statistic~~s~~, a difference table is hard to beat. But theoretically its just one representation of the IC, that is ~~It's~~ useful to have rather than being the total answer to the problem. Difference table

will provide about, now I'm guessing ~~am~~ and I'm making an estimate, will take advantage of about 90% of the cases. But It doesn't provide a 100% ~~and really~~ advantage and really when you get the answer, ~~when~~ if you get the first one and it produces the answer then that's all you need. You don't need it dredge all the way down to the bitter end. So it's a handy tool for shortcuts.

End of Side 1, Tape 2

Tape 2, Side 2

Q: We can back up to number 3 I asked about Yardley. If he was mentioned, and if he was, in what light was he mentioned. I'm very curious about the man himself I guess. The idea of how people actually saw him in the field, particularly after the 30's after his book had come out and he had become somewhat of a rogue, I guess.

A: Let me tell you what I know about Yardley. The first time I heard his name was when Friedman talked about the American Black Chamber and he reminisced a couple times. One of the stories he told about Yardley was that Yardley was a guest at Friedman's house for dinner one, one evening and Friedman, you know, was a great one for playing up cryptology and cryptanalysis and things and he was a little bit bugged by it in terms of present day slang. I mean he had a thing about it and the menu for this dinner was supposed to be in cipher and before the party got served the dish, they had to figure out what it was, and Friedman's story about this dinner was centered on Yardley's reaction because one of the items on the menu

was an indeciperable cipher cifré and cifra and they were speculating I guess as to what this might be and Yardley spoke up and said "Well it might be hash but no self respecting host and hostess would serve hash"and lo and behold that's what it was, (laughter) and that's the first thing I remember about Yardley. I didn't meet him because Yardley was a little bit of an uncertainty in terms of what we were doing in ~~terms of~~ the SIS. He knew about Friedman and Friedman's being a code ~~encipher~~ and cipher specialist for the Chief Signal Officer in terms of the code compilation program and that was the reason Friedman was hired in those days not for his cryptanalytic capability in the sense of intelligence production but for his cryptanalytic capability in the sense of improving the codes and ciphers and I think this is an important distinction and it ought to be underlined if we could underline it in the tape here. Well now, when Yardley's outfit was closed down and (the attitude of the State Department was pretty much negative towards the continuation of any activity like this) and the Signal Corps and G2 have nerve enough to get

up and start ~~a~~ the new operation outside of G2 (and away from the State Department) of course a great great envelope of secrecy was placed around it and one of the things you didn't do was to contact people who had been associated with the old Black Chamber activity because there might be some way of (the existance of the new unit leading back to the State Department and Stimpson or whoever it was at that time that had been responsible for Yardley's outfit being closed or taking action to stop it over in the Signal Corps), and it's amusing I've heard the discussions that the cover story is ~~their~~ they're just simply we're augmenting Friedman's activity ~~for~~ in support of the Signal Corps code production program and that's why we didn't get started on intelligence production I think until somewhat later even though we had an intercept capability that was coming into being parallel in time to the formation of the Signal Intelligence Service. Well what broke Yardley's back, I think there was some feeling that maybe later on Yardley and Manley and others would be called in. Well, let me introduce something here and sort of correct a misimpression that I may have given. Initially

and this is in the first few months, there was very little well I don't know of any contact with Yardley's group but before possibly within a year or a year and a half Manl~~e~~y was invited in and he came to Washington. Friedman brought him into the office and introduced him to Abe and Kully and Hurt and myself and we met him and he was an old man and we were very impressed by him because Friedman was obviously showed him a great deal of reverance and then Charlie Mendelsohn, Dr. Mendelsohn came in~~n~~ him. He was ~~a~~ at City College in New York and later on I think he moved around a little bit. I ~~think~~ believe he died from the aftereffects of scarlet fever. That was the diagnosis but there was great suspicion~~s~~ that he might have been killed by the Germans, because of the strange circumstances associated with hi~~m~~s being stricken with this disease. There was some suspicion that he might, because of the notoriety that ~~big doubt~~ leaked out about him, that the German intelligence services ~~might~~ may have found out about him and neutralized him but I think that was pure speculation. I think it was an old wive's sort of imaginative attitude. Now

these two gentlemen did come in and Parker Hitt came in and I was really pleased that we got the chance to meet him and he was he was really on our side, he and Mauborgne were ~~Mobern was~~ the great supporters within the Signal Corps of this concept. There was also a fellow whose name I might mention in that time frame and I'm wandering from your question but I don't think you'll get this out of me with any other question, was Col O. S. Albright who was the action officer in G2 and he was the one who drafted the G2 side of the plan for the organization of the Signal Intelligence Service and the Second Signal Service Intercept Activity. Well of course Yardley was not included in this ~~inter~~inner circle of people that were knowledgeable of our existence and our plans and what the Chief Signal Officer and the Director of Intelligence expected for the unit. The next encounter with Yardley and the one where he ~~first~~ forcefully came to our attention was when the Black well when the series of three articles in the Saturday Evening Post for which he got a thousand bucks each which was a fabulous price in those days for an

DOCID: 4223202

article like that and then when the Black Chamber came out Friedman really hit the ceiling. I just could not understand then nor can I understand today why this should have rubbed Friedman as hard as it did, but he was fit to be tied and I mean literally fit to be tied and he got ahold of the book and he and Mendelsohn collaborated in making well there's an annotated copy. I think it's down in the Marshall Library. You should get that and have it photographed. You'll get a terrific appreciation, a biased one, but some appreciation of Yardley and what Yardley, I mean the impact of Yardley's book on the cryptanalytic concept and the people involved with the Signal Intelligence SErvice. ~~You~~ You'll get how they reacted to it in terms of the people who were directing it. Of course Abe and Kully and I were such kids at that time it didn't amount, well we thought it didn't amount to anything but you'll get Friedman's and you'll get the kind of thing that went up to the Chief Signal Officer. I believe it was Ingalls. I don't remember who the Chief Signal Officer was at that time. From that minute

on Yardley's name was ~~MUD~~ mud so far as our activity was concerned and then

although Yardley ... there was some consideration given to whether or not Yardley should

be brought in because Yardley had a lot of people who admired him and thought

he was pretty terrific and I think ~~that~~ if they had chosen up on sides that they

would have voted for Yardley rather than Friedman to head this activity because

Friedman was pretty much an unknown quantity in G2 whereas Yardley was

a bit of a celebrity and one of the lights in the circle, small circle, of people

who were involved in intelligence and you must remember that the intelligence

personnel in G2 inbetween WWI and WWII were pretty pretty naive unsophisticated group of people

so Yardley, as a professional cryptanalyst, and this seems to apply to cryptanalysts

in general who had been successful and only those who had been successful, Yardley

was looked on as pretty much of a, well, ~~Mobern~~ Mauborgne used the word magician to describe

cryptanalysis. It was a little bit of that magician aura that Yardley had inherited

in the G2 circles but he was practically unknown in the Signal Corps and since

the Chief Signal Officer was ~~the~~ administratively responsible his OK had to be received before Yardley could come into the activity and the Chief Signal Officer wasn't about to go against Friedman's feeling which were very anti-Yardley at that time and so Yardley was really just closed out.

Goodman Q: Do you recall in that period, sir, whether or not anyone else in the Signal Corps took as strong as a position as Mr. Friedman did, seemingly did, against Mr. Yardley?

A: Well Friedman's position was unique because in ~~this~~ the Signal Corps they were more interested in proper Signal Corps activities and most of the Signal Corps officers that I bumped into looked on the Signal Intelligence Service, there's one exception, I'll mention his name, looked on it as a sort of extracurricular activity which they were doing the housekeeping for and they weren't particularly interested in supporting or being involved in the thing. They looked on it as something that well possibly should go on but that's somebody else's watch and I don't, I won't get involved. Now also since Friedman was the high priest of the cult his attitude more or less was accepted by the rest of the congregation

namely the Chief Signal Officer and the others who looked on him as being the keeper of the wisdom and so Friedman's wisdom was anti-Yardley and therefore this spilled over into the Signal Corps attitude and there is a certain amount of distrust I think too present because they felt that the publication of Yardley's book was a kind of a dirty trick and one of the things that resulted from it was that both G2 and the Chief Signal Officer with G2 carrying the torch we got this law passed about the revelation of information about 330-5, is that the one Hank?

AR 330-5?

(Hank) (I don't recall)

(laughter) I used to revise and help review it and produce revisions to it which would go down to the War Department for publication in Army Regulations so we were the action body on keeping that regulation up to date. Yes sir.

Goodwin Q: Did the folks at G2 react separately or in concert or were they particularly

203 startled by the publication? after all, ...

A: There was no question that they were really really put out by this thing. I think the people who were pro-Yardley up to the point that the book was published

turned against him. They thought this was uncalled for and while there was no law they could invoke to stop him and there was really nothing that they could invoke -- law or moral principles or anything else -- because they were sort of tied because of their position and to go out and fight this book would give it more publicity so they would just confronted ~~it~~ just like Norm Boardman every now and then is with one of this problems and they reacted a great deal like Norm Boardman reacts. They don't know what to do.

Nobody else would either except somebody who was brave. Now I want to mention this exception. Carter Clarke had, I don't know, he had an insatiable curiosity about intelligence matters and he was our greatest supporter. I first met Clarke when I was doing a stint of night duty down in the War Department message center. He was I think he was a captain at that time and he was in charge of the radio station over at Fort Myers, which was the transmitter site...

Q: It was WAR, wasn't it?

A: W-A-R, ~~That was the~~ is its call letters, yes. Not war in the sense of WWI (laughter), but I don't know why they chose WAR ~~but~~ except War Department, this is War Department top radio

station and he also was responsible for the maintenance of the message center equipment. What happened is that the antennas and transmitters were located over at WAR, Fort Myer, and then they were keyed remotely from positions in the back of the fourth wing of the Munitions Building where the message center was located and there was ~~the~~ whole lineup of intercept not intercept but operator positions along one wall, the last portion of the wing there, and the code room was up in the front left hand corner of the third left third of the wing and that's where I was working and so Clarke would come in and he was responsible not for the code room but the support of the code room, make sure we had lights, tables, furniture, desks, typewriters and all the things that you need in a code room but he wasn't responsible for the operation of the code room. That was sort of the personal responsibility of the communications group and, but as one of the members of that group, on his inspections and he would come in at the oddest hours of the night and just looking over the place and see if it was running right. It

was a good thing to do. He came into the code room and introduced himself and we got to talking and he was very curious about me and my background and how I liked the work and what I thought ~~his~~ its future would be. So we got to know each other pretty well. We ~~got to be~~ became sort of personal friends which was unusual for a young country boy and a regular Army officer because the Army officers were a cult unto themselves and they had to maintain that image and they didn't get too palsy-walsy with civilians. But In this case Clarke and I got to know each other so we were sort of a first-name at that time and later when he became my boss I called him Colonel. Now Clarke was intensely interested in this thing and I think he, while he never agreed in all instances with Friedman, he wasn't a rubber stamp, still he was a great supporter of Friedman and the things that Friedman was trying to sell. I think Clarke knew that you didn't win all the battles but you suffered some losses. As long as you won the war he was happy but he could lose a skirmish and never turn a hair. He'd just go and

start another fire some place else and if he lost that he wouldn't care he'd ~~just go and~~ start a third fire. I think a very remarkable man and totally unappreciated. Well I set him apart because he is unique and I think he made a wonderful contribution and helped ~~Mobern~~ Mauborgne and the others, Albright, by his support because one voice out there in the ranks sometimes will have as much effect as, ~~well~~ will offset a distant voice from the front row, and he had a a ~~great head for it~~ very good voice and he was very vocal. He had a mastery of words and I think he did a lot of pseudonym, nom de plume, writing forwarding. He had a couple of articles that I know about published in the Saturday Evening Post and he was a good journalist. Now enough ~~of~~ for Clarke and a little bit more about Yardley. I think I've said this before but I'll think its a good place to repeat it. Yardley's next appearance so far as the Signal Intelligence ~~was~~ ~~co~~ was concerned was when Yardley was hired by the Nationalist Chinese as a code expert ~~and~~ in their efforts to crack the Japanese military field ciphers. This came about directly as a

result of Yardley's publication of the American Black Chamber I'm sure because the Chinese thought if they could get this American ~~exploit~~ expert who had been so successful in the diplomatic codes working for them he might have the same degree of success on their military codes. Well Yardley didn't score a point I think in that game. He was completely whitewashed because (1) he didn't have good intercept, (2) he was so conditioned by the cable drop ~~companies~~ traffic that he have no concept of what you would expect from an intercept group and therefore it was impossible for him to organize one and (3) he had all the built-in difficulties that the Chinese have which he was a western or didn't understand. The kind of things like how you get ~~the~~ a Chinese to do something he didn't quite understand. He was trusted completely by the Chinese with the intelligence that they had gleened although they didn't trust him with the policies and political activities. He did have access to their intelligence files. The, after the Japs did what they did in China ... the Chinese suffered their heavy defeats, Yardley came out by the Burma road, he

was one of the last last guys to get through and came back to the states and at that time Akin was in charge of the war plans and training division, General Spencer B. Akin, he was a Colonel at that time and Akin thought it would be useful if we got Yardley to prepare some brochures, technical brochures, on the information, that ~~he'd~~ developed in his work on the Japanese field codes, military ciphers, so he arranged for a contract to be let. Yardley produced ~~the~~ some papers. I was the action officer, review the papers, ~~spring~~ explain the contract to Yardley and ~~later~~ lay the requirements out so I used to meet with him regularly, once or ~~like~~ twice a month in his apartment which is up on F Street ~~just short~~ just sort of north of the Munitions Building and he would present what I would look at his manuscripts and we'd discuss whether this is what we wanted or not and I'd ask him questions, you know, sort of feed him questions that he could answer because we wanted to get this we wanted to get as much out of him as we could. He was never permitted into our sanctum sanctorum but he did a couple of times come down to see ~~Yates~~ Akin and I

think collect his money and sort of formally meet the formal requirements of the contract situation. The some of the things that disturbed me about this relationship ~~is~~ were as follows: (1) Edna ~~Ramaseur~~ Ramsaier, Yardley's paramour, was an employee of the Signal Intelligence Service. I'm sure we had no secrets from Yardley (2) I often suspected that she was feeding him back information from us which she would include in his reports. I couldn't prove this. I discussed it with Akin and we decided well the idea here is to get as much as we can from Yardley. This give us a measure of what he knows which in itself is useful and probably as useful as any fabricated material that he ~~could~~ would put in and the feedback may stimulate him to recall things which and help us ~~to~~ answer questions which although not designed might be a more desirable situation than without it. I love this attitude of Akin's It was not one of anger "Kill the son-of-a-bitch off" excuse me maam, and whoever hears this tape, but it wasn't

374 that there at all. This is an operation. We will get the ultimate out of

it and if we have to play this game to get it, let's go ahead and play the game but let's don't be fooled by it. We're still in control of the situation. And this I think is a very sophisticated attitude towards dealing with intelligence things that a lot of people never develop~~ed~~. But Akin had it instinctively and I think it was the proper thing to do. I was disturbed by it. I didn't like the idea of you know buying back, this is the way I put it to Akin, buying back our own dope but Akin said well we're getting more dope in return. He says dope for dope is fair trade in my book and the money is incidental.

Q: Did he have any thing of real value?

A: Well he sort of confirmed (laughter) and it took a little bit of work on our part particularly on my part because I was the action officer, he sort of confirmed what we deduced ourselves and the information he brought -- there was some of ~~was~~ new and useful but it wasn't enough to help us master the situation. It was a tough situation. Yardley, I'll use my word "illuminate" Yardley illuminated the

information that we had developed and in some degree confirmed it but this confirmation is a sort of ~~mute~~ a moot question because did he confirm what Edna told him, assuming she did tell him, and I think she did. It would be ~~more~~ moot unnatural if she hadn't or is this freestanding information that comes from Yardley's own experience. I don't think we'll ever know and I don't think it makes any difference because it wasn't, as time went on, the Japanese systems in war time were much much more impregnable as a massive thing~~s and~~ than we'd imagined in those days so it did help get us conditioned.

Goodman Q: How did Mr. Friedman react to this renewal of the Yardley collection?

A: Why do you think I was the action officer? Did I answer the question? (Yes sir.)

Akin sort of said if I let Friedman go up there I won't get this. I will put the junior ~~man~~ in there to deal with Yardley speaking for me and Friedman was a little bit hurt by the deal because he wanted to be out in front. I think he enjoyed the confrontation with Yardley. He Yardley you see at one time was up there and Friedman was here and now the roles were flipped. This I think was

Friedman's ego that was hurt rather his judgment and I think Akin very wisely avoided the confrontation between Yardley and Friedman and I don't think ~~there~~ it would have been ~~fighting~~ pleasant because Yardley did still at that time have quite a few followers. Now let me say some bad things about Yardley. I think these are part of the sort of perspective that you want. I've said the bad thing about Edna and the possible feedback but usually when I would go up it would be about 10:30 or 11:00. Yardley loved to work late at night. He would oversleep. I'm sure Edna was living in the apartment with him. There was never any evidence of her around but I had a pretty sensitive nose and I the cosmetics that she used at the office were always present in a greater concentration in Yardley's apartment then they were around her desk. Do I need better evidence? and I'm sure Edna was there most of the time but she was never there when I was there. Yardley would usually be in a T-shirt, sleeveless T-shirt, somewhat dirty in front. He slept in it. Evidently he just slept in his T-shirt without any pajamas and

my nose was sensitive. He would sit down at the dinette table where he had his papers spread out. He had a desk with a typewriter on it and he looked pretty rugged pretty rough. Early morning just got out of blurry eyed sort of thing and the first thing he'd do he'd say "Can I offer you a drink, Mr. Rowlett?" "No, thank you." "Don't mind if I have one?" "Absolutely not. Go right ahead." (laughter) He'd open his desk drawer and pull out a bottle and he'd take a glass and he slosh in about two-third of a glass, tip it up. From then on he was first class and he'd do this two or three times while we were there. Sometimes he'd get a little too much before we got through and I'd just usually excuse myself. I had to get back and when would I see you again sort of and we'd make it the next day. This is what I saw about Yardley's drinking habits. Later on I think he tapered off because he got a shot in the arm when he was hired by the Canadians, he and Edna, to organize a cipher bureau up there and I don't know whether the archives show this I think I've mentioned it to you. I don't

remember reading about it but as one of the conditions for collaboration with the UK, the US laid down the condition that Yardley would either be fired from the job, Yardley would be removed from his contact with the cipher bureau, or that the UK could not exchange any American information with the Canadians as long as Yardley was there. The result was that the UK, who wanted a clean arena for our collaboration, brought pressure on the Canadians to get rid of Yardley and so Yardley was fired and I think he suspected exactly what happened. Yardley was no fool and so he came back and hoped his services might be wanted during the war and he was never asked and it was turned down any overtures he made. I don't I'm not aware of any overtures but I'm sure he must have made some and how could he help it.

Goodman

Q: Who took the decision to go after Yardley in that way?

A: Well it wasn't a decision to go after Yardley. Now let me make that clear. The decision was not to allow Yardley in but there was no malice. There was no

punishment in the context of punishment. It was not there. It was let us not permit Yardley to be in and if he is in Canada he will be in because it is inevitable that we will collaborate with Canada so they were simply just getting Yardley out of the way but it, ~~wasn't~~ there was no punishment context here at all.

6. Q: Was this on security grounds or was it because they suspected his ability~~?~~ ies, or....?

A: It was very simply that Yardley had broken faith with the cult when he published the book and he might publish another one. It was that simple. They didn't look on Yardley as a traitor. Yardley was admired but he'd done this thing and he hadn't been forgiven for it and that's, I mean it was that simple. Now there was nothing very complex about this and certainly we had too many other things to do. People who were running the SIS and responsible for its activity didn't go out on on a "get rid of Yardley campaign" except ~~for~~ where his activities impinged on our activities and there they took steps to insulate it and that was the measure of their action.

6. Q: I reckon what I'm really asking is if that sort of proposition were made to the

Canadians and the British? Someone obviously sat down and prepared the necessary policy documentation.

A: I don't think there was any policy documentation necessary for an act like this because all they had to do was to say "Look the US government is unhappy about Yardley's involvement here because (1) he was with the Black Chamber (2) we decided we took the decision he would not be involved in our new activity. He published the book. We didn't like that act. He is in bad graces with the government and we just don't feel that we should collaborate." I mean that's the measure.

Valaki Q: ~~My last question about that~~ the Canadians? For years when I worked on ~~were used to work out~~ problems in

551 which it seemed that the Canadians really would be working on too, it ~~this~~ resulted in aura _____ by exchanging with the Canadians. You know We exchanged fully with the British and some things with the Australians but there were just so tremendous limitations with exchanging with the Canadians and I wonder if I wonder ~~how~~ now whether some of the aura hadnt just hung on?

A: No Maam.

Q: Or just because of other reasons.

A: No Maam. If you mean was there a relationship between any reservations made in more recent years in exchange with the Canadians and was this based on the Candians hiring of Yardley, there is no connection and I can tell you why. Any reservations which we may have had in the timeframe that your question refers to is a result of arrangements between GCHQ and NSA as to the Canadians' role and the interpretation of these broad terms of reference were the limitation of the Canadian's so far as our exchange is concerned. It was simply the interpretation put by the people who gave you the instructions on these broad terms and these may or may not have been accurately voiced. I suspect that they were practical things and they avoided the philosophy behind the exchange and therefore they may have sounded strange to the people who were implementing them but not necessarily strange in terms of the concept under which the collaboration was being conducted, so I would say positively there is no connection between any reservations that

you may have noted and which formed the basis of your question as I understand it and what the Canadians did with Yardley because once Yardley was removed from the Canadian effort and we had insured and obtained assurances from the UK GCHQ people that this was not continuing then the exchange was really open to what was agreed on between GCHQ and NSA and the Canadians sort of took what the British advised them to, really what they were told they could have. The British were a little bit more tactful about it.

Q: ~~Let me~~ Could I ask you a question about the earlier period, prior to the publication of Yardley's book. In 1930-31 say as the junior cryptanalysts, yourself and Sinkov and Kullback, how did you regard Yardley as a cryptanalyst?

A: His work on the Japanese code, the work of the Black Chamber as we saw it through the archives and that was our window into it because Friedman didn't know as much about it maybe as we did. All he knew was the rumors and the heresay and the official understanding of it but we looked down there and we saw the raw material, we saw the worksheets, we saw the catalogs and other things and by the time we got through

organizing that material and getting it filed properly and sorted out the ADFGVX and the Japanese diplomatic and the other traffic we were interested in we had a very good appreciation of the depth of cryptanalytic competence that the Yardley organization had and they were very good at code recovery and code solution because at that time there was very little enciphered code used so it was a book breaking kind of operation. Manly was a tremendous book breaker. He was a master of languages and everything that ~~was~~ is said about him I think ~~was~~ probably not, ~~just~~ doesn't give him full credit for what he could do. I think its something short of what in my estimation Manly stature was. Mendelsohn was extremely good. I wish Mendelsohn was on our team now. He not only was a book breaker but was an imaginative man. He had good mathematical concepts although he was not a mathematican, I mean professional mathematican. He had a feeling for math and he could use it as a tool but in those days there wasn't very much opportunity for the mat well for the use of mathematical disciplines as we found when we got into the

DOCID: 4223202

cipher machines analysis. That's where your mathematical approach really paid off because you ~~looked for Akins~~ can bookbreak - it's probable word, at least I always thought it was because you can't ~~know~~ book break unless you know language and the reason that language helps you is because you have a good feeling for the language itself and you know what word is most logical there and so thats not mathematics, that's linguistics and its how words go end to end in the context of the language you're dealing with. You know more about this Virginia than I do but that's the way I look at it. I from a sort of broad cryptanalytic viewpoint I think I'm ~~am~~ pretty close to right.

End of Tape 2, Side 2

Tape 3, Side 1

Q: Prior to the publication of the Black Chamber was there a degree of mutual jealousy or antipathy between Friedman and Yardley?

A: I don't think so. I don't recall any ~~incidences that~~ instances -- I think there was intense rivalry but more of the nature that you found and I'll speak of this because personally between Abe and Kully and myself, I mean we were ambitious. We wanted to be good in our fields and I think Yardley was a professional and Friedman was a professional so there was a good professional relationship. I think there was a certain amount of not jealousy if you will but I think ~~it~~ this could have been jealousy if it had come where they were cast in tightly competitive roles but they were never you see. Yardley had been removed at the 1930 time and Friedman felt pretty secure because Yardley was not to be told about our new activity because it might lead back to the State Department and we'd be in hot water again you see and they might close ~~up~~ out the Signal Corps activity so I think Friedman felt pretty secure in that sense and there was no reason for him to

be anything but magnanimous toward Yardley but I think there's some evidence of sort of the professional competition that existed between them and one of the examples of that is Wheatstone cipher and the story of it. I believe this is recounted in David Kahn's CODEBREAKERS but the way I see it is a little different from David Kahn and it's something ~~that~~ as follows, that the Wheatstone cipher had been proposed as a military field cipher by the British and had been sent over to the UK and from the UK to the US and that part of the US action on it was to have Yardley make an appreciation a cryptanalytic appreciation of the thing and make an estimate of its security and recommend whether or not it should be adopted. Well Yardley when he analyzed it spoke affirmatively and said, Yes, ~~that~~ this is good and we should use it. And then for some reason Friedman was brought into the act and I think this was not maybe didn't suit Yardley so in the well in what followed this situation was generated for some test messages challenges that would be enciphered by Yardley and ~~was~~ submitted to Friedman to see if

Friedman could break them and Friedman had made a pretty good study of the thing and felt that he knew how to solve it and I think one of the Riverbank Publications talks about the solution of Wheatstone cipher and gives the Friedman attack on the thing. Well he got one of the components and he found the key word for it and he turned to Mrs. Friedman -- working on ~~for certain of~~ these test messages and said I'll ask you a question ~~first~~ and I'll give you a word and you give me the first word that comes across your mind and that's the answer so the component he had discovered I believe was cipher so he said to Mrs. Friedman "cipher" and she came back with "machine". He tried the word machine for the key word for the other component~~s~~ and it worked, and now there was a little bit of a, I guess of a hassle resulting ~~ed~~ from this between Friedman and Yardley because Friedman breaking ~~had broken~~ the messages, he ~~and~~ sort of put Yardley down. I mean Yardley's opinion then well Yardley was shown up as wrong. Friedman did break the messages and there was no contest and I think this may have been the kind of competition between them but they had never

come to the acromonious state which resulted from publication of Yardley's book. It was a kind of a friendly competitive thing where both of them had a certain stature professionally and like all professionals, mathematicians, historians, linguists, some sort of ~~regimation~~ reservation between personalities. I didn't sense any any meanness on Friedman's part if that's part of the question. There was none of that and I didn't know Yardley well enough at that time to know whether he had any such feelings but I can say that when I began to work with Yardley on this contract that I referred to earlier in no case did Yardley ever have a bad thing to say about Friedman. As a matter of fact we both avoided Friedman the discussion of Friedman if that means anything. Yardley ~~did~~ never attacked Friedman and I suppose he well I thought Yardley outside of his drinking habits and maybe his love life with Edna was pretty normal respectable person I guess by today's standards there wouldn't be anything wrong with what Yardley was doing but I didn't think it was the kind of thing to do in those days so maybe I was a little biased against

him. Did I answer your question?

Q: When the Black Chamber was published, you were working on the beginnings of SIS. Did that change your activity in any way? Did it throw a different light on it? Did it cause you to maybe redo some things or change direction or I guess what I'm trying to say the idea that this type of thing was in the open, sort of speak, cause the SIS any real concern or any real problem?

A: Do you mean other than Friedman's personal reaction to it?

Q: Right.

A: Yes I'm going to surprise you with what I'm going to say here. At the time that the book was published and I'm talking about my reaction, not Kully and Abe's. I think you're question is directed at all of us but I think I can reflect of theirs and mine. In the first place we didn't know what all the furor was about. I didn't. I couldn't understand why everybody was so bothered about this thing because this was done. The thing was closed. I was too immature in my concept of intelligence matters to understand the future implications of it and so I was

little puzzled and amazed and I sat there watching with curiosity. Now that was my personal reaction. So far as the work was concerned it made no difference because we were being trained and our code compilation program was in concrete. We funded for it. We had to meet deadlines and we went ahead compiling those damned old two part codes, great big things, doing that onerous job of proof-reading the cross section in the heat of Washington without air conditioners and you couldn't turn the fan on because it blew the cards away, got you all messed up so we just sweated it out _____. The answer? Yardley's publication of the book at that time had no effect but now here's the thing that's going to surprise you. I think looking back that Yardley's publication of that book was a terrific thing for the US government and the development of its cryptanalytic competence because Yardley's book caused the Japanese to realize that their systems were not adequate and in their efforts to improve them they went to something like the Red machine, to the Purple machine and they went from the

untransposed codes to the transposed codes and they laid us a challenge in a timeframe and in a series of operations which enabled us to meet these new more difficult challenges in a way that we ~~drew up~~ grew in strength cryptanalytically and COMINT-wise that we never would have ~~obtained~~ attained if the Japanese had stuck with the old Red machine so I am so glad that Yardley published that book that I could shout about it this morning just like I am and this is from my heart. Now look if the Japanese had not improved their codes in the way they did (1) we would never we would have had the intelligence but we would have never put machines in the proper context of I mean we would have said the Red machine is no good but you get something more complicated than that and nobody can do it but the Purple machine was so much more complicated than the Red machine that we had to work something like 18 months to get it and the navy turned it off. They said we can't break this. We're going to work on naval ciphers and that was their excuse but really they just gave it up because they didn't think it could be done. The UK did not break

the Purple machine and they had a helluva good cryptanalytic organization and their excuse was that they were busy with the Enigma but they had read the Red machine. I don't think the Russians had read the Purple machine because if they had their attitude at the Potsdam Conference when they certainly would have read the messages between Soto and Tokyo about the peace maneauvers, They wanted the Japanese Ambassador in Moscow to arrange. I don't think they would have handled the situation like they did or if they did the people sitting at the conference table certainly didn't know about the crypt analytic success which seems which would amaze me to no end and so I think that Yardley's book triggered and was the critical trigger for a series of actions which lead to the full improvement which we achieved. Now we might have done better under the circumstances but I think without Yardley's book it would have been much more difficult because look how long it took us to realize that the German one time pad was not a code system but a pad-generation problem that you could recover the system by finding

out how they generated their keys see and then by matching the key up with the intercepts and I think indirectly this laid the ground for that kind of an approach because again I'm saying something bad about my British friends but I think they were shocked and delighted at this movement forward, at this achievement It was a milestone in cryptanalysis, but Yardley's book helped us. It helped us a lot more than it hurt us.

(Could have very well been that the Japanese might have ~~scrubbed~~ sprung the Red and the Purple onyou in 1942 or 43 and then you would have been another 18 months after that before you'd solved it like you were before. You might never have gottin into during the war)(Hank)

That's another angle on it. I hadn't thought of that but I was thinking in the simple terms

(It was good that you had solved both those systems in time for them at the most critical time that you needed them)(Hank)

and it also had its feedback into our own cryptography with ~~a~~ the result that it improved ~~resulted improvement~~ it, and I don't think I've ever expressed myself as forcefully about Yardley's book as

I have right here but I'm convinced as I look at it today that Yardley did us a favor and he'll never get credit for it of course because the other angles are rather reprehensible but in the simple act of publishing these results he really promoted US cryptanalysis more than he could have in any other way. I think if he had been involved he couldn't have done as much for us as a result of this publication, and this is strictly fortuitous. (laughter) I can't quite figure it at all.

I'd like to add a clarifying thought to my comments about the advantages which accrued quite unintentionally from the release from Yardley's American Black Chamber although at the time it happened it looked as if a great disaster and I think I'm saying this correctly. If a great disaster had happened to the Signal Intelligence Service by the release of the information in Yardley's book as we look back today and examine this as one example I can make the judgment safely that it probably was a good thing and personally I think it

did help us but now I don't want these remarks of mine about the Black Chamber to be construed as an endorsement of the release of any other item~~s~~ of information whether general or specific. That it could in the long run be a good example. It could be just as bad as it could be good but you never know until 30 or 40 years have past whether it was good or bad and only if it has been released.

Goodman Q: While it may sound trite, I think perhaps the proper phrase is "based on its own merits."

A: I think that helps. We shouldn't use my argument that the release of Yardley's Black Chamber was a good thing that it is a good thing to release any other item whether it be big little or inbetween.

One comment I'd like to make sort of out of context to the question that's been bothering me for quite a while and I don't think I've said this in terms of your history program, but some of the open publications that have appeared in the past few years have made a big deal about the difficulties that we had in providing

new and ~~conditional~~ additional copies of the Purple machine when these were required. This is a

sheer myth because (1) the machines did not have to be built under a contract by

a contractor and in fact the security requirements would never have permitted

~~it~~ them to be constructed outside the Signal Intelligence Service or the navy yard

and (2) the design that had been developed by Rosen for our analog of the Purple machine

was based on the procurement of standard parts from telephone companies and it

was the way these were interconnected and controlled that enabled us to dupli-

cate the function of the Purple machine and since these parts were extremely

well engineered and designed by the phone company to operate many hours without

trouble we took advantage of this and so Rosen's layout, his design, of the Purple

machine was took all these things into consideration and we -- all we had to do

was to assemble some parts which could be fabricated and not identified as a

part of a cipher machine. For example the rotors were produced by putting

together several switches in ~~the~~ a gang and then wiring up the body contacts just

very carefully doing a wiring job. ~~It wasn't anything~~ There was nothing magic about it. We had some jigs which enabled us to very conveniently do this. It wasn't a big job. It was time consuming, onerous job, requiring a lot of patience and a lot of care but if you didn't get in a hurry you could ~~borrow~~ wire one of these things ~~off~~ up -- one man ~~and build it~~ could -- in a couple of days, and we had three men from the Second Signal Service company who were good wiremen and we bought enough of the switches. Akin was very generous with us and he had the idea that we ought to have these things in a great enough supply so if one of them went bad we could have another one on hand and when we wired up enough, ~~then~~ I ~~think~~ and 'd say three or four spares of each one of the ~~others~~ rotors was enough -- we put them in a safe in secure storage but we wouldn't want anymore because we could store the basic stepping switches in open storage you see without security requirements ~~because~~ so the critical thing in the construction of these machines was the wiring of these banks of telephone switches. The rest of it was a case of buying a few control switches, ~~a multiple double~~ multi-level switches,

some master relays, ah keyboards which we could get from IBM just by asking them. They were keypunch keyboards and the electromatic typewriters used were produced as part of our contract for the M134T1's and we had several of those around and they were IBM typewriters and very reliable. Now one instance has been overemphasized in public literature is that there weren't enough machines to distribute to the Pacific. This is an absolute myth because we had machines in depth, wired. All we had to do was assemble ~~them~~ and we could do these assemblies in a matter of hours and I'm sure that we could have put a machine together in less than a half a day and tested it, insured that it was operating, without a bit of trouble. So when anybody reads about the procurement difficulties, the manufacturing difficulties for the Purple machines that have been expressed by some of the writers. They can be disabused, the false impressions laid by these writers.

.....Purple machine that I think ought to be laid to rest, some of the popular writer

and I think Winterbot~~tom~~ham is one of them and his, the impressions that he leaves in the latter part of his book which deals with the Japanese war, certainly indicate to me that he didn't know the difference between the Enigma and any other kind of a cipher machine. The Japanese systems were not Enigmas. They weren't even principles following the Enigma. The Enigma machine was ~~cultered~~ closer to the American machine, the ABA or the M134T1 or the British ~~Type X~~ Typex or the ECM than it was the Japanese machines. Evidently the Japanese had distrusted any known type of mechanical encipherment such as the Enigma wheel or the Heb~~ren~~rew type of wheel and had gone to the concept of using a much more complicated type of substitution maze which resulted in a, to talk about it in terms of ~~a~~ cryptographic things, a substitution maze in the case of the 20 or the Purple machine or in the related recognate Japanese navy machine could be expressed by a box of equivalents or substitutions of 20 elements, 25 elements in depth. So you have a matrix 20 x 25 which there were 25 encipherments of each of the 20 elements across the top. Now this is a lot

more complicated concept than a simple wafer format in which we found the substitution element in the Enigma or the Heb~~ron~~ern machine because this is a single wired wheel with 1 set of 26 wires. Compare this with the Purple and the navy machine. Let's talk about the navy machine in which there was something closer to 26 and so there you ~~have~~ had not one wiring in a cycle which was repeated by itself the endplate as in the case of the Enigma or the Heb~~ron~~ern wheel but in case of which there were 25 separate complex unrelated, well, let's say unrelated -- they were just unrelated and they were pretty much calculated not to resemble each other as the Japanese when the Japanese decided on the type of wiring ~~well~~ so they were much more complicated type of rotor~~s~~ than we find in the Purple machine in the Japanese navy cipher then we found in the Enigma as expressed ~~for~~ by the writers or as we look at the same family the Heb~~ron~~ern or the ~~Type X~~ Typex which really is a converted Enigma.

One comment about Winterbot~~tom~~ham's ULTRA"SECRET. I~~'ve~~'ve got the impression when I looked at the first part of the chapter on the Japanese War that he felt that the

installation at Bletchley might have been used or a modification might have been used by the Americans for dealing with the Japanese problem and he didn't distinguish between ~~the~~ Japanese military ciphers and diplomatic ciphers. I think this might bother some people because since there was such a vast difference, since there was no relationship between the cryptographic principles employed in the Purple and navy machines and the Japanese military systems which were non-machines in the main. only a small example, Something less than a fraction, a fraction of a percent, could be ~~that the~~ ~~Japanese~~ expected in the Japanese military machine to be and this would be the Green machine, as we identified it in those days, andwe never found a case where that was used. I think we can logically assume that the bronze godess was completely useless in any way against Japanese ciphers and would therefore would not be of any benefit to the exploitation of Japanese ciphers. As I recollected, and I'm pretty sure my recollection is as good as anybody's, the bronze Godess was an analog ~~synonymal (?)~~ of the Enigma machine in such depth that they could duplicate

the ~~actual~~ action of the Engima machine and it was the specific wiring which was employed in the wheels of the Enigma machine that the bronze Godess dealt with and there's no way but no way in which this could have been employed against the Purple machine, against the navy machine and certainly against the Type of hand ciphers used by the Japanese military.

.....were transmission of intercept material and other classified information within the United States at that time permitted the material to be mailed in US mails with registered registered mail. No problem about it. The tapes we got from ~~Mobern~~ Mauborgne came in by registered mail. If a Signal Corps officer was making a trip across, it usually took longer for us to get the stuff by courier than it did by the registered mail so it was a practical thing. To sort of back this up to go into related activity one of the things we used to do was to send out code tables for the MI10 -- code cipher tables for superenciphering the military intelligence code number 9 and later 10 which replaced 9 -- and periodically, I don't remember whether it was a month or

three months we sent out a new set of tables. The rules were that within the continental limits of the US these cipher tables could be ~~well~~ wrapped; they were SECRET. SECRET military could be wrapped, ~~and in~~ then one wrapper which was sealed with wax seals and then put in an extra wrapper, both the inner and the outer having the proper address on it, the inner one being marked with the classification of the material contained and these were general rules which were applied and I've sent many a cipher tables to within the U.S. under those circumstances. Now when it went outside the US, ~~you were~~ it was not permitted to use registered mail but the G2 courier system (or State Department) courier system was used depending on which was making the next trip, so the rules within the US which applied to the handling of classified information included the way~~s~~ that we dealt with intercept material.

DoS

Valaki Q: I wanted to ask about cryptanalysis as ~~the~~ a cottage industry. ~~How~~ From what I saw of little memos here and there? that went into it, It seems that Friedman in the 30s

was sending out copies to different people to try to solve. Were these people on contract? _____

_____

in the Riverbank Lab.

A: Could you describe the traffic a little better?

Q: I can't. I just have a covering memo saying we're sending you a few messages or something like that and I don't remember what they were, specifically.

A: No Maam. We never would have sent any ~~mild~~ live traffic out that way. It would have been unheard of and I don't think Friedman would have ever done it and I don't think he would have ever been permitted to do it if he'd wanted to. I think there must be some misunderstanding in the context of the cover letter as to what type of material was being enclosed and it occurs to me that there were a great number of things that we dealt with the bulk of which was in analyzing systems submitted for war department consideration by private citizens throughout the country or private citizens throughout the world. We ~~have~~ had, I think

a couple by Englishmen and foreigners and Friedman used this material and the situation to increase our cryptanalytic capability because he figured that we took all ~~the~~ these, quote nut systems" submitted by nuts there would be some pretty good ones just by chance among them and (1) we might find a good principle and this is one way of ~~en~~countering them is to encourage people to send in their nut systems and (2) he ~~wrote~~ rigged operations so that the material~~s~~ submitted was prepared in such a form that he could incorporate it in his training program and I used to enjoy these nut systems when they'd come in because it was a great big puzzle and we'd solve them and send back well he'd ~~rate~~ rigged it this way for example. That we had a certain number of messages all in the same key, and then we had a certain number of messages in different key~~s~~ ~~was the same~~ and the number of messages in different key was the same text you see using different keys and the number of messages in the same key were different text so that he had a sort of a cross cut on the thing and it was almost impossible for some~~one~~body to invent a system with a you know proper sophistication in cryptography that

we couldn't solve ~~by~~ just more or less by inspection and I used to get a lot of fun out of doing these things. I have a feeling that the messages referred to in these cover memorandums are the solutions that we sent back to the people who submitted the systems to prove that their system was no good and I'll bet that's what it is but there never have been any ~~large~~ live COMINT type of traffic sent out on a contract basis. People would have been brought in, yes, to work on it. Reserve officers like Captain Gerand who was a ~~really an~~ relay engineer for Bell Telephone Company would have ~~Bob~~ brought in advisor and Mendelsohn to help out on the German problem but never would that live traffic have gone out so I must admit that there is something different here. hmm..

Valaki Q: The point ~~Bob and~~ I remember is that ~~we~~ I know where it is is here and I'll fish it out ... it was a letter to Childs in the 30s

A: Oh! Oh! Now this could be something else. Another thing we were interested in, and Friedman was particularly interested in this was historical examples of where

ciphers was used, for example, Benjamin Franklin with his ~~little~~ own code clerk and there's a whole body of material in the Library of Congress and there is any number of messages from. The code system that was used by the Lost Dutchman mine right across to the shorthand manuscripts about the ~~behaving~~ beheading of Mary Queen of Scots and Friedman and his cohorts like Childs got a great kick out of dealing with these historical and otherwise exciting examples and I have a feeling that that is the kind of thing that he would have sent to Childs but he would never have sent the material to Childs and I'll bet you Childs will tell that if he had Childs would have sent it right back because they were just too sophisticated in dealing with the secrecy requirements of this problem to have been so loose, and it would have been a terrible example to set for this rest of us anyhow. I would lay that one aside and say there's nothing significant in this. ~~It~~ This is of sort of incidental cryptanalytic interest, not having anything to do with the primary mission of the SIS, I'm sure of that. That's the way I'll answer your

Valaki Q: Could I ask about setbacks in the development of the agency, and this is on two counts. One is bureaucratic, just to put it in one pile, and the other is technical and ~~the first one thoroughly be professionally~~ the big question that you asked earlier, which is the ~~a big~~ milestone in the development.

A: Oh setbacks? Look it's always an uphill drag. Most of the set backs were monetary. As long as we had our salaries paid and we had problems to work on we got along. Remember there were only four or five of us. We had a nice vault which was secure. Our security problems were solved by locking the doors at night when we left. We didn't even have to put the material in the file cabinet. I remember leaving my worksheets out on the table and never having to worry about them. I just barred the windows and locked the door and went home. So there were no major security problems except keeping our mouths shut in dealing with the curious questions that friends and neighbors would ask about our occupational efforts. That was probably the biggest security problem that we had. Now

DOCID: 4223202

we did run short of stationery and supplies and things like that but we solved that problem by just going down to the dime store and buying five pencils for a nickel and I ~~probably~~ brought in ruled pads and old school pads because there wasn't enough paper in the, we'd run out of funds at the end of the fiscal year. Another problem we had was we had to take a months' leave without pay because funds ~~run~~ ran out I think, ~~1933~~ 1932 or 33 and I had a wonderful time down in Southwest Virginia in the month of May because we just closed up our apartment and went down there and lived on the farm, lived free for a month so it didn't bother us. Our problems, administrative problems, as reflected by my observation of what was going on around me, I don't know what the Chief Signal Officer was involved with but the problems within the organization -- there was more to do than we could get done and it didn't make any difference, if we didn't have the supplies to do this problem, we would work on another problem ~~but~~ that we had the things to deal with and we were learning in those days, so there was no urgency. We didn't have to meet deadlines

and there was no administrative inhibitions at that time. The only thing came up is we'd sort of ~~had~~ been promised raises and these didn't materialize and there was a little bit of unrest among some of the members. I remember looking down at the Civil Service and I found a new job down there. It was in P2. I was a ~~in~~ P1 in those days and so I made some noises about it. Not in the sense of trying to get more money but in the sense of changing careers and going to a job that paid more because I didn't put it in the context that if you don't give me a raise I'll quit. I put it in the context here is this raise, I'm going to take it. Abe and Kully I think had each his own personal opportunity but none of these other jobs materialized. I guess other people got them. We didn't begin having administrative problems until the, I guess after the war we had our ~~a~~ real one~~s~~. The climate in which we operated was ~~a~~ very favorable monetary-wise for us. We of course we didn't have money enough to get the IBM machines right off the bat but once we began reading traffic, Japanese

translations ~~xxxxxxx~~ which that bought us a lot of administrative relief and

Mauborgne
~~Mobern~~ and the other Chief Signal Officers were so proud of what we were doing

because it was getting them attention up in the office of the Secretary of War

and at presidential levels later on that if they felt we needed anything they made

sure we got it so we didn't have have much of a strive like we hear about

today and actually among us in this room I think there's more well pretty

well off. I think we got some good buildings. I think we got reasonably

good administration. I think we got reasonably good direction~~s~~from the front

office. There are good ones. There are better ones ~~than~~ and there are worse ones.

I think the administration of NSA is well above average of what I've seen in

other agencies. (Well CIA I found different and here I'll be a little critical

not of NSA but of the system under which we operate with NSA members. In CIA

CIA

there is no division ~~of~~ in military and civilian~~s~~ and the life of the civilian is

much more pleasant in CIA than it is where you have the civilian of course)

DOCID: 4223202

must give in to the military requirements and military personnel in the installation which is military in nature like this so really we had it pretty good. Is that what you wanted to hear? That's the way I remember it.

End of Tape 3, Side 1

Tape 3, Side 2

Q: Somewhere about perhaps in the 40s the Civil Service Commission no longer was

Valaki

providing people to the register, to the cryptologic effort, and could you tell

me how that came about?

A: Cause the system fell down. It was too clumsy and also the old rules the ~~old~~

bureaucratic rules as exemplified in the Civil Service Registers just didn't

work for the wartime ~~equipment~~ recruitment programs. So All the rules went out the window

we went out and picked them and hired them and we paid them and we didn't pay too much attention

to the qualifications and we got them in tested them and then if they didn't

suit us we sent them to China.

Valaki

Q: Oh are you talking about the military?

A: I'm talking about everybody. (laughter) OK we sent them to Siberia. We found

another assignment for them or we just let them go or we made it so unhappy for

them. We found a lot of patriots though. Certainly made the right kind of

sounds and sound like they had the right kind of qualifications and we made a lot of mistakes

but essentially when we found a good person they would up making the proper

contribution. A trivial ~~True to~~ example, somebody in someplace got the bright idea that people who were proficient at the game of chess might make good cryptanalysts. We had a chess player and I'll swear to God he wound ~~would~~ up on the ~~Staff~~ Judge Advocate's General's staff and that was the China we sent him to. He wasn't worth a hoot. The best source of people we had though was from the Signal School at Fort Monmouth and these were military people because General Reeder who had been with us as our boss, second commander in our War Planning and Training Division before he was sent up to Fort Monmouth, was in charge of the Signal School so he took the IQ scores of all the people who went through the school and he made out the top block and he sent them to Arlington Hall Station and we got that's where we got people like Dale Marston and Bill Bundy. McGeorge Bundy was slated to come down here except he got sidetracked to go somewhere else which is pretty well known when you read his books, Walt Freed was a terrific man in terms of intelligence, John Siemen was another one that I remember, Walt Jacobs whom you all know came in

a little differently but when they came through from the Signal School ~~in~~ at Fort Monmouth, down here to Warrenton, at the intercept station where we phased them in and then brought them down to Arlington Hall Station after their clearances had been received, we knew they had to be good so, I think Art Levenson came in that way. You just name the, Kirby came in that way, ~~Wally~~ Ollie Kirby. Now that was the military recruitment. The others we didn't have a Bill Reeder out there in the front line so we had to let them in droves and we had some of the strangest things like ~~the~~ gals from North Carolina who had never worn shoes even. They'd come to Washington and the recruiters had gone out and picked them up and Lord there was a we had a terrible time screening these people out and I think this was the result of throwing the old Congress Civil Service System because it was so intolerable. We had to get closer to people quicker.

Q: How about the college recruitment program? Did you have one then?

A: We had all sorts of recruiting programs. I don't think they ever got identified as one particular thing. If somebody knew somebody who was possibly a good candidate for our kind of work why contact was immediately made with them.

Q: Valaki Could we go back to the late 30s at the time when people were still being brought in from the Civil Service register as mathematicians or ... clerks? How were the linguists brought in when it came time to start publishing end product.

A: In a variety of ways. They had linguist~~s~~ roles, rosters, set up by Civil Service for the G2 (and the State Department) with language people, so there were junior translators I suppose but there were language rosters. We ~~fed~~ ? them ~~back.~~ ? The trouble was to find people with a foreign language could be hired because of security clearance reasons. These security clearance rules were pretty arbitrary in those days. They weren't very well thought out. ~~They~~ You had to be sort of a second generation American if you were that then you could be cleared. If you were first generation you might be cleared but if you weren't born in America you couldn't be cleared. These were the broad categories. People from bigger centers, population centers like New York, Philadelphia, and Baltimore were looked at with little more carefully than people from ~~Oak~~ Rose hill,

DoS

Virginia. I didn't get formally investigated and cleared until the war was half over. It's amusing what happened -- at a staff meeting, General Corderman was the head of the Army Security Agency and we were talking about security clearances and Jim Slack Col Slack who was his executive officer made the announcement at the meeting and Corderman says, ~~said~~ "I don't want anybody in this building who hasn't been formally cleared." and he says that's the way it is isn't Jim and Jim says "No Sir". He said "What do you mean" He says "Well you got a guy here at the table who isn't, hasn't been formally cleared." Corderman looked around and said "Who is it?" He says "Frank Rowlett". Corderman says "Frank haven't you been cleared?" You see I had come in ~~early~~ in '30 and I was a country boy from Rosehill, Virginia and everybody looked at me and said we won't waste our time with this bird which was stupid so there were a few of us who sort of slipped through and didn't get cleared but by the end of the war everybody had had some sort of formal lookat and I'm amused everytime I think

about this that the consternation that was on Corderman's face until he found out who it was and then he said "Well we better clear him anyhow". That was his sort of way of getting out of the situation he had developed by his sort of pontific profession, I'm sorry, go ahead. That's about all I can give you on that. It was chaotic.

Valaki Q: Did you ever ~~acknowledge~~ know ~~(of Driscoll)~~ Mrs. Driscoll (?)?

A: Not very well.

Q: Quite interesting if you heard about the story of the system that possibly she invented in Friedman's _____ and then they never spoke ~~throughout~~ -- ... Mrs. Driscoll wouldn't speak to Friedman again.

A: May I ask a question? What was the system?

Q: I have no idea.

A: OK I'll tell you what it was then. Mrs. Driscoll was the best of the navy cryptanalysts. She was the high priestess I guess of the cryptologic cultists over there and when ~~Hebron~~ Hebern accepted the contract to build a cipher machine for the navy the navy had good foresight in going after a commercially built device because it took a little more than the sophistication of the navy yard which was

DOCID: 4223202

very good at building shipborne equipment but and a radio laboratory of course is very good at radio but the sort of electromechanical components of ~~the~~ a cipher machine was something that just hadn't been, there wasn't any background. There wasn't any experience in that field and it took somebody that was pretty much of a mechanical genius to put something like that together in those days and ~~Hebron~~ Hebern was that type of a guy and so he had gotten the concept of this cipher machine and talked ~~to~~ me into giving him a contract and so he produced the first model and in his discussions with the navy he met _____ Agnes _____ Driscoll and he was so impressed with her ability and I think also a very ~~troubled~~ clever man that he proselytized Mrs. Driscoll and took her on as a techical consultant in his work with~~in~~ him his contract. I don't think this would be tolerated today in terms of conflict of interest but in those days it made no difference. So she went to work for Heb~~ron~~ern and then they produced the device and sent it back to the navy and the navy tested it and they took Mrs. Driscoll's word evidently that

it was sound cryptographically and didn't work very hard and some SOB over at the navy decided that that wasn't good enough for him so let's get the army. I think what they were trying to do really was to get the army in on the contract more than it was to test out the device so they talked to Friedman and the Signal Corps about it. They talked to the Signal Corps and then talked to Friedman. Friedman talked them into giving him a challenge problem. I think there were 10 messages and you can read about what Friedman did ~~with~~ to the Heb~~ron~~ern machine in ~~his~~ the little black book that we had in here yesterday. Subsequently the navy decided that they wouldn't go after the Heb~~ron~~ern machine and got some more funds and looked elsewhere for a device. Well since the contract was not followed through on Heb~~ron~~ern couldn't afford to keep Aggie on his rolls so she became jobless and she came back and went to work for the navy and I think that is probably the thing you refer to and I think these are the substantial circumstances whether she ~~natted at~~ got mad with him for something else or not but this is

I think ~~what~~ where Friedman ~~to~~ did make life miserable for Mrs. Driscoll but not in the sense of meanness or ~~viciousness~~ maliciousness but in the sense of honest evaluation of the system which was proposed for government al use and ultimately might have been adopted ~~for~~ by the army. I think Friedman is completely clean of any malicious act in this context and you can't blame Mrs. Driscoll because she, ~~was~~ as the high priestess that thought the navy had a position of pre-eminence and she couldn't have anything but hurt feelings as a result of what had happened. Now this is an answer to your question. The part that you raised later but going back, did I know Mrs. Driscoll? I met her a few times. After we had solved the Red machine and had finally broken the news to the navy that we had recovered it so -- there was always a certain amount of uncertainty about what you ~~do~~ did after you ~~have made your~~ had a major breakthrough, you see. Who do you tell about it? Because certainly you've got to ~~have~~ tell somebody because if you're going to get the information from the, ~~and the~~ any benefit from the information you're producing the people in G2

DOCID: 4223202

have to know about it and then after that had been decided, and how you're going to get the information over there, then you had to decide, did or did you not tell the navy and how much did you tell the navy or not? Well Friedman I think was absolutely right on this and I don't think he ~~made~~ met any opposition from the Signal Corps although there was a great deal of discussion about the merits of it under each circumstance but the idea was to have no secrets from the technical people in the navy and the people in charge of the technical operation but limit the cryptanalytic procedures and techniques to this group. Don't generally publish them and talk about them outside the groups and this of course obtained in the army ~~sort of~~ so there were ~~amologous~~ homologous situations in the two services regarding the release of information. I think we were more we operated with ~~more~~ greater liberty in releasing things to the navy than the navy group could to us because there were certain, I think, old wounds over in the navy -- they ~~who~~ didn't trust some people in the army and I think one of the things they distressed them is that Friedman had gotten

quite a bit of publicity you see. His pictures had been in the newspapers and they did the usual thing that people do when they are not certain. They said don't tell him ~~every~~any thing. They had nothing against Friedman that was derogatory. They just didn't like the way he was doing things and they didn't understand what had happened so they they I think were cautious. But now going back to Mrs. Driscoll, after the REd machine was solved and we had talked to the navy there was much discussion between Friedman and Wenger and one of the things, Wenger wanted Aggie to come over and have the thing explained to her by the people who'd done it. That is the solution of the Red machine. So we arranged a meeting one afternoon and Mrs. Driscoll and a couple of junior navy officers who were students over there came over with her and I'll be very specific. This was some months after the initial breakthrough had taken place and we had come to the point of where we could predict in advance the keys that were being used by the Japanese so instead of solving each days' traffic and

recovering the keys for each each period's traffic we simply went to the book and looked it up and plugged in the machine because we'd solved it for the whole year you see. That's a nice trick. I can't remember many cases where we were able to do this and so I was to explain to Mrs. Driscoll exactly how we had achieved this forecast of the keys. She came and sat down and she didn't, after saying ~~say~~ "~~Nice~~ Glad to meet you", She just sat and she didn't say a thing and Friedman said "Well, Mr. Rowlett would you please explain to Mrs. Driscoll just how you did this." So I took my books and my worksheets and I sat down close to her and I explained and she listened and she didn't ask ~~any~~ a questions and when I got through I kinda looked at her you know waiting for her [to ask questions] and she didn't and I said "Well, any questions" and she shook her head. Then she said "Thank you very much" and got up and left and I never did see her anymore. I never did meet Aggie Driscoll after that. She was a quiet person I guess but now wait a minute. I'll take back. I did see her later because

when the consolidation took place there were several occasions when I did talk to Mrs. Driscoll but never -- at that time though the world had passed her by. She was a most unhappy person. But I don't think and this is my evaluation. I don't think Mrs. Driscoll could keep up with the progress that had been achieved both within the army and the other parts of the navy because I think she just got passed by particularly when Raven and that crew came in and of course she got along very well with Commander ~~Cipher~~ Safford. They were old friends and then when the collaboration with the British started I think she got left way down the technical ~~level~~ role and that's enough about Mrs. Driscoll.

Q: How old was she at that time? in the 30s?

A: (laugh) I'll I'll try to think. She must have been about 15 years older than I. I'd say she was born about 1900,1895.

Q: She'd gone to Riverbank.

(She had?) (VV)

(Yes)

(I didn't know that)(VV)

(That's one of the things I found out down at the Archives.)(HS)

(Did she study under Friedman?)

(I don't know who she studied under but she ... There was correspondence between

Fabyan and _____ who was head of OP20G at the time and he sent he sent her to Riverbank. Th~~e~~ere were two guys. Also Wilson, later Admiral Wilson, had gone through Riverbank also along with another ~~we~~ guy which you never hear of never hear of him again) (HS)

A: Isn't that remarkable?

Q: Yes.

A: I didn't know that.

Q: And then as a matter of fact I think Fabyan's comment was that she was doing very well.

A: Well now look she was pretty good in terms of the progress of that day. She just didn't have the background and education and the kind of things that were needed to get in this new field of machine cipher analysis. I think she was well over her head in the work ~~of~~ with Heb~~ren~~ern

Q: Yeah, these are different things, different way different time period.

A: She was very good. ~~Problem~~ Probably in her early days ~~just~~ and then probably just got too much for her. One mystery.

I've been thinking about it in connection with my own thoughts about the development of our success on the Japanese ~~traffic.~~ ciphers. When we when Friedman was talking with Wenger and describing to him our early attempts ~~to~~ at solving the Red machine, Wenger told Friedman about a navy machine but he didn't describe it in detail and the recollection I have is that this ~~is~~ was a machine which had been solved by Mrs. Driscoll working with some naval officer whose name I've forgotten right now but when Friedman began to press Wenger for the details of how the machine operated hoping it might help us in our work on the Red machine Wenger found a place where he stopped and he didn't go beyond the point. I have yet to see the details of that solution. I know that it had a rotor somewhat similar to a half Heb~~ron~~ern type of rotor similar to what the Purple had. Not the Purple but the Red machine had which produced a vigenère square of one alphabet sliding against itself either forward or backwards and it had two components. In the navy machine I think they used the ~~conna.~~ Kana. I can't remember whether it was

48 or 50 or 47 or what. I know there was a 47-point interrupter wheel on the thing which controlled the movement~~s~~ advancing or well let's call it advancing the forward or backward movement of the two commutators ~~either~~ each of which provided a cryptographic substitution device for the two components which the ~~conna~~ Kana alphabet was divided and structurally it was similar to the Red machine but we never got from Wenger, before the solution of the Red machine, any of the details about this and I have often wondered why he didn't level with Friedman as Friedman was leveling with him. After the solution of the Red machine had been achieved and we were more confused by the _____, Kully and I, we were the ones that read the first message in the Red machine. We were more confused by the dope that Friedman had relayed to us from Wenger than we were helped ~~so~~ 'cause we wasted a lot of time. If we'd just gone ahead and looked for what we could find instead of looking for the things that Wenger had told Friedman and Friedman had tried to explain to us because I don't think Wenger

had I don't think Wenger understood what he was talking about really because he never was much much of a technical expert on these things. He could use the words but it was quite an accident if he described the thing accurately. At least that was my feeling about it, so Aggie evidently, Mrs. Driscoll, Aggie evidently had achieved the solution of this navy machine. At least it was attributed to her, as I think back about it I just am real puzzled by the whole circumstance and about the only sensible thing I can conclude is that the navy had had a second story operation for the some how or other through ~~its spinach~~ espionage activities recovered this machine and I'm not so sure that the thing was done cryptanalytically. It's we found out we had to do in the army with the Red machine and the Purple machine and the J19 and other things.

(I think they pinched some stuff from New York)(HS)

Well....

FBI (working in conjunction with the FBI and the New York City police department)

Well and then there was another one ~~the smuggling operation~~ of this was..... I met him after (I went to work for CIA) and there was ~~as~~ a locksmith that used to work for navy and he was doing some

CIA

contract work for us, training people in the art of picking locks. You recording this? And he .....

Q: Valaki In the early 30s were you ever aware of the ciphers used by any of the other U.S. agencies or is that going to put you over with the army _____ or

DoS

A: (the navy or State Department? Panama Canal Department?)

Q: Oh, I didn't know about that one.

A: Yeah. A little bit. (We did not see codebooks used by the State Department.

DoS

We knew from Friedman who had a very good relationship with ~~the~~ David Salmon, _____ who was the head of the cryptographic section of State Department. I forget his exact title but he was in charge of the compilation of State Department codes and he relied on Friedman's advice and judgment a great deal except that he wasn't competent to really appreciate what Friedman was telling him so there was some knowledge of what State Department was using.) Our knowledge of naval codes was general. We never saw or used or became involved in the systems used by the U.S. Navy.

Q: Valaki Excuse me. When you say the codes, do you mean ~~generatically.~~ generically?

A: I mean codes, young lady. Precise sense because nobody used cipher machines in those days. They hadn't reached the state of perfection which made them reliable enough for code room use and in that regard the Japanese got a little bit ahead of us because they were out with the Red machine, using it practically before the Germans were successful in applying the Enigma to their current messages and the U.S. Navy and Army (and the State Department) and the UK all had not moved up to the point in cipher machine development where they had a machine that could be used for enciphering and deciphering messages. Simple enough for a coderoom operator to use and reliable enough to do the job so the Japanese were one up on us in the practical application of the machines although the machine was cryptographically a dog. It wasn't very good as any modern cryptanalyst would tell you about the Red machine but it was pretty hot stuff to the Japanese in those days and of course the cryptanalytic capabilities of the rest of the world just hadn't reached the point where ~~it~~ they could deal with

even a simple thing like the Red machine so we were generally acquainted with what they were using but we didn't have the codebooks in hand. We knew how they worked but we didn't know the details. We knew the general ~~contents.~~ concept. There was no reason really for us in our capacity as cryptanalysts and sort of developing a cryptography of the war department because we were at that time compiling the codes and I mean literally codes, the war department staff codes, the war department confidential code, the MI10s and the division field codes and the army field codes which were on the code production program. We were busy with that and we didn't have time to sort of go into other areas.

Q: Valaki So the rest of the world ... ~~was a code?~~ were the codes. Now from your perspective now which country would you say ~~is~~ was the most sophisticated after Japan. Apparently Japan was then was the most sophisticated and led the world in ... machines.

A: No Maam. Japan was not the most sophisticated and I would say somewhere down about the middle of the pile. I believe the people who ~~have~~ had probably the best sense of cryptographic security in those days and I'm including the U.S., State

DOS

Department and the army and the navy ~~and the~~ in this comparison. I'm not excluding us. I think the British had the best concept of cryptographic security. Now let me explain that a little bit. People like John Tiltman and Travis and the graduates of OB40, Admiral Hall's outfit, had been involved in the preparation of British naval and diplomatic and military ciphers and John Tiltman as you well know is has been an expert in this field for many years. They used ~~two~~ good sized code-books with additives or superenciphered with something similar to.... the additive ~~printo~~ principle were applied in their own ways, and they had also a realization of the amount of work which would be involved in the breaking of the system so that they didn't overload the system and thereby destroy its security by misuse or overuse and they had the proper concept of for key~~chain~~ change states? and other things. Now they maybe their security wasn't the best in the world but they sure had the greatest sophistication in dealing with ciphers because it was a combination of practicable ciphers. The pragmatic, pragmatic aspects as well as theoretic.

145A TWICE

Now these I know about and I can say in the ones that I understood that the British in my opinion were at the top. I don't know what the Russians were using but from what I have learned since I think the British were well above the Russians in sophistication. The well just an aside for a minute one of the I believe it was an ex-Russian national who had been adopted by GCHQ was really the fellow that introduced the concept of the one time pad. I forget his name but somehow or other the name Federlein (?) comes to the front. I don't know whether that was his name or not. I do know that the Russians knew about the one time pads and so did the Germans. They called it the Wubburn W U B B U R N but the generic term applied to short additivewhich later on extended to a bigger additive. Now the Germans were pretty sophisticated as we found out from World War II systems. The military field systems were just about the same as the ADFGVX used with more sophistication and taking into account useage time factors, amount of usage and how much traffic might be sent.

Probably better than the German sophistication in WWI but the grading was sort of narrow. There's not much difference between the WWII sophistication and the Germans so far as the field ciphers were concerned, military field ciphers and WWI. I think the same is probably true of the navy, German navy, so far as codes were concerned but when we get in the active situation of WWII we find that the greatest evidence of German sophistication was ~~is~~ their use of the ENIGMA. Now the German Enigma was a very reliable device mechanically. Its greatest fault was ~~is~~ the fact that it ~~you~~ used a "lamp ~~lank~~ bank" and you had to read the lamps ~~blanks~~ and record the message whereas the Japanese Red machine ~~was~~ had a printer attachment so it automatically printed the text. In that sense the Germans were a little bit behind the Japanese in their practical exemplification of their cipher devices. The security of the German Enigma though was greater than the the Red, much greater, and its usage, the Enigma usage, was much more secure than the Japanese usage of the Purple machine and the navy machine. The Japanese didn't quite

understand the usage ~~mode~~ load factor, how much traffic you can send and they didn't allow for that as much as the Germans did in their change of keys. Also the number of wheels and the in variability of the digmawheels ? ~~for~~ added security factors which the Japanese Purple machine and its related navy machine didn't provide. French, Spanish, Italian somewhere down below the British and the German. French I think were not as, well, they were about on an equal with the U.S. The difference between the French and the US the Americans yak more and send more traffic and send more traffic and as a result the use factor weakened our codes. Also our physical security in the understanding of how to deal with the physical security of codes was pretty immature on the side of the Americans and I'm sure anybody who wanted to copy (an American code book State Department type could.) I know definitely from many sources of information many - I'm talking about, I can think of four different sources of information now that confirms the compromise of the strip cipher (as used by the State Department) and so

DOS

DOS

I would say our sophistication falls we had some doggone good ideas on the drawing board as we used our codes and I'm talking about now the State Department which was very poor in its physical security and whose codes books were antediluvian in date, navy which hadn't yet found the cipher machine it wanted but the amount of traffic the navy sent was far below the use factor which created a weakness in the system ~~unable~~ that it enabled it to be solved by cryptanalysis. I don't know what about physical security measures used by the navy but I never found any evidence that a navy cipher had been violated ~~in its~~ -- that is, a ship ~~to~~ or shore installation. I don't know about naval attaches. I don't know whether they had much traffic or not. U.S. military ciphers I know were violated. I know that the Fellers codebook was stolen by the Italians. I mean the codebook involving the Fellers incident that I'~~ve~~ talked about earlier was stolen by the Italians. I found this out after the war. Circumstances are good TV script. The strip cipher was also violated and I know the Japanese got the details of the strip

cipher from Defense who had traded cryptographic information with the Germans and the Italians and we received the strip cipher as part of that and we used to when we were reading the Japanese military attache cipher we'd concentrate on the traffic from Finland because in that traffic the military attache would send the recoveries that the Finns had made of the American strip systems back. Had to send them by radio you see encoded and we intercepted them and I might explain there was no ~~it was dole~~ surface, sea or ~~see our~~ other communications possible between Finland and Japan at that time because so very exposed? to them and submarine warfare situation was such that they couldn't have vessels traveling between Europe and Japan so they were forced to go on the radio circuits in code messages and send this intelligence information. We were reading it cold and Captain Jim Molk who was in our CSEC organization, I used to call him up and ask him to come over and he'd go down and look at the partial recoveries in the Japanese military attache system then go to the State Department and go through their

vaults until he matched up the recoveries with the actual strips that were in use and then bring back the set of strips and we'd crib them into the military attache messages and ~~were published~~ recover more MA key. The fact that they were ~~encrypt~~ encribbing, we ~~clued~~ cribbed in our own (laughter) (The same ~~doggone film~~ dumb old crib) (VV)

I mean this is a fantastic story. Nobody would believe it and I'm sure that the only reason you believe it is because you think I'm a truthful man but we did that. But it's fantastic that such a thing was possible I think in the time-frame of sophistication of ~~WWKK~~ II cryptography so I would say while we had ideas on the drawing board our sophistication from the standpoint of what we were doing was deplorable yes deplorable. Friedman knew this. We knew this, Abe, Kully and I. ~~Mobern~~ Mauborgne knew it. Akin knew it and we were working awfully hard to change the situation but the massive nature of the war department, the time lag for procurement and funding and other things in the manufacture of a modern device, the state of the art just wasn't there and of course we didn't have ~~a~~ the crash

capabilities for protection ~~and it~~ that suddently came into being with the outbreak of the war.

H5 Q: Can I ask you a question on the Enigma while we're still here?

A: Yes Sir.

Q: We have some documentation that shows that between 1923 and 26 reports came back to Friedman about the usage of the German commercial Enigma and Friedman put in an order for two of them and due to one thing or another he didn't get ~~them~~ two. ~~He didn't get the two~~, he finally got one in 1930. Do you recall any working on any any ~~of~~ on the commercial Enigma?

A: I sure do. After we'd finished the work on the Swedish machine, the strip cipher device and other things and had gone through the repeated Friedman's exercise with considerable help from him on the Heb~~ron~~ern machine he gave us the Enigma to study. We did not have a bunch of problems ~~with~~ in it. We had the machine and the machine itself to study and I think what Friedman wanted to do was to set up a problem similar to the one that he had used in proving the challenge that

the navy ~~had~~ gave him. He wanted a similar kind of a problem for us to work on but we had already been in training so long and I think he kind ~~a~~ of felt that maybe until we had some actual usage of this commercial Enigma which we hadn't encountered at that point in time ~~into~~ many of the intercepts that it would be better to study it and not waste our time in a simulated problem which could be anything but real, so while it might have helped us ~~to~~ understand the Enigma he just never did get around to giving us an assignment involving messages enciphered by this commercial Enigma and I I think he was right because I don't think ~~we'd~~ it would have done as much good, probably wasted a lot of time. I don't think we'd have learned anything we didn't learn later on anyhow.

End of Tape 3, Side 2

'ape 4, Side 1

.....that is mishandled through some mistake and through some failure of the rules and the regulations that apply to it and there is a bit of a mess to clean up and everybody goes around and reexamines the old rules and makes the new set of rules. Now this ~~step~~ doesn't mean that the new set of rules are any better, it just means that they are different and that they are based on that situation which resulted in a mistake. Now I have seen any number of cases where the decision to improve the ways and means of handling information has been taken and actually we had to go back to the old rule? (1) Because the new rules corrected most unusual and rare set of circumstances and (2) that the people who were dealing with these things had a hard time understanding the new rules and changing their practices so it was better to limp along with the old rules which maybe wouldn't satisfy all the special circumstances but which were designed to satisfy most of the circumstances then it was to introduce new

rules which took care of all the exigencies that might arise and this has happened many many times in some of these fancy systems that we put into effect in the cold war situation in Berlin I think where you had the crash messages going from the source to everybody in Washington without any possibility of them being analyzed by mature intelligence officers created more confusion than they created good situations.

Probably the best example of what I'm talking about is found in the scurrying around Washington which took place looking for that winds ~~Winns~~ message. Actually there was no need for the Winds ~~Winns~~ message. It didn't mean a thing if they'd sent it. I don't think they sent it. Stafford said he saw it but he never could prove it. I looked for it. I never saw it. I think I would have seen it if it had been there because I knew what I was looking for. Friedman looked awful hard for it but he was a little bit remote from the situation and he couldn't find it and Col Sadler and Bob Schukraft Shucraft and all of us helped each other and we scurried all around looking for that thing and we never did find it and later on

when the TACOM team went to Japan, Erskine and his folks discussed this with the Japanese and I believe their report substantially indicates that the military didn't trust the diplomatic Japanese diplomatic corps enough to tell them that the strike was being made so the diplomatic corps was never alerted to the point of where they could have sent the Winds message which would have meant what everybody thought it meant. Now as a result of that a lot of soul searching was done in the ~~middle of~~ military circles ~~of~~ in Washington including the Army and the Navy and probably up at the White House where they felt this pain probably as much as anybody else and certain rules for handling the magic summary and other material which was being distributed at that time were put into effect. These were much well they were designed to make better distribution but nobody could have anticipated the Winds message and what would have well what resulted from the fact that ~~the~~ we didn't receive the message but it was presumed that we had received it and the action that was taken was based on the probability that

there would be another critical message like that and while this probability seemed high at the time actually the normal system seemed to work quite adequately without this special gimmicks that were introduced to take care of the potential second Winds type of message.

Q: Now your question is specifically what good would thorough research and analysis of the commercial Enigma would have benefited us in terms of dealing with German military and naval and air traffic as exemplified by German usage of the Enigma machine under wartime circumstances?

A: And the answer is we would have been aware of the general principles underlying the usages of the three services, air, land and sea in Germany but practically each service in Germany, the Air Force had one set of wheels and one system of rules for using the Enigma and it was a different Enigma from that which was used by which was exemplified by the commercial model we received. The main difference is that the military Enigma had a plugboard between the endplate and the keyboard so that you could change your connections between the keyboard

and the enciphering component as a part of the period key change and in some cases this ~~will~~ can change several times a day, something like every six hours or so. Now our study of the commercial Enigma if we'd gone into deep research probably would have been a waste of time when we got around to dealing with the actual Enigmas used in the let's say by the German army because it was something less than the machine used by the German Army and the simple principles that we could have used for solving the commercial Enigma would have been much less powerful than would have been required to produce the answers with the military type of Enigma. Now as I recollect and I believe I'm correct in this, the German navy had one more wheel in their basket than the German Air Force and the German Army and consequently their machine would have been more difficult to deal with the German Navy machine that was would have been more difficult to deal with so I think in looking back that the commercial Enigma gave us an understanding of the underlying principle which is ~~important~~ employed namely rotors with the umkervaltz

~~with~~ the reflector and then the double use of the rotors because the input and output endplates were identical and it was the electrical wiring that enabled the double use of the wheel to be achieved in the Enigma and this didn't happen in the American version of the 134 series, the SIGCOM and the ECM, because we used the one way circuit. The British ~~type X~~ Type X did use the reflector, the umkervaltz principle and used Enigma circuitry.

Q: They were all three of a family though weren't they?

A: Yes, they were indeed of a family. The difference between the Enigma and the Heb~~ron~~ern which ~~of~~ of the two general classes, the Heb~~ron~~ern used a reversing switch so that it in effect when you went from the decipher mode into the encipher or vice versa you simply in effect turned, reversed the current ~~through~~ to the wheels. Now this is fine and electrically it has certain advantages because the resistance path through the wheels is shortened. Now when you send it down, the current down, through the wheels around through the reflector and back then you've got at least twice the resistance and since its a very variable thing and will vary with each

contact in the wheel in the endplate or the separater plates if they used separater plates between the wheel and the adjacent wheel but you get a factor in there which is pretty unpredictable and then with use the resistance becomes so great the machine doesn't function properly. This is probably the reason the Germans didn't have a printing mechanism on theirs because in the Enigma principle the current went through the circuit but through the wheels and returned from a reversing plate at the end and the connection between the keyboard and the lamp bank which was the recording component of the Enigma machine was affected by a sort of double kind of single ~~pull~~ -pole double-throw switch. The key in this type was a single ~~pull~~ -pole double-throw switch and so when you depressed the key to send the current through it was impossible for that light or ~~that~~ the indicator associated with ~~that~~ the key to be used because the circuit came out always at some other place. Now that's another distinction between the Heb~~ron~~ern type circuit because in the Heb~~ron~~ern type circuit a letter can represent itself. A plaintext letter can

represent itself in cipher text but in the Enigma circuit the plaintext letter can never be represented by the same character. Going back and a little bit more on the printing principle, it could be that the Germans tried printers. They had pictures of solenoid operated typewriters but I think the circuitry of the Enigma the resistance factor that I talked about earlier was they didn't resolve it. Now the British very interestingly had a printing mechanism on the Type X but the way they got around this resistance factor was principle that the Bell Telephone used in its relays and it had double contacts, bifurcation and they had double wires going through the Enigma wheels and double string of contacts so if the one failed the other one might carry the current through so it reduced the probability of a bad circuit or resistance contact by about oh by a reasonable factor something like 4 instead of 2 or 1.

Q: Were we able to read the British Type X?

A: There wasn't any point on working on it, was there?

Q: No, I'm just curious. The reason I asked that is all these three were of the

family. It must say something about US cryptanalysts. That they broke the German system but the Germans never broke us, or was the difference that great?

A: The German cryptanalysts were handicapped because they were too competitive. I think if you look in the history, the TICOM history, you'll find there was something like 7 or 8 different organizations all doing the cryptanalytic work on allied traffic. The trouble with these organizations is they were so anxious to get attention, the little bit of mail, the intelligence that they 173 all skimmed the cream off and they did the easy ones and nobody, none of them, were ever able to concentrate on the more important and more secure systems and bring~~ing~~ them under control. I don't think they could have with the sophistication in cryptanalysis and with the capability the computer capability that is available to the Germans I think the security factor of the ABA or the ECM would have been ~~xxxxxxxxxxx~~ far beyond their capabilities if they had all been together in one wad and worked on nothing else because the recovery of the wiring of

irratically step set of wheels is quite a complex problem that can be attested to by people over in CSEC and some of the other sections of prod or some of the sections in Prod. I don't think the Germans could have coped with this. I don't think they could have read the British Type X. I never saw any evidence that they did. I never saw any evidence that they had captured information about the Type X and if they had I'm sure that they would have done something about the Enigma because the British sophistication of the use of the cipher machines was pretty high for those days.

Q: Your question is is there any significance in the fact that the three major powers the ones with the greatest degree of sophistication in cryptography, is there any significance in the fact that they used rotor type machines and I'd say grossly the answer is yes and in detail here is what happened:

A: The first concept of an commutator look an electrical substitution of letters of plaintext by letters of cipher text using circuits came from a Swede whose name was _____ and who invented this concept along about the turn

of the century sometime in the early 1900. His idea was not a wheel but it was sliding strip of contacts, equally spaced contacts, which slid between two sort of end plates and these contacts were interconnected in a sort of a haphazard or random way so that as you slide this stick of contacts and of course there had to be 26 wires and 52 inputs and 52 outputs to provide for the all 26 could be enciphered at one time so you effected a new substitution simply by pushing your stick with the contacts further down the groove. This was the first concept. Now that was later turned into a wheel because you could by making the circular arrangement of the 26 contacts then you didn't have to have the 52 contacts for the endplates and also you could put the wheels in cascade and from this very simple idea of the Swede Mr. Arvid Damm Vaney, Hebern in America and Dr. Scherbius who was also known as Willi Korn Kohn I believe its WILLI KORN KOHN, The name of the man to whom the patents down the patents office were issued, took this concept and out of it came two different slightly different machines both using the

wheel. In the German version, the Dr. Scherbius version, I believe his name is spelled SCHERBIUS, The Enigma principle was used where you had the endplate with the set of 26 single ~~pull~~ -pole double-throw switches in ~~the~~ your keyboard and the ~~lamp~~ lamp bank together with the reflecting plate so that you ~~set~~ sent the circuit the substitution circuit through and it came back so you got a sort of double use of each wheel. With the Enigma version of this wafer-like commutator wheel if you will device. Now the Heb~~ron~~ern idea was instead of the double ~~pull~~ -pole double-throw switch arrangement in the reversing plate he used a simple gang switch ~~which~~ with 26 contacts 26 circuits from the, well, the 26 contacts into the first endplate went through and came out another 26 contacts and then to an indicating device like ~~the lamp~~ a lamp bank or a bunch of solenoids operating typewriter keyboards. Now the enciphering and deciphering mode in the Heb~~ron~~ern device had to be satisfied by a multiple switch which would in effect deal with the 26 circuits in and out in such a way that the endplates that the wheels were reversed. I

mean the circuits through the wheels were the paths through the wheels ~~were~~ was reversed so it just really flipped the indicating device and the contacts which you fed the enciphering contacts and the reading contacts. You ~~switched~~ flipped them from one end of the wheelbank to the other and that's the difference between the Heb~~ron~~ern and the Enigma roughly. Now we in America like ~~to~~ the reversing switch principle rather than the Enigma type because most of the work had been based on Heb~~ron~~ern's development of a cipher machine under ~~a~~ the navy contract we spoke about earlier and of course that concept ~~is~~ carried on and the Enigma itself is not too well understood and I think one of the things that instinctively turned the Americans against it was the fact that the Enigma did give a little bit of a clue as to what the plaintext was because a letter couldn't encipher itself so both the electrical characteristics and the lower resistance ~~to~~ thru the wheels coupled with the fact that there was this non-[illegible] encipherment, that is the letter couldn't represent itself, lead the Americans to prefer the Heb~~ron~~ern type of circuit.

Now why did these three of course the British, it seems to me like they picked up the Enigma circuit and they didn't weren't exposed to the Heb~~ron~~ern as much as the Americans were because of the navy contract and Friedman's analysis of ~~is~~ the navy device. They weren't aware of that and they weren't conditioned psychologically for this kind of approach so the Enigma looked pretty good to them and so they just went ahead and tried to improve it mechanically and electrically and produce the ~~Type X~~ Typex machine. Now the common strain that runs through these is this invention ~~that~~ of the Swedes which later on turned into a wheel, the commutator concept, and the state of the art kind of ~~lead~~ led to a situation like Newton and Leibnitz and the invention of calculus. It was time for this to happen and the state of the art had ~~lead~~ led the people who needed good cryptography to use that which seemed to be the best thing to them and that was the cipher wheel because the cipher wheel was much better than anything else that we saw. The Damm machine used a keyboard and an indicator device with the

~~electrical circuit~~ electrical circuitry and the mechanical control and that was very poor. I think we were projected into the He~~bron~~ern type well the use of the wheel type cipher machine because there just wasn't anything else available and I'm sure that's exactly what happened with the Germans and the British.

Talking about the security aspect of American systems, a little personal story about General ~~Mobern~~ Mauborgne I think you all might find interesting and ought to be somewhere put down in the history if you get an opportunity. I think its significant that when we revealed to ~~Mobern~~ Mauborgne the fact that we had been successful and we were able to produce translations, decodes and translations, of the Japanese Purple system after the 18 months that we'd been working on it and I spell this out because I want to set the context here correctly for what I'm going to say, I think it's significant when he saw this and was amazed that we had finally achieved this after 18 months work that his first thought was well now can somebody do this same thing to our systems which we are about to put into effect

and this was the question that he asked Friedman right then and there. It wasn't so much a praise for what we had done but he was immediately translating what he was looking at in terms of his problems and his responsibilit~~ies~~ and I think this was a very amazing trait that ~~Mobern~~ Mauborgne had and I think it ~~simplifies~~ exemplifies the philosophy of the Chief Signal Officer that we found in General J. O. ~~Mobern~~ Mauborgne.

Q: Specialists. Sometime ago ~~they~~ say in the 1950's even, '60s? _____.

Valaki:

~~Was~~ there was such a thing as a chief cryptologist who was a ~~for~~ Friedman and there were few senior cryptologists and all kinds of fancy terms ~~what kind of~~ _____ and apparently ~~and~~ now I may be reading into it, _____ this bunch of people ~~were~~ was responsible ~~for~~ (pause) was the ultimate authority, technical authority, for code and ~~c~~cipher and I should think both making & breaking the same.

But now now there is such a thing and when I tried to find out recently who was the chief- say who was the _____ number one cryptanalyst or cryptologist, ~~of this caliber~~ ~~they~~ there isn't anybody ~~got him~~ and somebody said that ~~comparably~~ possibly it would be Bill Lutwiniak

Lutwiniak by virtue of his ~~statistics~~ position. But

I want to know is how did it come about that we lost this identification ?

the super experts in the technical field?

A: ~~Very good~~ That's your question.

Q: Yes.

A: Okay. My answer, ~~to~~ this is Frank Rowlett's answer, is that these super experts are a bunch of myths and what we're looking at is a an organizational structure devised by M group and the people that have to do the jobs in M in order to get the proper recognition and pay for people who had been ~~in~~ assuming senior staff responsibilities. Functionally its a beautiful idea but practically it's a little bit of a solution of convenience because the senior cryptanalyst is the guy who knows most about the problem that you have to work on and this is regardless of his grade and I can remember an instance where Walt Jacobs who was a sergeant ~~who~~ ~~joined~~ was running a bunch of majors in directing them in the technical activities over at Arlington Hall Station during the war so I would say that your concept of the so called organizational pyramid that you just used is

basically a fallacy. There is no such thing and that good administration demands that you find the fellow who has the skill required by the problem and in modern cryptography and cryptanalysis the field is so broad that you'll not find any man who is master of all the branches of it. Now you'll find specialists in a variety of fields because it ~~had been~~ has grown so big and so broad and this would be contrary to what happened maybe in the early years when Friedman certainly was ~~a~~ the machine expert as we came into the early 30's and he knew more about cipher machines, ~~their~~ their use, application and weaknesses than anybody else. But now, there are many more types of ciphers machines and there are many more people who have been, ~~able to review it and~~ introduced so you can pick and choose for your specialists in ~~with respect to~~ any given aspect of this thing and I don't think you need to worry ~~know too~~ much about the pyramid effect because if there was such a pyramid its the organizational administrative structure that was being reflected and not the skills of the people who are involved and I would presume if you'll sort of ease your rules that you

could say the guy that's been hanging around the longest and had the most experience ought to be your ~~under the~~ senior man and I can think of no better candidate for this than Bill Lutwiniak who is also been involved in a lot of things but I ~~find it~~ am inclined to think that you could also go down to Research and Development organization and find people both in the intercept and the cryptanalytic-computer fields who could qualify as being very senior, very senior cryptologists even though they might not wear ~~have~~ the tag of a cryptographer or cryptanalyst but walk out with the emblem of an engineer on them. Now I guess what I'm saying is that your the guys who are up close to ~~at~~ the top are the ones who have had the greatest exposure to a variety of problems and who have done well in more of them than some of their collaborators.

Q: Valaki

We help the NATO countries help improve their systems so they don't spill our secrets, that there hasn't been that much ~~type~~ of a change in new ~~the~~ systems. Just to a certain extent but not that much (Rowlett chuckling in background) we ~~and~~ still can read [redacted]

without any help [illegible] systems they've made

themselves and this is true just about for a lot of them - but anyhow -

and I just wonder if you can explain it and also ~~there is~~ that despite

all kinds of skills and all kinds of information that has appeared in the paper

and you would think that anybody ~~who~~ could just rush home immediately

and change the systems and throw out the old crypies and get

a new bunch, or something and relatively speaking nothing has happened.

Either that or we managed amazingly to be there to meet them when they come in to pick up the machine or whatever.

A: (laughter by Rowlett) Virginia Really do you expect me to give an intelligent answer

to something I dont understand either. I don't understand it. You know we're always scared to death

if we improve a nations if we expose a better cipher to a foreign nation ~~nations cipher~~ they will replace the ones that we can

read ~~xxxxxx~~ by this new version but some how or other just like seed falling on

unfertile ground. It don't take root and it don't grow and I can't understand it.

I never could understand it. and I've come to the conclusion maybe that John Tiltman's

remark is probably is more germain

to this situation than anything else and ~~I receipted for~~ I'll repeat it here for the sake of bringing us up to date that ~~in~~ when cryptographic system~~s~~ security is questioned ~~that~~ ~~sperind and the~~ people that are usually turned to are the experts ~~in the~~ who devised this system and the~~y're~~ that motivated by ~~the~~ sort of 2 impulses which add up ~~and direct their~~ thrust and the first is that they because ~~I would back down~~ of their background, their training, and their understanding of the situation think this is a good system and it's the best they could produce which they did in all honesty, and therefore they don't understand why it isn't good and second ~~you have~~ even if they ~~just~~ question ~~to~~ the system or if they ~~said~~ felt it was insecure, or had their own doubts about it ~~it~~ they would be most reluctant to admit their failure because it could destroy the ir professional standing and so you will find I think a sort of reluctance sort of a natural human trait in the cryptographic masters of foreign nations to adopt ~~these~~ new systems because they are afraid it will destroy the ir professional standing or they don't understand enough about the

weaknesses of the system that they've endorse to be suspicious of it. (I think this is the case of David ~~Bowman~~ Sperry in the State Department around 1930.) He just, one, had such a limited understanding of cryptology ~~from the~~ because ~~sense~~ that to be a good cryptographer you've got to know both sides of the coin that is what makes a good system and what makes a ~~great~~ strong system and how to join the two to produce a proper cipher. I don't think his depth in that respect ~~is~~ was very great and, second, he just couldn't afford ~~the~~ to change the system because ~~he~~ it would have admitted that he had made an error (area)? decision that was wrong

Q: ...Giving a lot of information low - level information on cryptanalysis to some of the people in third party intercept third party practice. I was just wondering what do you think it would do to the cryptanalytic ~~xxxxxxxxx~~ expertise in the country in those countries. Are we giving them a leg up that we shouldn't be giving them?

A: I don't know, don't really know because the world is a real conflict situation we have

now and there certainly are two parts. I don't think we should go too far in the release of information but if we're going to use these people we ~~have~~ got to tell them enough about the problem so that we can take advantage of their geographical location and their skills because our manpower requirements can just never be met if we try to do this all ourself. We learned this years ago. One of the reasons we went into third party arrangements was to multiply our intercept capabilities for that very precious geography which we don't enjoy. Now part of the price we pay is for selected third party nations that we can trust and look like long term friendly people. It's to share information with them but we got very carefully to screen that information and release it in such a way that well for example if we're reading the traffic of the country we're collaborating with we certainly don't want to dry that up. Well now you just can't have your cake and eat it so you ~~have~~ got to make the choice between whether you deny yourself intelligence about that country or help get them to help ~~to~~ you

~~14~~ 175

to do the kind of job that you need to have done, and each case has to be decided on its own merits. I think we're getting way over our heads here if I try to go further than that ~~to~~ in answering your question because you got to examine each one on a its own merits and I've had to be involved in several of these examinations and it gets to be a very complicated problem and the one complicating factor that I'll sort of drag out as something to be on the watch for -- that the intelligence analyst, the people in the intelligence game whose bread and butter is derived from the intelligence produced through NSA's activities on that country are going to be deadset against cutting off that flow of information and usually they are the ones who cast the deciding vote and it this isn't necessar~~y~~ily the ~~whether~~ ~~to~~ place [redacted] where the deciding vote should be cast and that is my word of caution.

Q: Why did Friedman select mathematicians settle on mathematicians rather than any other batch of people?

Valaki

A: That was for the selection of the first group and the fallout of the Yardley

funds and if I can talk about the $10,000 that was available to the Signal Corps for hiring junior cryptanalysts. Well I think the answer to that is fairly obvious to me because I saw it while it ~~what~~ was happening. Friedman had just was still in the still was just very soon after Friedman had been so successful against the Heb~~ron~~ern machine and solved the challenge that the navy had produced. Now if you'll look at that writeup you will find that the key to Friedman's success was basically a statistical advantage that he had developed. Now he was convinced from that experience working with against the Heb~~ron~~ern machine that mathematicians who could understand statistical things and statistical principles ~~as well~~ and laws might turn out to be better cryptanalysts for that kind of a problem, mainly a machine problem, or related machine problems than people who didn't have the background. He was simply taking advantage of their schooling and their training in college or whereever they may have been trained to forward their preparation for their cryptanalytic training. I think it was that simple. Now most of us who followed on after

Fred~~i~~man sort of observed that yes this was a pretty good thing that he did because he was looking for somebody who had statistical training as part of his background and that since it worked for Friedman it ought to work for us and then pretty soon we kind of lost sight of the fact that Friedman had a very pragmatic basis for this conclusion and we sort of generalized it maybe too freely and said that "Oh yes we will deal with mathematicians and look for mathematicians first" but I go back in my mind and I can think of a Greek scholar who turned out to be one of our most brilliant cryptanalysts and I can think of some mathematicians that I wished to God I'd never seen.

Q: Valaki ~~Who~~ What has given us the impetus to improve our systems from the outside and to conduct (?) our own self-examination. Did the defection of M&M also spur us on to look at our systems again?

A: Probably not. There may have been a little impulse in that direction but the M&M didn't have much contact with our own crypto systems. They were more or less

involved ~~with~~ in the Prod aspects of the thing. I think there ~~were~~ was some overtones of the CSEC operation there. We looked into it but I don't remember at the time that we looked into that we found their exposure to our current systems was anything to worry about and anyhow sort of as a background to this one of the concepts we had in mind when we laid out our cryptosystems was that they could survive ~~that~~, such a circumstance so I think all that needed to be done was to ~~know~~ note with interest that ~~within us whether~~ Martin & Mitchell had been exposed to certain CSEC things and to make sure that these had been appropriately changed either due to the timeframe in which they'd been exposed or because they were now now in the state of defection and then I think there was some effort made to look at what might have been compromised in CSEC ~~and~~ but I think my recollection is that we came to the conclusion there wasn't anything there that was earthshaking, distressing or course, but there were many more important distressing things associated with the Martin & Mitchell defection than what they carried over in CSEC. I think

we were mainly concerned about the effect it would have on other nations. I know we sat waiting for the other shoe to fall for a long time and I don't recall much effect that we observed. I think if it had been anything real startling it would have surfaced but it was more or less business as usual in terms of the coderooms of other nations. Our impetus to improve systems is not a reaction to something that happens in real time. It's more an instinct of preservation and its been built up during the years going back to some of the things I've referred like the Fellers incident, the 228, we have learned some lessons that have been so deeply impressed on us by circumstances of the historical situation in which we found ourselves that we have subconsciously assumed a certain instinctive reaction that we perform when we prepare ~~an initial~~ and issue a system. Now as I saw it from my experience in where I sat in the last few years we had a good strong instinct in regard to the construction of the system. How long we let it stay in effect, the physical security surrounding it which

we had very little control over but we could lay down certain rules you see and have inspectors to go out and look about the installations and see what whether they were being conducted in accordance with the best practices and most important to sort of keep track of how much a system was ~~being~~ used so that it didn't get overloaded and thereby result in a compromise of some sort because it hadn't been used properly - it had been used too much. Now these are sort of SOP I think in making your cryptographic decisions. Some of the things that I bumped into that hadn't fallen into our instinctive apparatus were the more modern sophisticated kind of things like spurious radiation and stuff like that if it means anything to you and these had to be taken into account, I think particularly in Moscow and usually though when we sent a system to be used where it might be compromised in lets say ~~in~~ a communist nation or something like that we made sure that this was a special use system and that it wasn't universally used so that the traffic lets say from London to Washington if you

can imagine that oversimplified situation could not be compromised if the Moscow to Washington link had been physically penetrated by the Russians, a second story job had been done on that.

Tape 4, Side 2

Your question about the special advantages of the Madam X the relay type of Bombe over the mechanical type of Bombe which the British and the navy employed; The U.S. Army uniquely employing the relay type which we called the Madam X and other Bombes being more or less the navy being updated version of the British mechanical Bombe. Well the Arlington Hall Madam X type of Bombe had an advantage over the navy and the British type of Bombe in that it was particularly useful for finding the setting of wheels in a message in which the indicator was unknown and one of the messages dealing with the Battle of the Bulge which contained the key information had lost its indicator and the crux of the message as I recall and this is probably an oversimplified and maybe too well recollected circumstance but one one part of the message which revealed the point the whole point of the Battle of the Bulge was in as well as the geographical location was intercepted but could not be decoded by

the Bletchley Park outfit because they didn't have the indicator. Well it was not recognized in the watch office at that time that this message was of such importance so it got so ~~showed~~ picked up and transmitted to Arlington Hall where we ran the dud-bust operation on the unknown messages because there were quite a few of them and when it was broken and sent back it was the particular message that the intelligence analysts had been looking for which was a missing part evidently and they were looking for ~~an~~ the answer to it and when it came why then the whole picture of the Battle of the Bulge began to emerge as it could be deduced from the Enigma traffic but at that time it was too late to anticipate the what the Germans were up to so the Battle of the Bulge was already under way and the golden opportunity was missed because the indicator had been missed by an intercept operator and we sort in retrospect having looked at the advantage of the Arlington Hall dud-buster as I like to call Madam X now as opposed to a Bombe, we learned through the rest of the war that we could make a better use

of the dud-buster aspects of Madam X then to use it as a straight Bombe and we concentrated on it from that point on out so that we were able to provide I think a very valuable adjunct to the British Bronze Goddess operation ~~in~~ that Winterbotham brags about. Now this is I'm generalizing. I haven't thought enough about it to give the details but this I remember. I know we talked about we just if they had just got that sooner we may have saved a tremendous amount of lives. It's a scary business we're in, particularly in wartime because you know that just little shade of difference in judgment can mean a difference between losing a battle and winning a battle.

Q: Did the British know that our analog was much more sophisticated than theirs?

A: Are you recording? Did you get that question? I would like to change your question a little bit. The British realized the peculiar advantages which the Madam X type of construction afforded in terms of the dud-buster aspect for example but our Bombe was not as fast as the British. I mean we could run a three wheel Enigma setup as effectively as the British could and dredge it out but it would

take us longer -- the relay operation was slower than the mechanical operation. I think it was I don't remember the factors but ~~it~~ there was an appreciable advantage in time that the mechanical Bombe had over the relay operated and we had gone to the trouble or at least the engineers and the telephone people who had put the Madam X together had gone to the trouble of selecting the relays and sort of speeding up their operation and ~~operating~~ they operated them much faster than they normally would operate in terms of telephone requirement because we wanted to shorten the running time as much as we could but there ~~is~~ was a limit as to how much you could speed these things up and Sam Williams who was one of Bell's greatest relay experts lived ~~at~~ with that installation until it had served its usefulness. He just kept right on top of it. Actually I don't think we were justified as I look back in time to make a judgment. I don't think we were justified in building the Madam X because it certainly wasn't ~~sufficient~~ as efficient as a mechanical Bombe. I think the navy made a wiser decision but sometimes it is better to

be stupid than smart because we would have lost the advantage of the dud-buster and I think it was worthwhile to have a dudbuster even though it cost a good million bucks and it would have more than paid for itself if we'd if circumstances had permitted us to fill in this gap in the Battle of the Bulge message. I mean and there may have been other cases which well you notice the Battle of the Bulge because you lost, you pay attention to it but there may have been ten or fifteen other cases where the dud-buster advantage would be as significant as that message which we lost.

Q: ~~So it~~ Certainly would have been advantageous had the British had that advantage on their system.

A: And had we realized it sooner, but you see it was mechanically impossible because the nature of the to do this kind of a thing the way the British machine was designed and the way in which all you always had to have a good probable word to crib before you could line up the message. Well now the dud-buster aspect of Madam X didn't require crib. It used other things. I don't ~~imagine~~ remember

now just what they were, but Dale Marston could tell you. Leo Rosen. Matter of fact out of this concept that the Madam X Rosen designed and put together a beautiful cryptanalytic device which was mainly relays which was in effect it was a dud-buster for the ~~Hamlin~~ Hagelin system so he could locate the Hagelin wheels, just run the thing and it gave you ~~a~~ statistical index. A sort of IC and this is what we used whenever we came to ~~a~~ the point of reading the messages about the Japanese surrender. This device was useful in reading one of the legs of the information travel order. To clarify this last point a little bit the surrender message was since the Japanese couldn't communicate with us directly they had to send the surrender

the what we call the surrender message that is their announcement they were ready to negotiate an unconditional surrender to some mutual party like the Swiss. The Swiss in fact are the ones they selected so the message went from Tokyo to Berne. The Japanese Ambassador in Berne and then it was decoded there, taken over to the Swiss foreign officer and then sent from Switzerland, Berne, to the Swiss

Ambassador in Washington ~~and~~ who then delivered it to the U.S. authorities. I've told you this story, haven't I?

(Not in that detail)

Well this is interesting historically. Well here is what happened. In we knew the message was coming because we'd been reading the traffic but we hadn't seen the message so we ~~sent out~~ set up a special intercept services. In San Francisco we had ~~xxxxx~~ a landline into one of the wings at Arlington Hall Station and when that message came over the air we had a good copy. I don't I think it was San Francisco but anyhow from an intercept station we had a line running to Arlington Hall Station and I think it was San Francisco. It may have been Monmouth or some other place or it may have been Fort Hunt, but there the message was being typed out on the teletype. We were all set up for it so when the message got on the air and its first transmission of course was to get it to Berne and I think it had to take two steps maybe somewhere in the Indies, the East Indies and then on over to Berne before it could be received because of the radio transmission situation at that time, ~~kind of scare~~ atmospheric conditions, so we knew when that message went on the air and we also knew from

the pilot messages that it was going to be in the Japanese code that they used for such things which we called LA code ~~for~~ L.A. LA is a diagraph ~~for their own private~~ that identified the code. Now there was a young girl down here in Virginia or West Virginia somewhere who felt worked on that code and loved to work on it and she had memorized the code and we put her at a table right next to the teletype and when that message came in this young lady looked at ~~got~~ it and wrote down the plaintext just as almost in the realtime it was being typed out and then it was one of Ed ~~Rishour's~~ Reischauer's boys who was on the telephone calling over to G2 talking into a talking to a stenographer who was producing a typed copy on that end you know from what he had read to her on the phone so that when before the message was receipted for by the first jaw the information was in the hands of G2. Now this is really really fast operation. We didn't do this for every message but we did it for the surrender message and of course the President was vitally interested in this thing and word got to him as quick as they got a clean copy

from right there but we were a little distressed because there were some garbles that came in I mean it wasn't a full transmission so they had to when the message got down to Berne and the Japanese received it ~~in~~ and decoded it which was not in the same time frame. I mean it was a long time. The message got there. They had to ask for a retransmission and then we had to wait until the message was delivered to the Swiss foreign office by the Japanese amb... his messenger boy, ~~for~~ the Ambassador, and then they had to decide what to do with it, encode it and send it to Washington. Well we intercepted that message and we broke, we were reading the Swiss code at that time, so we checked the message being sent through the Swiss diplomatic system against the Japanese version that ~~was~~ we had intercepted out of Tokyo and let that word get over to G2 and confirm the transmission. Well this of course started long after lunch and went on until well close to dinner time because it takes time to do all these things except from our standpoint we were right there the minute it ~~We~~ got on the air from Tokyo. That's all we

wanted.

(Could have told the Swiss not to bother.)(laughter) (We already have it, thank you).

This would have been wonderful. That reminds me of something like that happened.

Of course to wind up the thing it was along about 6:30 or 7 ~~:00~~ o'clock when we got the closeout, you know that it had been ~~in order to~~ delivered to the Swiss Embassy here in Washington and then those of us who had been sort of worried about this thing, I went home because I wanted to see what was going to happen on the radio, you see. I wanted to get away from that place. I knew the war was over and so I went on home and sat there, and didn't go to dinner. My wife said "Why don't you come on and eat?"

I said "I'm tired. I want to listen to the radio a while."

"Well, I'm going to take the kids and we'll eat."

And I sat there you know just anxious as all get out waiting for that radio report to come through telling us what was happening officially and it finally came through and now I could say to my wife "Did you hear that radio report?"

(laughter) There is a little bit of a sort of a incidental situation. B4 was

the Japanese translator who and some how or other the word got out in B4 this message came through in English [illegible] anyhow it came through. Well now every God damn translator in B4 began ~~honking~~ hunkering and hovering over that little girl who was doing the best she could to decode this message and I walked down. I had sense enough to stay away from the place. I mean I didn't want to bother her. She was down there doing her ~~best~~ business. All I could do was to help her and the best way I could help her was to leave her alone and when I saw this gang coming down there I just put on my Colonel's bars or whatever you wear when you're a Colonel and I told to get the hell out of there, They were going to break the floor through and leave her alone. And then I got scared and I went down to see Dink Hayes who was running the _____ and I said "Look now you know this is more excitment than we've had for years What are ~~you~~ we going to do about it?" and he goes "Well we better do something. What can we do?" and I said "We just go and remind them". and he said

"Well you better get out there and remind them, Frank." He says "I'll do some and you do the others" so we got to Kully and the three of us went around and announced to people "Yes, we've received the surrender message and yes, the war was over but for God's sake don't go home and brag about it. Go home business as usual. Please don't give away these secrets because we don't know how valuable it could be for us to continue this information and just go home and be surprised like everybody else when you ~~hear~~ get the news over the radio. And I think that was wise. I think ~~he was~~ we were very thoughtful in doing that. Big moments in your life? ~~That's~~ of course, the biggest moment when Hank Graff called me on the telephone and said "Colonel, cut it." That was a wonderful thing. I'm sorry I'm wandering off.

Q: Goodman That's all right. The L.A. code goes back quite a ways doesn't it? You all had done some work on that from Yardley's stuff.

A: Well what had happened is they used a version of the L.A. code in Yardley's time and then they evidently updated it. It was a utility code. It wasn't

a secrecy code.

Q: You ~~were telling~~ told me once before that the L.A. code was one of the first things

Goodman

you all had looked at in the vault.

A: Yeah that was a little bit about that if you'd like. What happened is Kully and Hurt see I was compiling the codes and Abe was doing I think he was doing correspondence courses and so Kully got fingered to work with Hurt in getting this make the first move into the Japanese stuff. They picked out some messages and Kully would decode them, you see and then he'd hand the decodes to Hurt who would look at them and Hurt had a batch of traffic in the L.A. indicator and it didn't quite make sense but he kept saying "This almost reads. It's just, it's just beyond me. I can't make sense out of it." and then finally his cryptanalytic training came to the front and he began to change groups and I can remember it was a real exciting time because Hurt got so excited himself that it was contagious and he ~~said~~ says "Look they changed the code." and Kully said "They couldn't have changed the code." and Hurt says "It almost reads and, he says if I make this an RU instead of an

? N
MU he says it makes a good word. So he and Kully pretty soon ~~it~~ solved, worked out the variations that had been introduced by the Japanese cryptographers. Oh it took them I think a day to clean up the thing. It wasn't too much of a job and this was very useful because it encouraged us to dig deeper into the traffic because we felt like the changes that had been made weren't going to be so significant that we couldn't bridge the gap from what Yardley had done to what we wanted to do and that's in fact what happened.

Q: Valaki How did you start working on traffic. Did you have big tables and sort it out in piles? Did you take a little bit at a time and look at it and wonder what to do? Did you know how to cope with quantaties of traffic because there were little exercise books you know in a little book all the systems are the kind that can really solve one at a time or taking two at a time. They don't really require massive material and organizing massive material to get into them so you were confronted with quite another situation. How did you manage?

~~How did you manage?~~

9-/96

A: Well ~~I can~~ let me tell you what we did and you can produce the answer to your question.

As I recollect we we had sort of two phases to this. One ~~is~~ was to look over the material that Yardley's group had been working with and which was down in the vault so we started out with that. Sort of in the same time frame but separately we had the current material which was coming in in dribbles. We didn't have any cable intercept at that time, it was mostly ~~See~~ Second Sig [Second Signal Company] produced material, and We'd been looking over this current stuff that come in ~~because~~ of course we sorted out the Japanese and everything else and we put the Japanese in one pile. We could do this very easily because it was either addressed to Kochi or ~~Guy Nu Guy Jen~~ GAIMUDAIJIN and signed with the Ambassador's name Kochi Washington ~~Guy Nu Guy Jen~~ GAIMUDAIJIN Tokyo and that was easy. Most of it was ? numerical traffic as I recollect in the Japanese diplomatic stuff. So we had a big _____ of the navy we had a ~~big~~ half a file drawer of stuff. It wasn't too much. See there

Q: wasn't much interest.

Q: This is the current stuff you mean?

A: Yes this was the current stuff. This latter and Abe and I were pretty much

spare timing this batch while Kully and Johnny were dealing with the Yardley material. And some of it well the two general categories that I remember now that come to my mind as I look back were those that were divided evenly into five letter groups consistently in five letter groups and those that had groups of varying length, ~~that go~~ anywhere from usually 8, 15 or 20 letters. And then there was a batch of Japanese plaintext and these were the three piles we sorted into. The stuff with varying group lengths we put over in ~~the~~ a pile~~s~~ and said we'll look at that later because it doesn't look like any of the things we found in Yardley's place and then let's then see if any of this current material matches, can be worked with the Yardley's systems and so that's when we began to try the old code charts recovered by Yardley against these messages. That's what Kully and Hurt was doing with the current stuff because there was no point in working any longer on the Yardley stuff because most of it had already been decoded and processed. It was just a familiarization thing with that but to test the codes

against the current intercept was very important thing to do. Well it was in this process of testing the codes that Hurt ran across these messages that looked like they might be about ready to read and once he spotted these and only Hurt could have done this, the others, were'n't we didn't have enough language to allow us to do that kind of a judgment so once Hurt got a clue and then he saw what was happening of course, now our action became much simplified. What we did then was to take the current traffic and go through and find out what characteristics would enable us to identify traffic characteristics would enable us to identify the messages in this code that was readable and so we sorted that out and Abe and I did the sorting, and I think Kully did the decoding and he and Hurt together sort of put the messages.....

When Hurt received the decoded when Hurt looked over the decoded sheets that Kullback had produced he was able to ascertain, translate the messages although he was a little bit familiar with the language used in ~~by the~~ Japanese diplomatic traffic his

ability as a Japanese translator allowed him to make the translations immediately of the contents of the message. Of course the LA code at that time and later on as we ascertained was being used for administrative matters which were pretty trivial so far as the information and intelligence was concerned and so there was no world shaking translations produced from this simple code breakthough. Now after we had been able then to subtract the quote LA code from the other systems we began then to subdivide the remaining traffic into categories based on the external characteristics of the message which now became meaningful to us because as we looked at the LA decodes we could understand something about the way they numbered messages, the format, the plain language and we looked for the same kind of things that Yardley had discovered when his group was decoding these messages and then of course we pretty soon packaged up the replacement systems which was carrying the better information that Yardley had been able to produce such as that ~~said~~ for the naval conference held in Washington. They had

evidently changed their codes and this would not of course be surprising to you or was it surprising to us, so we had then had identified what we were going to work on as our first problem, one of these unsolved messages, and then we tried to put them together, packages or sections of them together which would insure that we were working on one system and not a multitude of systems and we'd look for repetitions and simple evidence like that and pretty soon we began to build up a body of traffic that we felt was homogeneous, one system, and later on we were able to break into this. Of course it wasn't the sort of "identify it today and read it tomorrow". It took us several weeks of poking around trying to find out what was the best system. We couldn't couldn't proceed like Yardley's group had done with their indexing because he and his people had organized their a group working on Japanese into clerks and translators and codebreakers and we were clerks and translators and codebreakers all in one with only one very proficient translator and that was Hurt and we had to devise some

way ~~to~~ of making our catalogs for the bookbreaking operation because it was unenciphered code so that we could achieve the end that Yardley's catalogers had achieved, ~~mainly~~ namely the location of the group, groups in front, groups in back, and then work out the numbers and dates and more frequent Japanese language groups and this was pretty slow process. A lot of cut and try and finally we developed a technique, and we began following it and we began to get results. Now I think I answered all your questions.

End of Tape 4, Side 2

Tape 5, Side 1

Q: Do you recall any contact that you had with with Fabyan and Riverbank in the 30 's?

Goodman

A: I can't recall any contact with Fabyan. I rather suspect I met him once but I wouldn't swear to it. The role of secrecy which we had to satisfy in respect with our purpose, namely eventually to become the cryptologic organization of the Signal Corp or the War Department and the proper fear that any exposure of our activity might cause it to be killed off. I think precluded Fabyan's being introduced to us because he would have immediately identified this and he was notoriously a man who liked to make noises and I doubt I really doubt that we met him but I may have, but it was a long time ago and if I did it was probably in 1930 and not later so I'd say there was no contact with Fabyan and if there was any contact it was sort of incidental and would have been handled in a very reserved manner.

Q: In the 19 in the 1920's with Yardley in New York doing cryptanalysis what was the Signal Corp doing in the 20's and specifically what was Mr. Friedman doing in the 20's?

H.S.

A: Yardley in his effort, the one up in New York city, was aimed at the production of intelligence in support of the G2 well the State Department requirements and incidentally in support of G2 because State Department was funding Yardley's organization with a sort of token contribution of I think it was 10 grand, that G2 provided, the War Department code program I mean the program of cryptography now as opposed to cryptanalysis or COMINT in our present day nomenclature, that Yardley was doing, the COMSEC activity was in the War Department and it was divided into two packages as and I think ~~that~~ I'm reasonably correct on this, the Chief Signal Officer was responsible for the design, the compilation and supervising the use of codes, with the supervising the use being a very ~~mute~~ moot question because it was an area for conflict between the Adjutant General and the Chief Signal Officer and the Adjutant General was responsible for the publication. Now in the sense

DoS

that the Signal Corps would prepare the manuscripts and the AGO (Adjutant General's Office) would do the publication. The AGO also did the storing and distribution, mail room operation that we used to look on the Adjutant General as Post Master of the Army and a very limited concept of their duties. And also the operation of the coderooms and preparation of the message for transmission by the Signal Corps circuits or other means, Signal Corps within the military establishment, other means if they were outside of the military establishments for example to the military attache in London or some other foreign country, the cable would be filed on ~~the~~ a commercial circuit but any message from the War Department message center to any of the ~~core~~ Corps areas of the three departments would be turned over to the Signal Corps where they would go on the War Department net and then there were certain variations to this rule but messages might be sent by the Chief Signal Officer on landlines, Western Union, to points within the U.S. There was a kind of well it was probably designed

based on the a previous concept of the roles of the Chief Signal Officer and the Adjutant General in terms of the formal ideas at that time but when you've got it down to the practical concept there was a certain amount of overlapping and particularly ~~of~~ this concept of the Chief Signal Officer making sure that the codes were properly used but had become a pretty acrimonious subject and laid the groundwork I think for what happened about the time ~~that~~ we came in and that was getting all these responsibilities of the Chief Signal Officer including moving the message center and the code storage and distribution program from the AG to the Chief Signal Officer. Now I think I might elaborate on that a little bit, probably deviating from your question, but I think its important to note this. When the decision was taken to form the group, ~~of~~ the SIS, there was still the concern about an official ~~edit~~ edict from higher ~~in~~ than the War Department causing it to have to be stopped. Now they had to justify the existence of this group by and its emergence at that time by ~~the~~ a change in the organizational structure

and also the Chief Signal Officer stimulated by Friedman who was aware of the insecurity of our systems was much concerned that and G2 particularly was much concerned that better attention should be given to the ~~program~~ practices and the use of the systems and with the physical security ~~majors~~ measures should be improved. So everything was for putting it ~~on~~ under the Chief Signal Officer and there was nothing that the Adjutant General's office could produce except that we'd been doing it for a long time and we think we're perfect and nobody believed that latter statement because they weren't perfect. The people who were sophisticated enough to know were distressed. Col. Albright. He had no words of praise for the Adjutant General's way of doing the thing. I heard him say one time that it ~~there~~ was a change that was long overdue and that the country would suffer would have suffered tremendously had the change not taken place so there that is sort of the rationale behind it. Now did I answer the rest of the question?

Q: Uh, how about then from 1921 to ~~1~~929 Mr. Friedman was in code construction, compilation.....

H.S.

A: Yes. I'll give you a little detail on that. I believe that part of his career is pretty well set forth in David Kahn's book but initially Friedman was hired as a sort of consultant by the Chief Signal Officer for his expertise on codes and ciphers. He had made a reputation for himself up at Riverbank ~~with~~ by his work on the Wheatstone and the Star cipher which was the forerunner of the M94 and I believe that he had done the Vernam system for the AT&T cipher while he was up at Riverbank and this was so far ahead of anything else that anybody within the U.S. government had done, the Chief Signal Officer had ~~let~~ got Friedman ~~to~~ come down and he wasn't under Civil Service, it was sort of ~~excepted service~~ an exempted position that Friedman ~~had~~ held and they gave him a ~~sort of~~ some office space and secretarial and clerical assistance and Friedman then laid out the code program for the Chief Signal Officer and it was not until sometime after 1930 that Friedman ~~was~~ ever able to move from this exempted position status on to Civil Service roles you see.

So he was technically an employee of the Chief Signal Officer but organizationally he was somewhat of a consultant I would imagine. Organizationally in terms of an administrative concept. Now there was nobody else of that stature in the War Department so Friedman was pretty much of a one-man operation with one fellow who was a perfect typist and some secretarial help. Finally, ~~by~~ about the time we got there Friedman had a fulltime secretary ~~ial~~ but he had lost the clerk who was a veteran and I think his upper limit was being able to do an accurate job of typing whether the word was spelled correctly or not he could type it accurately so Friedman didn't have much help really. All he was doing was on his own and he had no facilities in support of him except well he had the vault where things could be stored which was sort of donated by G2. He had access to the message center and things like that but because of his position he could go over and study what was being done in the Adjutant General's group that were dealing with the code production, well, with the Adjutant General's cryptographic responsibilities and because of where he was he had

Pos developed contact~~s~~ ~~at~~ with the State Department and contact~~s~~ with the Navy although the navy was pretty pretty hard nosed about letting anybody outside of a navy officer get into their ~~a~~ code room especially selected personnel assigned thereto so I doubt if Friedman's access to the navy ~~room~~ group was as free as it should have been really and I think he had a little better relations with Salman than he did with the navy group because Salman felt very insecure, at least that was my estimate when I met him ~~about~~ of what he was doing in his position, but he was just overwhelmed by the organizational difficulties that confronted him and his own lack of sophistication in cryptologic matters. One of the things which I observed with a great deal of interest was sometime in 1930 we made ~~a~~ the physical move of the

Pos coderoom from the Adjutant General's building, the old State ~~and~~ War and Navy Building which is now up there next to the White House in Washington, down to the Munitions Building and put it in the corner room in the last third of the wing just across ~~in~~ from the radio operator's position so that the message center was colocated with

the transmission facility. Some rooms had been selected that could be locked, sealed off with a little bit of an entrance area so that people who brought in the ~~mail~~ and picked up the ~~messages~~ didn't get into the coderoom and see what was happening so the coderoom activity was really sealed off and conducted behind closed doors with a little bit of a front office type of arrangement for messages to be ~~dropped~~ and ~~picked up~~ and administrative and other matters to be handled without interference with the coderoom. The coderoom operation itself was pretty simple. It involved the use of the war department telegraph code and the military intelligence codes and that's all I remember right now. The none of the messages were encoded. None were enciphered. They were all encoded in this tremendous code and if the message was to the military attaché or in the military attaché system it was I mean all the military war department messages were encoded in the war department telegraph code, the great big code that we used for everything. But a message to a military attaché was encoded in a separate system which I believe at

the time the message center was brought over was MI, military intelligence code, 19

and these messages were always enciphered with a set of cipher tables, 10 tables.

Tables 1 and 2 were the reciprocal of each other, tables 3 and 4 likewise, 5 and

6, 7-8, 9-10 and so you really had five tables in encipher and deciphering versions.

This was looked on by the Adjutant General as the ultimate in security and if you

had to send a message that was really sensitive if there ~~really~~ was such a

message in those days it would have gone in the MI10 code if people on the other

end had the code. If they didn't it would have gone in the War Department

Telegraph Code.

Q: Goodman Did the Adjutant General prepare the Military Intelligence Codes or were they

being done in-house by _____? (2/2)

A: That gives me a question to clarify what I said earlier. The manuscript for

the military intelligence No. 10 code would have been prepared by the Chief

Signal Officer and the manuscript would have been turned over to the Adjutant

General and from there on it would have been ~~the~~ an Adjutant General's responsibility to have the code printed, to store and account for the code, that is to keep it in safe conditions and when it was issued to determine who got the code and if they did in fact receive it and to get the periodic reports that the code was in hand and non-compromised. At least that was the affadavit that was required from the holder of the code and to recall and destroy the code you see when it was superseded by the next edition. I believe that the military intelligence code, ~~of~~ cipher tables that I described, the 10 tables, substitution tables, which super-enciphered the code groups prepared in MI9 was prepared in G2 by the special section under Friedman's supervision because even at that time G2 wanted to keep its own hand in its own business and I think this grew out of some of the practices that had been developed in WWI so these tables were of course turned over to the AG after they were mimeographed and they were not printed and the word is multigraphed and this has a special connotation because in that timeframe there was a

reproducing device with which consisted of a drum with a lot of slots in it and a supply of ~~tab stops~~ type slugs with typewriter face and you composed your whatever you were going to reproduce on this multigraph device just like you would set type and run it through a press except the type ~~is~~ was set ~~up~~ on this drum with a lot of grooves in it and G2 was responsible for the setting of the type and the running off of the tables and I think from then on the Adjutant General took over and handled ~~it~~ them, distributed ~~it~~ them, counted ~~it~~ them and stored them as necessary and of course there were tables ~~that~~ which were used for a given period of time. I think there was three months and then they had a bunch of emergency tables in case one got lost or compromised they could ~~prepare a~~ declare the table out of date and ~~produce~~ introduce the emergency table and it was up to ~~G2 G3~~ G2 and ~~G2~~ the G3 to get cracking and produce another one and get it out to the field. I don't remember whether it was one or two emergencies. ~~but~~ I think one of the things we introduced was two emergencies so in case the emergency was lost we had a backup. Now when the coderoom came over only two

cryptographers came with it. These were Benjamin Smith who was just about ready to retire and a Mr. Williams who also about ready to retire and this was the carryover of expertise and people from the Adjutant General's office. These two men I got to know well because I work ed in the coderoom for two reasons.

(1) As part of our training, our indoctrination, Friedman and the others who were with him thought it was a good idea to have us get some code actual coderoom practice and of course this was a little bit well here's what happened. Mr. Williams wanted to go on leave for a month. It was a long way it to the Mid West where he lived and he had for years been taking his summer leave in one slug and spend it with his family. He was either a bachelor or widow er and he went to see his old family and he spend this 3 or 4 weeks of annual leave out there and since this was his last year he just had to go this summer because he was preparing for retirement and had to make the arrangements for where he was going to live because he was tired of Washington. The town was too big, too busy in 1930 for him to tolerate it so he wanted to get back to

quiet and peaceful the Midwest and I got fingered to take his place. He was doing the night shift. We had day shift, night shift, no swing shift because there wasn't enough people or enough business to require this so you were going in about 4:30-5:00 o'clock, overlap the day shift, find out what had to be carried on and then work until the slate was clean, take the messages across the hall, give them to the chief radio operator who would then take each one of the packages that you laid out, the one for the Philippines department, Hawaii and the corps areas and pass them out to the respective operators just like you know a waitress would serve your meal after you've put your order in for it. That was the coderoom operation. All the messages had to be typed in regular form , standard form, put on the special preprinted pieces of paper which then would be filed and you always kept a carbon, two, I think one or two carbons, it doesn't make any difference but there was a message center record of these things. It was pretty business like, and pretty efficient. Now it was a wonderful thing, I think looking

ahead that This shift took place because again this helped condition us in our concept for the role of monitoring our own systems and see ~~where~~ whether they were used properly and I think the experience we got from watching the traffic pass and actually working in the coderoom, because Abe and Kully and I all did this except my ability to type sort of meant that I got called more frequently for coderoom duty than Abe and Kully because they were very good at decoding you see because they'd decode the message and pass it over for somebody else for typing on the day shift but since neither could type and you were required to type and since there was only one guy on at night obviously I got the night shift and I enjoyed that because I got to learn a great deal about the kind of people that are responsible for the transmission at the radio end of the thing which most cryptanalysts never come in contact with today and I also got acquainted with the difficulties they encountered, with the kind of problems they had in receiving messages and also their special skills and how to take advantage of them.

And this was extremely useful background training because you couldn't get that anywhere else. You never could have got it at Signal School or anywhere else because there it was in real time and you were living with it, and you could begin to sense the weaknesses in the system by observing it in terms of your own specialized training as a cryptanalyst. Now I elaborate on this because I want to emphasize that there was no capability for this kind of examination of the use of coderoom practices and radio practices in the earlier years before we actually got involved in participating in the coderoom, while it was under the Adjutant General agis, and I think this in a large measure accounts for the sad state of well the non-existence of cryptographic security in the 20's and early 30's, the early 30's because you just don't change practices of this nature overnight so it took us about 3 or 4 years to get the coderoom situation cleaned up and as a part of this we had to get some new codes compiled and new cipher tables, a variety of things like that. One example of the benefit of this is when we put in some of our new

codes, war department staff code, war department confidential code, which were the two _____ first ones that went in. The War Department Staff code could never be used without encipherment and a system was formulated for that. I won't go into details but I will go into the details of the system that was used for the War Department Confidential Code. Friedman was a great believer in transposition systems and he thought transposed code would be pretty good. He thought this would be a good place to try it out, so we prepared and issued transposition keys to be used for enciphering messages in War Department Confidential Codes and based on our coderoom experience and how it was used and by going down into the coderoom and looking at the traffic that was prepared, by this time enough enlisted personnel, sergeants and corporals had been ~~detained~~ obtained to do the work that Mr. Smith and Mr. Williams had been doing. By our examination of the traffic coming in and going out it became evident to us that the War Department Confidential Code enciphering system that we had proposed would not

stand up and so I remember getting sort of in an argument with Friedman about this and a challenge resulted in which we took a days traffic to see if we could solve it and so help me we did and this I think was the first example of where our group, ~~our~~ the little group under Friedman, showed (1) the validity of the contention that the Signal Officer ought to be responsible for the review and coderoom practices as well as the compilation, well the actual supervision of the coderoom. I don't mean ~~the~~ review because he still had that. The actual supervision of the coderoom and the application of the cryptographic system just showed the wisdom of bringing that over and putting it close to him because well actually the system fell apart of its own weight because we sent indicators ~~to McClere~~ in the clear which were bona fide code groups and the enciphered text of course was made up of code groups from the same garble table. Well with the indicators in the clear from the code vocabulary you could reconstruct the garble table and then you could determine the limitations placed on each one of the positional elements

in the five letter code groups, so we'd go back to the principles of the ADFGVX and the ADFGVX research we were doing was coincident in time with this thing and it just fell apart. Now this I think is worth noting historically because it shows that the concept that Mauborgne and Hitt and Friedman and Albright and the others who had been strong supporters of the Signal Intelligence Service coming into being, it showed they were right and encouraged them to go on and of course it was a big feather in our hats. Friedman ~~was~~ felt a little bit disturbed about it because he had proposed the system and then his outfit comes in and destroys it but he went up and very honestly faced up to it and he says"Look look at what happened. Look at how this group that we have started training straightened us out here you see. I've proposed this system and they destroyed it. This is wonderful, sort of." and he took that kind of a pitch which I think should be noted. He wasn't resentful. He was non-plussed. He was distressed like I was with the 228 but he faced up to it and said this has got to be

changed and we took it out. Crawford was the officer in charge of the War Plans and Training Group in April of 1930.

Goodman

Q: That was David M. Crawford?

A: Major David M. Crawford. He was about five feet eight, yeah. You got it? About five feet eight, blue eyes, sandy hair, athletic built, athletic build, wore rimless glasses, little bit nearsighted I think and very intense in his conversation and most gracious in his attitude toward young country boys who'd come in to learn to be junior cryptanalysts. He made sure that everybody that came into the office was introduced and with the proper manners, requirements had been satisfied and that there was peace and harmony with in the office. He was a very outgoing tremendous personality and loved to talk. He was always talking about something. He loved to try out ideas on other people, other people to get their reaction to them and sometimes he would take an adversary position even though he didn't believe in the question to stimulate the other person ~~and~~ to argue with him, and ~~he~~ it was very good. I remember one case where he and Friedman got in a big argument

over the difference in meaning between adhere and cohere and so Crawford proposed

~~to~~ the Friedman ~~that~~ and he go poll Abraham Sinkov, Solomon Kullback and Frank Rowlett

to see what was the true meaning of this word (laughter) and we simply confused

them because each one of us had a different concept of what cohere.... Mine I

knew what a coherer was in a radio sense you know. It was a radio detector and

the old radio detector was initially called ~~the~~ a coherer because the substance

they used to rectify the radio signal would act would physically pull itself

together when the signal was applied so they called it a coherer you see. Well

Abe and Kully looked on it as ~~a~~ the adhere type of principle where cohere you know

two things came together and stuck together and Crawford was trying to get the

finest distinction. I'm elaborating on this because it shows the type of mind

that we had in the Chief Signal Officers staff at that time and he had a tremendous

range of interest, things which not only were meaning of words type but things

related with the military profession and he was an avid reader and he liked to

DOCID: 4223202

speculate on world events and things like that and it was really an education to have David Crawford around. He was a first class Signal Corps officer. He was well respected by all up and down the the line and finally became a general and I think in charge of the transatlantic well some of the European communications because he was involved in the SIGSALLY program that is the master voice encipherment system used between the US and across the Atlantic with one installation in London used by Churchill in conversations with the President and there was another used by the War Department I believe in North Africa after the space had been cleared out of the Germans and they had a base in North Africa. And he was involved in that from the standpoint of the Signal Corps management of it and very capably got it installed. And He's the one that told me this story once that they'd gone up to see Mr. Roosevelt to see whether Roosevelt needed an extension up in the White House or just where he did want it. when they presented this to Roosevelt and he said "Well now where is Churchill going to

have his?" and they told him that Churchill was going to have it right next to his quarters in the underground which was down in the underground in London you see. They'd taken part of the underground and put the Churchill's headquarters and the battle parts of the government down there at least those that had to remain in London and then Roosevelt sort of wanted to know can this my end of the thing be put over in the Pentagon? and they said well we can put it right here in the White House if you want it Mr. President, and he said "No, I'd like it in the Pentagon." And they said "Well would it be more convenient for you to have it here?" and he said "Yes it would be. Churchill would be calling me at all odd hours at night and I wouldn't get a good nights sleep but if he knows I have to drive over to the Pentagon to answer it he won't bother me as much." (laughter) He told me this story. I think this is a little bit of a personality sketch of David Crawford that might be useful for people to keep in mind when they think that somebody had to be Friedman's boss in those days and I haven't seen Crawford's

name mentioned as much as it ought to be mentioned. It's important to note that he was there at the point of transition and was most helpful to me as an individual because he was a gracious, ~~and~~ friendly man and I admired him and his granddaughter works in the Agency today. I can give you her name when I get back to Rose Hill if you want it. Might be interesting to talk to her about him.

(Very much so)

Now there are other personalities post 1930 I can talk about but these right now I can't think of any more. What I'm referring to is Corderman was one, ~~Beecher~~ Bicher was another, Harold Hayes ~~was~~ was another, Mark ~~Rhodes~~ Rhoads ~~was~~ was another, Capt Nathanial Lee Baldwin who was the first man to send a radio signal out of China. He was over during WWI and assigned to the Russian forces in Siberia. He was a very very proficient Chinese language man and he ~~was~~ the man ~~who~~ that introduced me to the Chinese character dictionary. I'd never been able to figure out how you would look up a Chinese character if you had a dictionary of Chinese characters and he showed me

how and it was a wonderful revelation to me because it's an amazing thing and a lot of people are curious about that even to this day. And in addition there was a whole variety and you'd have to go down through the roster followed on after these folks, Capt King, Henry O. P. King, William O. Reeder and more. This is a good question. I'm glad you asked it because I think I'm going to fill a gap.

Q: Could you give us ~~any~~ your recollections of any significant cryptanalytic successes other than the ones we've already talked about previously?

A: Well I've talked at length about what's been done on the Purple and the Red and the Japanese diplomatic systems, J19, the transposed code. We've had some mention of Tiltman's success in breaking into the Japanese military attaché cipher where he made the initial penetration once we determined what the system was and we set up a unit to collaborate with the UK and we recovered that and that's the one which

DoS we found out (the State Department strip system had been violated) and that was very significant from an intelligence standpoint and we also found out a great deal

about the capabilities of the cryptanalytic organization which we were pitted against, Japanese participation. While it was not a clear crystal clear picture at least it gave us some idea that this kind of thing was going on and a measure of their competence because we didn't quite understand how they'd broken into the strip system and so we gave them credit for more than they deserve but that's a little bit different story. I think the main just to review these for a minute and add on some that I haven't already talked a little bit about, Certainly the work done on the Japanese military systems is a chapter a full chapter unto itself and should be people like Kully should be talked about to fill in that gap. I think it would be presumptious if I tried to talk about the work there. I'd mentioned the GEE in other context and that I think was a terrific cryptanalytic achievement. The principle aspect of it being that we recovered and we learned by experience that we could go behind the use of the system and figure out how the key had been generated. The closest we'd come to

this before was in the case of the Japanese system we had predicted the Red keys for months in advance and also we found out that the Purple keys could be predicted so we were going back into the solving the code compilation problems rather than the use and as a result of solving the what was happening in the code compilation area we were able more or less automatically routinely to produce decodes of messages because we had generated the same materials in effect that the code compilers Japan in terms of the Red and Purple reuse keys and in terms of the GEE we had provided ourselves with those materials you see so all we had to do was to supply them. I think this was a degree of sophistication that had never been reached. I think we reached it before the British did really and I would say this is one of advances we made over them. The now since we're talking about systems and not techniques we were able to recover the German Floradora that was sort of the second the one time pad was the most secret German code and then the Floradora was to the most secret code like our War Department Confidential code was to our War

Department Secret code. It was sort of regular use and it used the same it used a book of additives. It was a two time additive rather than a one additive sort of. That was a significant piece of work done by Kully and his group. We had been under such pressure to get on with the German and Japanese and Italian that we had not gone deeply enough into the other countries for me to claim that we had made any significant progress outside of the three. The Italian code was pretty straight forward. I don't think there was any, unfortunately for Abe, I don't think there was any real extraordinary challenge in the Italian systems. They were somewhat behind the Germans and the Japanese and of course Kully was extremely fortunate in finding that kind of a challenge in the German problem and of course the main thing about the Japanese is that since they used machines and since the Japanese language ~~is~~ was a very fabled one from ~~the~~ a cryptanalytic standpoint because of the real remarkable statistical aspect and since the cryptography used by the Japanese sort of progressed step by step at a time instead of taking great leaps

why we sort of lifted the calf when we got up in the morning and when it got to be a full grown bull like in the transposed code we were still able to lift it. We sort of developed our strength along with their advancement and I think these kind of things are the significant ones to mention. I could have overlooked some because its been a long time since I thought about these but now in addition to systems we worked, there were three other milestones I think might be examined. One was Friedman's conviction that we should automate both cryptography and cryptanalysis and the automation in cryptography took the form ~~to include~~ of improved cipher machines and the automation in cryptanalysis initially took the form of procuring the IBM equipment, the accounting equipment which he deemed superior to Hollerith because it was more flexible and that I think was a tremendous step forward which we achieved under Friedman's direction and then the next step was where we modified the accounting equipment to do special purpose things . . . . .

End of side 1

Tape 5, Side 2

~~Lets~~ Well, go back just a little bit. I think the next big step was the development the modification of the accounting equipment to do special problems like we found in the Geewhizzer and the great advantage that accrued from this development in terms of keeping up to date with the Japanese transposed codes and then this set the stage for some further progress and also for making some mistakes because I think the navy's cryptanalytic equipment program, the old IC machine exemplified by the ~~British~~ Bush variety plus the optical devices the navy had under contract from the Eastman Kodak Company were aimed at doing the same kind of things but the trouble with them is they were designed to deal with trivial problems like matching ~~alephbets~~ alphabets and things which no longer were being used in enough quantity to make ~~it~~ them significant because the type of fractionation system which we had learned to deal with in terms of the ADFGVX was greatly similar to the type of transposition system used by the Japanese in their transposed code systems and so we opened up a whole new domain ~~which resulting in~~ as a result of the Japanese going to the transposed codes. If they'd

stayed on their simplier charts their security would have been about just as good. We wouldn't have had to work so hard of course nor would we have developed the strength the cryptanalytic strength that we developed ~~in~~ from their introduction to these new systems. They just simply paced us up the ladder. That's what they did by their efforts to improve their cryptography and I think we could learn a lesson from that even with our own systems today and forever and any country could learn a lesson from that. I think it's the principle that we need to be aware of as well again its lifting the calf when it is a small creature and then if you keep lifting it and stay up with it no matter how big it gets you can still lift it if you develop the strength (?) of the code. It's that principle. Now beyond that a lot of things happened more or less well let's see what they are. The improvement in cipher machines while we may want to separate it out from the cryptanalytic work really was based on cryptanalysis because we could not have achieved the security that we attained for ~~the~~ US communications, Army and Navy, and joint

without this thorough grounding in cryptanalytic techniques which enabled us to determine what were bad principles and what were good principles and so we could sort out and determine that this type of a machine was a good one. Now we had again some bad experiences like the 228 story that I told but we grew on that, so even our disasters could be turned to advantage. Probably the biggest step forward in cryptography at least from my viewpoint that we achieved was our realization that we had to go to the one-time tape principle which again gives you the total security that you require and that had one weakness which we were distressed by until somebody came up with a simple answer. If you Use the same tape twice the message is ~~laudable~~ vulnerable, so I think Rosen invented the tape splitter. Once the tape went through the head the key tape went through the head it was destroyed. Well this distressed the code clerks and the communicators because they wanted well it meant that if there was a break on the other end you had to use ~~another~~ a new key tape and they didn't want to do that. That was inefficient. You had to have another transmission. You couldn't

go back and use the old transmission. Well we just decided that yes we will spend that effort and we destroyed the tape after it went through the tape head and that's the only way you could avoid the ~~death~~ depth, and once we crossed that psychological accepted that concept psychologically, that there could be no reuse of the tape I think we were in total security, and the only thing to our dis....well which we had to worry about then was the physical security and later on spurious radiation which we didn't know about in those days. Now during the war a lot of good things were done. I think the SIGSALLY was a sort of a milestone. I don't believe it was the greatest thing that came down the pike, but it was certainly A new mode in cryptography because here we were taking the voice signal and enciphering it and I believe SIGSALLY was ~~a~~ indeed a good system and incidentally just about well within the last few months I noted that the patents ~~had~~ have been issued on the basic principles underlying the SIGSALLY which you might want to look into for your archives. This was in a news release. I think it was in the Sunday paper somewhere where ~~it~~ they talk~~ed~~ about inventions and

new things that have come out and it was about three paragraphs and to me it could only be the SIGSALLY. Two other things I think need to be mentioned. We had ignored plaintext entirely until the war had been going on for quite a while, then we discovered ~~a~~ that lot of information. Actually I don't remember how we came to get into this but we finally decided ~~that~~ to setup a unit to examine Japanese plaintext that had been intercepted over I mean ~~under~~ in terms of hand (?) plaintext and this had a tremendous wealth of information and it was probably better than some of the military information that was being produced from G2 about particular geographic areas, I'm sorry by B2, Kully's outfit, cryptanalytic unit responsible for Japanese military (159) ciphers, study these ~~Japanese~~ plaintext messages produced information that just didn't appear in the enciphered messages and this was useful to ~~Rishour~~ Reischauer and his group and this probably will surprise you but we found out how to use an information section, Dr. Ward's group came to age and we found out that by compiling and organizing and cataloging collateral information that we

could save our cryptanalysts a lot of effort and I think some of the messages particularly in the South American countries and Spain, Portugal got a great benefit from this section because the diplomats here in America would encode press reports and if we could find the newspaper clipping that they were reporting on then the codebreaker had an exact text to work from and his job was greatly simplified, so We were able to multiply then our codebreaker's talents in this particular instance by using a bunch of other skills to support him without these skills having to be trained in the depth that the codebreaker had to be trained so we were dodging the training program that we would have had to employ had we gone ahead and tried to recover the text of the message by brute force but to have the crib in front of us was a very useful exercise and I don't believe in any of our discussions here that I've had with you I have mentioned the importance of this collateral information to you (?) [bit] and while it isn't technical in nature ~~if~~ it certainly was a valuable thing from the standpoint of speeding up our production of information

in achieving the solution of ~~the~~ difficult systems which otherwise might not have been ~~obtained.~~ attained.

Q: Could you describe the relationship that Captain Hastings from, the British ~~Colony~~ COMINT rep in the U.S., had with the SIS?

H.S.

A: Yes. I can tell you something about it. This was Capt Eddie Hastings who was on the directorate level at GCHQ and very close to Travis. He came over I think the purpose of his first visit was to take a look at the American activities the Army and the Navy in particular and maybe the FBI. I don't know whether he got involved in with the FBI or not but sometime after Dennison, who was the first of the British COMINT types to come over, Hastings came over and went almost through the same course that Dennison had gone through. He spent more time I believe with the navy unit, the OP20 G group than he did with the SIS but that probably was because as I recollect he was a captain in the British navy at one time but we showed him roughly what we had showed Dennison and I probably maybe a little bit more because Dennison was pretty tired and a bit of a sick man when he came over and I don't

think he personally enjoyed these liaison trips because he felt uncomfortable and distrusted the .... He was a very friendly guy by nature but he just wasn't cut out to be to do that kind of a job. Eddie was Eddie Hastings however was a lot more outgoing than Dennison and consequently I think got a little better reception particularly since we'd found that Dennison was not a menace but a friend and then we opened the doors at least more cordially, whether they were opened wide or not for Hastings. These are general impressions I can recall of his trip over. He was played quite a role in terms of the policy actions developed in GCHQ and probably had as much to say about the liaison arrangements as anybody else on the staff and I'm sure his purpose, the purpose of his visit was to make an assessment of the two U.S. units that they were going to have to collaborate with and this assessment included the COMSEC aspects as well as the SIGINT aspects. I think his role was more of an advisor to Travis and to the London SIGINT board or whatever the ~~London~~ board was at that time because he was a lot less responsive to technical explanations than

than Dennison who was a damn good, a very skilled technician. Hastings was not. He was more of an administrative type. At least this is my impression of him and if he was a good technical man he certainly concealed it very well. He was we found him a man easy to deal with. Reasonable. When there were points of differences that came up and one of the biggest points of differences which I think probably disturbed the British but which they made no noises about was the U.S. absolute refusal to reveal anything about a U.S. crypto system. We just that line was drawn for us that you will not give any information to the British about these things including our machine ciphers. ~~Exxxxxx~~

Q: Who made that decision?

A: I don't know whether it was made at the Secretary of War level or not but I know that both the Chief Signal Officer and the Director of G2 were in complete accord on this and well for what its worth I thought it was a very prudent decision. I just didn't feel like that it was called upon us to expose our own crypto techniques because well just bluntly some of us knew we were going to win the war and we

knew that the British had a good cryptanalytic organization and we knew that if we did win the war they would be on the winning side too and we were inclined to believe that the collaboration might well continue after the war and therefore why give them a leg up on entering American communications because at that time we didn't see anything else on the drawing board to replace the systems we were using. We had just reached about the maximum that we could visualize at that time in terms of the state of the art, ~~in~~ efficiency, and we thought well we'll be using rotor machines, that'll be the big thrust for American cryptography and why tell them some of the more intimate details of it. Now this endured ~~to~~ till almost the end of the war. I think it was an accidental exposure of an ~~ABBA~~ ABA to the British. Of all the people it was John Tiltman and I think John was very honest about it. He came and, as I recollect this if it was John Tiltman he did come and say that he had seen this and he wasn't supposed to but he wanted us to know about it, Displaying (?) Plain good personal faith and good GCHQ faith with the Americans

and of course there wasn't anything else except ~~except~~ it ~~was~~ John Tiltman that came and told I believe he told Friedman and me about it. I'm a little hazy on who the individual was but I know he was a Britisher. On the other hand the British and Eddie probably had something to do with this decision, quite freely exposed us to crypto systems they were using and I rather suspect at the time hoped that we would relent and reciprocate but we never did and there was one instance though-- ~~that~~ I've got to reminisce a little bit about here because its a personal thing. When I went over the first time the Travis you know told them to show me what I needed to see and among the things that I was shown I was known as being very deeply involved in COMSEC at the time. As a matter of fact I represented the Signal Corps on some of the COMSEC discussions that we had in terms of joint combined communications and how we would meet the combined communications requirements and so I was recognized as being sort of a COMSEC type. Well the British at that time had under development an automatic teletype enciphering device and I got shown this

quite by accident, and I found it extremely interesting because it was the only thing that I had seen in the UK that seemed to me like was up to the state of the art. It was a beautiful job and there was no damage done really because it was only a matter of a few weeks until they ~~began~~ were going to expose it to us anyhow because they wanted to use this device for enciphering COMINT material. It was fast. I think Winterbotham ~~in~~ and his outfit needed something faster than motorcycles. Travis's remark when he found out about it was "Well why did you have to show it to Rowlett? You couldn't have picked a worse guy if you wanted to keep it a secret" because that was my field you see in those days. Been worse if it had been shown to Rosen of course. Now Eddie Hastings continued to be involved in the policy aspects of our collaboration, both sides, COMSEC and COMINT, probably until the end of the war and then this happened as we got closer and closer in collaboration with the British. The policy lines were pretty well laid and most of the interchange was done on the what we always called the technical level if that has any meaning

but there was face eyeball to eyeball technical exchange and that was where most of my interests lay so I didn't see too much of [Eddie] except at international conferences, things like that because he sort of moved out of the picture and I think he was ~~many~~ handling other things for Travis because he had come into this as a sort of special assignment quite possibly.

It might be interesting if I reminisced a little bit about my understanding of how advances were made in cryptology and compare in this discussion the SIGINT world or the COMINT world or the cryptanalytic world with the COMSEC or the cryptographic world. The I'll have to do this a little bit haphazardly I think because we've got to jump from one to the other and keep the timeframe moving along because this was a bit like a rail fence. The center of gravity shifted from one side of the timeline to the other side so we'll go into the COMSEC maybe and then into cryptanalysis but I think the and I will start with 1930. The advance at that time the big advance was in the field of COMSEC. This is the thing I noted because on the drawing board

was Friedman's idea of the M134 and contracts were being let to have this device constructed and it was to be tested out by issuance to the three overseas departments. As I believe it was had just a few devices built. COMSEC records can tell you ~~that~~ how many. Now this device and I am going back a little bit, this device resulted from the work Friedman did on the Hebern machine which is covered in the technical paper which describes his attack, successful attack, on the on that machine. Now in this device ~~it~~ incorporated the defenses against the weaknesses which Friedman had discovered in the Hebern machine. It was basically a Hebern device, a five-wheel device, and the reason there were five wheels in it is because there were five holes in the teletype tape and the idea was to issue ten wheels and they were reversible wheels so in effect you got ten basic wheels and ten other possibilities so it gave you something factorial ten to factorial twenty in terms of the wheel selection for a given day's traffic. That was quite a numerical advantage. The way Friedman had arranged these wheels was to avoid the

sort of simple minded and most fortuitous case of a wheel ~~slipping~~ stepping against an endplate continously one by one because it was this kind of a an arrangement of the selection of that wheel the moving wheel the constantly moving wheel of course in the Heb~~ron~~ern it was a meter-like motion against an endplate was the thing that enabled the statistical evidence to emerge from the cipher text and you could determine this by making the right kind of frequency count so Friedman recognized this and he destroyed that attribute because ~~this~~ his tape caused the wheel to move erratically even though it moved only a step at a time you didn't know when it was going to move and that was important and that was enough to smear the statistics in the small amount of traffic or counts that you could make from from the traffic intercept that was ~~essentially~~ potentially available so these are the kinds of things that Friedman overcame when he began to build his generation of the M134 and we called it T1. Now keep in mind that this ~~is~~ was on the drawing board. Now when we got to work we'd go over on the other side of the fence, because we examined we repeated Friedman's

exercise on the Hebern and then we went into other machines like the Swedish machine, the Damm machine. I believe that's a B211 isn't it? Number just comes to mind right now and we found out a little bit more about that. We as I mentioned earlier had looked at the Enigma the commercial Enigma that Friedman had bought and we looked at a bunch of other things the Kryha is one of them. The strip well the cylindrical cipher device, Type M94, that was more or less an exercise in repeating what Friedman had already done because he had been very successful in obtaining the solution that and so we began to build up a feeling for machines and how to deal with them and then this set the stage for the real advance and that was when the Hebern Mark II was developed and the navy sent it over for us to the same kind of a challenge Friedman had except the machine was so much better we had to have more traffic so that the amount of material we had to work with was greater. I think the conditions were not as difficult as they were in the case of Friedman because they gave us the wheels. What we had to do was identify the wheel

settings because ~~at~~ by that time we became aware that mature security consideration was that the enemy would capture the machine with the wheels and the problem was reading the back traffic. ~~If~~ If you could remedy the situation by issuing new wheels and using the same machine but you couldn't do anything about the traffic that had already been transmitted and intercepted so we postulated that the wheels would be known and I think this was the main difference between our work on the first Hebern ~~Hebron~~ and then its ~~this~~ successor. The successor was also designed to avoid the constantly moving wheel being located next to the wrong endplate because I don't remember whether it was plaintext or cipher endplate right now. I could think about it and decide considering what the logic of the attack but the there was no wheel next to an endplate that moved constantly. The constant moving wheel I think there were two wheels which moved constantly and then the other three moved erratically and that was a much better keying principle than we found in the previous model. Now at that point in time I think we advanced a little bit in our cryptanalysis.

It may not look so to people who are dealing with the more sophisticated machines today but in those days that little step ~~is~~ was measurable because I think we were getting closer to the practical considerations that had to be applied in assessing our own cryptographic security but I think the next step forward and this gave us more confidence than anything else because sure we were applying what we had learned to ~~the~~ machines, about machines, to live traffic to produce intelligence and after we got started on the Japanese we finally isolated out the Red traffic and we got to work on that and when we saw the Red machine, that was a big step forward on the cryptanalytic side because it took the I mean we felt confidence as a result of this because we had been successful and because we'd gone through the veil [of] secrecy that communications the cryptography that had wrapped up the Japanese message we'd penetrated that, and brought out the underlying device, actually reconstructed it, based on what we had learned in our previous work and what Friedman had taught

us and we just went in and solved the machine without a knowledge of its mechanics or how it operated and we needed that at that point in time because we sort of felt like we had grown up. We can now start drinking and smoking you see with impunity we were grown up cryptanalysts and that was a big step forward. Of course I'm condensing a lot of work into just one little package and just pointing at the milestone but it just took a lot of climbing for us to get to that level and then we began to ~~pull~~ fold back some of these concepts into our cryptographic world and I think I mentioned this morning the transposition encipherment of the War Department Confidential code and how we proved that the this was not a secure system based on our examination of actual material~~s~~ which had been transmitted and that gave us also confidence because we felt if we could take War Department traffic which we had not, which had been honestly prepared in the coderoom and transmitted, this was the real stuff, and we could break it then we were still pretty good you see and I think this is an example of where the product well our cryptanalytic skills caused

us to move forward in, not the development of new systems but in the rejection of systems ~~were used~~ for use within the War Department communications structure and that's just as important as finding new ones. ~~Of course~~ if you reject them all of course you've got to find a new one but if you got a whole bunch and you're using a bad one the sooner you discover and reject it the better is your security and in that context this ~~is~~ was a step forward. I think the effect was more psychological on us and the Chief Signal Officer and the people in G2 who knew about this than it was a material one but again when we are in the business of using codes and ciphers the psychological element seems to dominate and override the technical considerations because people will continue to use bad systems simply because they don't realize that they are bad or they refuse to admit that they are bad and we of course found out that it was better to admit that they were bad then to continue to use them for whatever reason and that hadn't been recognized by us before and may sound real stupid and foolish as I talk about it but it meant a lot to me

because I was there. I had the attitude. I became converted. I became a Christian and so I worshipped at a different altar from then on and in that sense it was a real thing ~~for~~ to me. Now probably the next step forward was in the development of sort of well it was the Friedman's model of the M134 used the tape for the for the keying element, the motor key that set the wheels forward, to put it in crypto-graphic terms. Well this is the thing that ~~impressed~~ distressed me because I was making the tapes and it became clear, I think to all of us who were involved in this thing and of course somewhat of a disappointment to Friedman because he had hoped that he had solved the problem but when he found out that we were having all sorts of ~~problems~~ trouble with the tape production that was an essential part of the use of the M34T1 we had to devise other techniques for advancing the wheels and that's when we used we we discovered and accepted the rotor principle as being the generating mechanism or means for advancing the cipher maze wheel and I think this ~~is~~ probably was the most significant step forward in COMSEC at that time because for these reasons. The

navy since we had destroyed their faith in all the Heb~~ron~~ern machines, were seeking a device, a mechanical electromechanical device, that would satisfy their fleet requirements and their ship-to-shore and shore-to-shore station requirements. They didn't have anything ~~to~~ that suited them. They had a lot of things on the drawing board ~~that~~ but it ~~there~~ just wasn't anything that was good enough for them and they were dissatisfied with what they had and they were still looking for the ultimate so there was a hunger on their part. On our part in the army we had the same requirement~~s~~ that Friedman was trying to satisfy with his M134T1 but we had rejected the M134T1 because of the tape construction problem and we had to go to this other means of key generation which was simple and much more desirable because it avoided storage and issue of a lot of keys and you could have a small package with same ten wheels you see generat~~ing~~ed both the key and performed enciphering maze so your keying was simplified and your distribution of materials was simplified, certainly the physical security problem of storage, there was as much volume

and about all you had was the maintenance manual and a key list and instruction book and a set of wheels and that was it. Now in the old tape method or additive method you had to have enough additive~~s~~ or tape to satisfy the volume requirements which would be generated on that circuit, well more than enough to satisfy them because you took the optimum and then had a cushion ~~which~~ that you chose. Well the two requirements then meant that something had to be done and as a result the army and navy joined together. The navy took the quote million dollars unquote quote no year funds unquote they had for cipher machine development that somebody once said Franklin D. Roosevelt had gotten for them when he was Secretary of the Navy and I believe that's true but it needs to be verified. They had the money, and now I'm going to brag, we had the ideas and so we provided them with the ideas, they provided the money, we let a contract, the first contract was navy and the second contract was army, the follow-on contract was army and so the M134, I think it was T3 or T4 the ~~ABBA~~ ABA or the ECM, lets change our nomenclature now, started to come into being.

Now I'm talking about this like it was just a matter of a few days but it wasn't. It was more like several years. Just an observation on this ~~other~~ point. You know it was a tremendously fortunate thing that the army and navy both joined together in the development of the cipher machine in those years because imagine if the navy had gone ahead with one of their versions and suppose they'd ~~b~~bought a ~~and~~ modified or and improved Heb~~ron~~ern type of machine for naval use and suppose that the army likewise had gone ahead and developed the M134T4 or ~~ABBA~~ ABA then we would have had two unique machines for use, one in each service. The this would have been allright in peacetime but if you can imagine a wartime situation where joint communications are certainly required then it would have meant that one service would have had to accept the other's equipment and that the other service would have had to provide the equipment and then you could have three systems and the same message might go in an army system, a navy system and then ~~a~~ the joint system and this is cryptographically unsound but fortunately the joining together and using the same device

and the way the machine developed you could achieve new keying or separate keying simply by reordering the wheels or setting out a new set of wheels. The same chassis could be used and all you had was a box of wheels and the keying instruction to effect well you needed three of those. One for the service, the army, one for the navy and then one for joint. Now later on when we got in with the British and this ~~is~~ sort of an incidental advantage of the type of system that we were lucky enough to have was that the type X machine could be simulated using a special set of wheels ~~in~~ on the ~~ABBA~~ ABA chassis _____ pretty simple. As I recollect one of the solutions which we discussed was instead of having an endplate we just had a reverse set of wheels but anyhow we could use the ~~ABBA~~ ABA chassis and Type X wheels and we didn't have to provide the British with ~~ABBAs~~ ABAs, our device, because the ~~ABBA~~ ABA chassis and the special wheels we wired up with the special motion provided a better machine than the Type X itself so it was a needed improvement on the mechanical version, the electromechanical version

of the Type ~~X~~ Typex which the British were struggling along with. Incidentally I've seen some of those in operation and I of course I was conditioned to by American technology and the British cipher machine technology at that time was different, they looked like they were clumsy things to me and not very well engineered but they were reliable and they did get the British through the war. Now the luck was that when Pearl Harbor was hit these ~~ABBAs~~ ABAs were just coming off the assembly line up at IT&T and the first ones which were intended for the ships in the fleet were just ready to be being packaged and sent to Washington. Well you know what happened to the fleet and you know that at that time the army started mobilizing and we needed cipher machines in a hurry so what we did instead of putting the first machines and sending them over to the navy as was our plan, had the war not started, a decision was taken to give the divisions, this is when we used the division level an army communications center ~~at~~ in the War Department Headquarters center, the first machines that came off the assembly line and all ~~they~~ we had to do to modify those machines for army use was

for somebody to take a little bit of a nice cold chisel and a hammer and go down and knock the nameplates off the Navy ECM, the nameplates off, which is a little metal or plastic thing and the other guy would come back and [illegible] on the army nameplates and then instead of the army waiting for the next batch the navy the next batch of course with the revved up production requirement the navy was quite willing to take the second batch. Now this was just sheer luck because we went into the war with a good cipher and we I think found out later on that it was not ever violated or compromised by cryptanalytic purposes. I think the one that was lost at the Remagen bridgehead gave us a lot of worry but they found that thing in tact. I think it was a pretty lucky thing and I do believe this was kind of a wonderful corner of the rail fence that I've described here in terms of the advancement of American cryptography. Now mind you this took about six or seven years so you can't identify it as a particular piece in time but it's sort of spread over the years and it involves a lot of things that went

on before.

Q: H.S. Hanna Utpatk [redacted] the 134Q1 except for a different rotor mechanism.

A; Well we can look on them as generations.

(Light)

End of Tape 5, Side 2

Done 31 Aug 76 (?

6-10

Tape 6, Side 1

comparison of advances or really consolidation of advances in the two fields

The one of the most signifcant things that happened was ~~that~~ Friedman's first

efforts to mechanize the business of cryptanalysis. He was aware but not too

familiar with the nature and operation of ~~Hollerith~~ the Hollerith system and the IBM system. He

assessed the things accurately. The two initially because of the greater

flexibility of the IBM and he set himself out a course of action aimed at pro-

curing these devices for our to assist us in our cryptanalytic work. He also

had visions that they would be extremely useful in our code compilation program

and since he learned enough about them to establish how they could be used in the

code compilation problem he was very persuasive and finally managed to get a

small unit made available to us so we could do some testing of it. Actually this

unit ~~their~~ the first efforts were not on machines that were in our area but they

were in other areas and I ~~remember~~ working at nights with equipment that had been

rented by other well Quartermaster Corps was one and we used to get permission to use this equipment on the swing shift when it was sitting idle for our testing purposes and so we worked both day and night in those days preparing the materials ~~for~~ on the daytime and then go in for several hours in the evening, use the machines and then come back and sort of make an estimate of what we had achieved the night before and ~~we had~~ lay out our program for the next few days and carry on until we had completed our assessment program of their advantages and actually tested them on the problems, live problems that we had solved and the first thing I think we did worthy of mention was we punched a set of cards with the code vocabulary ~~with~~, the plaintext vocabulary for a 10,000 group code known as the Division Field Code, and the first one we produced ~~in~~ was the training edition. We did this because it had to be done outside ~~of~~ the area, the controlled area, the vault area that we were working in and we thought for security purposes we'd go ahead and get the vocabulary punched out and then run off the first version and see what we had to do to produce

others. Well this was a terrific thing that happened because once the cards for the plaintext vocabulary, ~~or~~ the 10,000 cards, had been prepared we had a deck of cards and all we had to do then was to get the code groups somehow or other punched on these cards in a random ~~way~~ way and or to say more simply scramble the cards, punch the codegroups on them and then re-sort the cards. You can get one version and if you sort it on the plain language it's the encode version, if you sort it on the codegroup it's the decode version. Well I have a suspicion that we scrambled the plain language groups without numbering them to start with and so when we we had put the codegroups on in logical alphabetical order we also had numerical equivalents associated with these literal groups and we ran off then well the process ~~is~~ was this. Let me just go step by step. First thing you did was to get a manuscript of the 10,000 plaintext meanings that you wanted to include in the code. The next thing you did is you punched a card for each one of these. The third thing you did was to assign these meanings to your code vocabulary in

some haphazard random or otherwise unpredictable order and I think the precise word here is unpredictable because it might be non-random and non-haphazard but the idea was to confuse the cryptanalyst so I think the proper word is unpredictable fashion. Use the se value cards through a sorting process to prepare the two versions then forget the codegroups element on the card, rearrange the cards in a logical order and well in a useful order, they don't have to be alphabetical but get the cards set up in such a way that you can control the next step which is the punching of a new series of codegroups on the plain language cards and then through the process of sorting and printing you could produce version, edition No. 2 of the code and then repeat the second process for as many times as the area on the card will permit you and then you can use the same deck of cards for producing several codes and when you run out of space then you wire up the plain language equivalents and reproduce them on another set of cards and if you're real smart you will have done this before you messed up the cards with any other

extraneous information on it and I remember what we did essentially was to put together the plaintext vocabulary, then we scrambled it, and put ~~on~~ all on (?) the codegroups in order and then we had to resort on the plain text and since these groups, the plaintext equivalent, sometimes had several I think we set an upper limit of somewhere in the 20's maybe 25 as the longest phrase we could put on there. We had to sort over 25 columns and we wondered how stupid we could be after we got involved in that but it was too late to do anything about it because all we had to to sort number these 10,000 serially in alphabetical order and then you could make five sources instead of 25 well it was really more than 25 because a numerical sort is a one run and an alphabetical sort is a two run so 25 times 2 as opposed to 5 times 1 is quite a time factor. Well the little pitfalls like that. I mention ~~that~~ it because we were so happy to have these things we sometimes didn't sit down and contemplate just exactly step by step what we wanted to do. I don't know whether this is too bad or not because we certainly learned a lot of hard ways to do easy things (laughter)

by this somewhat thoughtless approach. Well the first code came off and that was a surprise but the real payoff came when edition 2, 3 and 4 came out because it was very little clerical effort. It was purely a mechanical machine operation and printing the sections with the IBM tabulator and the question was can the printing office use this IBM run as a manuscript and when we found out that they could the code production problem suddenly took new and less awesome and frightening dimensions because a lot of the things we were doing were so time consuming because they had to be done by hand, the machine was doing automatically for us, and we still didn't get away from the final check, cross-check you see, to make sure that somebody in manipulating the cards didn't slip or the group was misrepresented. The final crosssec... crosscheck, encode against the decode, still was necessary and we didn't solve that for quite a while. I don't think we ever satisfactorily solved it because we went on to other things and we got out of the code production problem. So the Friedman's adoption, the realization of his dream of mechanizing

part of the cryptographic cryptologic activity, was proved almost immediately or within a short time period once we got the machines, and the demonstration was so persuasive that he had no trouble in getting the funds for his own installation and we had a very modest one. We had I think two punches, one sorter, one reproducer and one tabulator and as I recollect -- this may be borne out by some of the documentation -- that we were forced to order the cheapest printer but IBM didn't have one of the cheaper ones so they provided us with one of the more up to date ones. A simple printer wouldn't do all the things we needed but when Friedman wanted a bigger one I have a feeling that IBM was just doing a good bit of company PR so they gave us ~~a~~ the big one because they figured ~~that~~ later on that we would buy more and they didn't want to prejudice their rental proposition to us by giving us one that wouldn't be adequate so I think they very cleverly gave us ~~a~~ the big one in lieu of ~~a~~ the smaller one. I use big and small in terms of plugboard counters that were contained in the machine and some of the

refinements that they had built in to the newest model so we got the newest model printer for our installation. Well now this opened up a new training program, to get a little bit personal here for us, because there was nobody around. We didn't have any clerical force to operate the machine so guess who got the job. Abe, Kully and Rowlett, and Larry Clark came in and then Sammy Snyder came in later on and he sort of specialized in the use of these machines but all three of us got a pretty good indoctrination in the use. We could ~~work~~ wire plugboards. We could even use, I could use, the keypunch and I did and I often punched up my own text, made the cards, ran them through and had the whole deal just like a present day computer programer will run his his whole project. I mention my experience with it [redacted] because I think it was typical of all three of us. Now what about the use of these machines in cryptanalytic endeavors. I've talked I think enough about what we did in the code production program and I just might add that when it came to developing cipher tables and key tables and things like that the

IBM machine could be utilized in lieu of the hand methods we were using so we got away from a lot of the drudgery that had been bogging us down in our code production program as soon as the machines came in. Now the lets talk a little bit about ~~the~~ cryptanalytic use of the machines. Probably the first big problem we used them on and I there may have been others but I do remember this one and let me put it this way, when we got ~~the words~~ to work on the Red machine, when we'd isolated out that batch of traffic and started a full blast attack on it we had our IBM installation and it was freed from its code production program to do whatever was necessary in the analysis of the Red machine and we of course were kind of stumbling around and fumbling in the dark because we didn't really at that time appreciate the capabilities of the machines so it was a learning process for us and I think the work on the Red system where we had to do certain frequency counts and other things to satisfy our statistical problem, helped us ~~to~~ appreciate what these machines could do. Now it actually boiled down to this kind of a situation.

I want to hurry up and put it in this context that while the machines were useful in working on in our recovery of the Japanese Red machines we would still have done it without them, so they weren't critical, they were only useful and it wouldn't be fair to say if we hadn't had the accounting machines that we wouldn't have read the Red machine. We would have and we could have read it sooner than we did if we had time to work on it and this was even before the accounting machines were available. Now I think ~~that~~ the accounting machines the next significant well probably the first significant contribution the accounting machines made in cryptanalysis was in the work Abe and Kully were doing on the Italian and the German systems because this well let me describe something. The catalogs that Yardley described in the Black Chamber that his people were putting together for the recovery of the Japanese codes before 1930 could easily be produced by processing the cards through an appropriate program in the accounting machines so the number of personnel which would was required to work on the Italian and the German problem was cut

back because we had the machines available to do this for us, and there we found out that the machines on those two problems the machines were vital I think and as I said they weren't vital for the Red machine but they were vital in the code recovery program and the key recovery programs that were involved in the German and Italian work and that is where we found, we proved that the machines were indeed valuable for cryptanalytic process~~ing~~es. Going back to the Japanese problem which I know more about than I do the other two and I feel easier talking about it. Each time we had a code change in the Japanese of course the machines were invaluable because it did the cataloging work for us and since the Japanese codes were less involved and had a fewer number of groups to recover we didn't take long and it wasn't nearly the drudgery and didn't require the tremendous cataloging process that the bigger codes in the Italian and German section required and so we usually interrupted the other work enough to provide us with catalogs for the Japanese codes. These were very short interruptions because it didn't take too long to recover the Japanese codes. The greatest use though of the IBM

equipment we found in the Japanese section was in the preparation of the frequency data and the work sheets in the Purple machine solution. This, we standardized our format and so you could go from one indicator to another indicator and not have to make an adjustment and your statistical data was all pretty well organized and I would say that the accounting equipment was critical thing in the solution of the Purple machine even though it was useful in the Red we couldn't have done the Purple without the or if we had it would have been more like 36 months instead of 18 months so by now you can see we're dedicated to the accounting machine~~s~~ as a cryptanalytic tool but now we're ahead of the computer stage. The most dramatic thing I can recall in that time frame is when we were confronted by this Japanese transposed code system. Now the Japs had been using a sort of a primitive transposition system for special messages. The office chief eyes only ~~kind~~ type but this was a sort of seven element transposition so we usually deciphered it by writing the groups out, five or seven or whatever the key link was and then simply

reordering them without even putting them in a matrix. They were so short.

~~Well~~ But now when they put in this J19 concept, that type of code where they used ~~the~~ a key 15 to 25 elements in length the matrix with the certain of the upper lines crossed out and applied the transposition key in the conventional transposed position type operation, the problem got to be extremely difficult and the Japanese group of course was confronted with the recovery of these keys in ~~the~~ a proper timeframe. We found, we developed, a hand method for doing this that was I think very clever and very useful and ~~I think~~ very good but what we were doing, it was taking a small force available, this was Albert Small and Bob Furner, myself and Mary Joe Dunning and ~~Jean~~ Gene ~~Grotelen~~ Grotjan?, later ~~Jean~~ Gene Feinstein, and a few others whose names I, whose faces I can see but whose names I can't remember right now. We had ten or twelve people working full time on trying to recover these keys and the recovery-to-use ratio was about one out of six so we were falling back five feet every time we climbed up one. We weren't getting out of

that hole going in that direction. So what happened as I recall Friedman was not too deeply involved with us. I think he was having some some his health wasn't too good so he was not ~~really~~ being as deeply involved for health reasons in our activity as he wanted to be so we were confronted with the problem of devising some better way of recovering these keys because we certainly weren't going to completely satisfy, we weren't going to achieve, the total exploitation of the traffic that we had trained G2 to expect because we had been doing it before and that distressed us and distressed G2 more than that and distressed the Chief Signal Officer so we were all unhappy and since there was nobody around that knew more about this problem than Furner, Small and Sammy Snyder and myself we decided we'd put our own work on it and just let the folks we'd trained to do it mechanically. I mean the junior, the cryptologists, cryptographic clerk type, go ahead and do what they can and help them when they ran into a snarl and we would devote all our cryptanalytic skills to devising a new way of recovering the keys. I'm

dragging this out a little bit because I'm trying to show that we had to have a motive for doing this before we would undertake the research and the motive was the necessity for recovering these keys in a shorter timeframe and we didn't have enough people to do it and we couldn't expect to get enough people in and trained in time to do any good so we had to go to something new and much more efficient with the result that we began to explore what we could do in (1) improving the statistical tests that we needed to make to do the column matching to get the key recovery to see if we could adapt the or any way use ~~the~~ this accounting equipment to facilitate this operation and (3) to discover other techniques and advantages in our statistical activity which would sharpen up the key recovery operation. Well in this in this endeavor I think the team Small, Furner (FERNER), Snyder and Rowlett sort of again formed a composite where we each put in our own, our own specialities. I mean it wasn't one person dominated. It was where four people joined together. Sammy was, Sammy Snyder was very good for going down to

DOCID: 4223202

the machine room and producing a very, a most reliable IBM treatment of whatever data you gave him ~~for~~ to process. Small was sort of he he lived with the machines and he sort of was the new idea man to develop new programs using the machines and Furner FERNER was just a doggone good, and cryptanalyst and mathematician and he could take Small's sort of brilliant glimpses and reduce them well not reduce them but convert them because he enhanced them, he didn't reduce he enhanced these into practical applications and he made them real. He'd sort out the sort of glint in Small's eye and he would come out with reality and I guess my role was more that I encouraged and I helped and I had a certain ability with my hands. I could produce things, so among the four of us I think we had a pretty team there. Well without going into the details of how this was achieved the four of us contrived a program which we thought could be satisfied by the machines but the missing thing was someway of converting the text into a special presentation machine. We had to have something more than the IBM machine is what I'm saying before we could

do this. Well where do you find this thing because in the first place you don't go and bring in a bunch of engineers and tell them you working on Japanese codes because we'd have to tell them that and the second we weren't quite ready for this because we didn't know really what we wanted and the third we probably knew much about the theory, ~~and~~ the wiring and the logic necessary to produce some kind of a mechanism as anybody else in the world, certainly more than anybody else that we knew about so we kind of ganged up and figured out what kind of operation had to be satisified and we took advantage of the spare parts box for the Purple machine which had been built at that time and we devised a sort of commutator-like device which was essentially a well a half-Hebr~~on~~ern wheel like we used in the Red machine which we had the parts to build ~~at~~ that, but the logic behind it was essentially different and I remember taking these parts home over the weekend and wiring them up while my wife was in the hospital giving birth to our second child. I was babysitting the young fellow. Now I mention this very personal thing because these are the

people who did that. I mean we had to do them sort of under ~~the~~ those circumstances. I'm sure Small sat at home and burned up ream and ream of paper trying to figure out the right kind of way of presenting the data to the machine that, the accounting machines, and I'm sure Farner spent similar time and I'm sure Sammy did because it was a sort of 24 it was a preoccupation with this thing and once we got the thing working and tried it out and it did do what we hoped to achieve we refined the our very primitive thing after naming it the Geewhizzer and put it to work. Now this I think this is a very exciting thing that I was involved in and I get a little emotional as I think about it because we could see the frontier move. We climbed up on top of the mountain. This was Alexander Spotswood and his boy looking over the confluence (341), and we got up there and we didn't stop like Spotswood did. We didn't announce that we'd open up the west. We went down and we saw what we had uncovered you see. Now another exciting thing about this, and I'm really spreading this out too much but I've got to say this ~~and~~ to

get it out of my systems sort of, was that the navy also was working on this problem and when they they had been watching with interest our experimentation but (1) they didn't have equipment dedicated to cryptanalysis which we had and (2) their cryptanalysts hadn't been pushed as close to the accounting machine application as we had and so they sort of looked and wondered why we were doing this because they didn't really didn't understand and while they hoped we would be successful they didn't really believe we would be. This was sort of the attitude that I think they had and I'm not saying this in a derogatory way, it's just the way it was in those days. Well when we began they really got religion ~~and~~ when we began to recovering keys at about four times the rate they could and we were recovering keys that they actually could not achieve by their own techniques and then they came over and wanted to know how we were doing it and could they have a Geewhizzer sort of. Now I'm oversimplifying this because it went over a period of about two weeks but I think this endeavor on our part

encouraged the navy to make a greater use of IBM equipment and to undertake with new vigor an enhancement of their cryptanalytic equipment program. This is the IC machine, that I mentioned earlier that Bush had put together for them. I think it led them into this optical system contact that they got into with Eastman Kodak and set the stage for a lot of navy talent to be directed into the cryptanalytic mechanization area and so this and I'm bragging, and I don't care if I am, this lucky result of ours in terms of Geewhizzer I think put the whole context of cryptanalysis in a brand new light. It could be mechanized and mechanized successfully, and that great advantage could accrue from devising programs and special equipment to do these cryptanalytic processes that sometimes had been considered impossible because of the manpower and time requirements.

H5 Q: What date are they? Right there.

A: Look up J19. I could tell you but I'd have to think and I don't feel like it.

Q: Must be 40, 41?

A: It was after the Purple. It was about a year and a half before Pearl Harbor.

(Oh, okay)

A: Who's got the Geewhizer z paper ?

Q: We got it

Valakp

. You might like to see it.

A: I would. I'm real curious about that. Now is this what you want Henry? I'm rambling a lot.

Q: Yes, That's fine.

A: We rambled a lot in those days and I guess maybe...

HS Q: Well this was the only thing I was trying I was trying to put it in a date somewhere. I knew it wasn't after 41. It had to been before the 18 months in the Purple went from what 39 to 40 so it was somewhere in there.

A: When you're ready I'll start recording again.

(small talk chatter)

QX I think a few more comments are ~~germain~~ germane to this development of this Geewhizer z because it sort of indicates just where we were with reference to the rest of the cryptanalytic parties we were associated with. I talked a little bit about the navy. What about the British? Well finally when we started to collaborating with the British I think they found this Geewhizer z a most amazing thing because

we were doing things you see that they had hoped to be able to do but they hadn't as yet mechanized with all the wonderful research and development that they had done on the Bombe, ~~but~~ still that was a different kind of a cryptanalytic operation and the Geewhizzer just opened up a whole new approach and I got to brag about Small a little bit here because his idea of using logarithms which, a logarithmic equipment for the statistical element was a terrific thing because instead of having to multiply the probabilities which were involved in our computation done by the equipment and which would have been impossible with the accounting equipment. Small's proposal to use the logarithmic method? meant that you could add because the true probabilities are measured by the product of the prospective probabilities and not its a product relationship and not an additive so we we he devised tables which converted the well I'll call it the absolute as opposed to the logarithm expression. He devised tables where we could make a probability measure of these things and instead of using converting them back these

tables I mean converting them back to the absolute phase these tables were adjusted so that we could go directly to the logarithmic value and of course its a pretty obvious thing after its done but before somebody invents it you its quite another thing so Small was able to do this. Now a little bit about what other people did. When Verkuyl, the Dutchman, came after the war had started, we found out from him that he and his units had ~~saw~~ solved some of these transposed Japanese diplomatic messages but they were using the very primitive methods that we had developed and both the army and the navy were following when the system was first introduced and I know I was a little bit put out by this if I can again be ~~exponential~~ forward because I had to accept Verkuyl in my section against my better judgment and my logic at that time was not sharp enough to envision that Petersen's defection to the Dutch that later on occurred but it was simply a ~~detective~~ protective instinct that I was following sort of based on lets don't tell the Brits about our own cryptosystems and I just didn't see telling this Dutch officer

about our techniques for the solution of the Japanese transposed codes because what we had was so far ahead of what he had and you can imagine how anxious I was to learn what he knew about this so I could make the measure. The judgment obviously was that we were that we had something that they never could have achieved. My instinct was protective and Friedman joined me in this and the Chief Signal Officer thought this is the way it should be done ~~and~~ but G2 turned him down and said we've got him. We promised him. Our relations with the Dutch, diplomatic, ~~and~~ such ~~and~~ that if we don't use him, if we reject him that we may antagonize and otherwise ~~make~~ may generate problems elsewhere. Well of course G2 was a little bit in the drivers seat so we had to accept him. I wish to the Lord ~~that~~ I had I don't think the Peterson thing did as much damage as everybody thought it did but still it could have done that damage and I wish that our first instincts and impulses Friedman and I presented had been accepted and acted favorably on. The French knew about the Japanese system, I learned later but never did break into

it. This was Col. Black and his people. I don't think anybody else anywhere in the world had achieved that particular degree of sophistication in that particular type of statistical approach and so I believe there is one of the significant milestones ~~of~~ both in the production of intelligence and in laying the groundwork for the development of further specialized devices used either in conjunction with the accounting machine equipment or in sort of in total concept of the specialized machine like the Dudbuster associated with Madam X, with the Bombe operation, but without this first entry I don't think and the timing of it I don't think we would have been able to do some of the things, computer of a computer type that we later on achieved. Now I think some other we now cross over to the COMSEC again because we are getting up pretty close to where the war is about to happen. We haven't had Pearl Harbor yet and the Army Communication Service had determined that they were going to use teletype or rapid communications and of course you couldn't use it in ~~the~~ clear so we had to -- we started work on the some concept of enciphering teletype but before the war

happened this sort of fell in abeyance and the equipment was not on the drawing board even when the war started but within a few months after the war started the requirement became a very real and Stoner just laid it flat on the SIS. Stoner was the head of, General Stoner was the head of Army Communications Service, ACS is the acronym, and that covers a lot of evils as well as ACS and the Signal Corps. He just laid the requirement right on Friedman personally to produce something so we this is when the SIGCOM first came into being and I think I've told you the story of how it got issued out and we had to recall it from use and replace it with something else which turned out to be the one time tape concept, the SIGTOT. But this was after WWII had started and we were actually sending troops and equipment over to North Africa and I think our capability for using the one time tape principle which was sort of a reversion to what Friedman wanted to do with the old M134T1 if you'll remember because we had to generate key tape. But not a reversion to a something that was

impractical because the state of the art technology had advanced and produced equipment much more reliable ~~than~~ in the timeframe of 1942 then it had a decade earlier, 1932 and 33, so we were able to generate the key tapes and do this in a mathematically secure way. In other words, the requirement here is something that's unpredictable. Now it doesn't have to be random, probably its better if it isn't random because if you try to do random set up a randomizing machine ~~it~~ you got to satisfy a lot of mathematical requirements. In the cryptanalytic world it's you just want the thing to be unpredictable. You don't care how its produced. It could be produced by design or by random or whatever as long as the guy doesn't know what's coming up next you got to be happy so we had key generators in great quantities to generate this unpredictable key stream which then was fed into the code production program and produced the tapes used by SIGTOT. Now I think you may be a little bit surprised at the next thing that comes out but you see this key generation factory leads us right into the concept

which we discovered when the German one time pads system was broken because in our analysis of the SIGTOT principle we asked ourselves can somebody figure out how we generated these keys and take advantage of it, if they get one key from a booboo where the tape is used twice for two different texts they can obviously recover the tape. WEll now how much of that would they have to have before they can figure out how the tape was put together and predict the tape.

End of Tape 6, Side 1

ape 6, Side 2

Well now I don't think this concept of examining the key as we did with SIGTOT was as significant thing in as I may make it in what I'm going to say about it in the context I'm going to speak. When we got ~~the word from~~ to work on the German one time key but here's sort of what happened, and I'll point out where they come together and show that we were psychologically ready for this kind of a thing at ~~a~~ the time when we needed to be. The simple background behind the German one time key operation was that the Germans sent some pads, distribut~~or~~ed their pads, and I believe the circumstances were as follows: There was a high level German foreign office individual whose name ~~escapes~~ slips me for the minute but he came to Washington and he was going to visit several German foreign office installations on his trip and as part of his luggage -- he was acting as a courier for the code production people in the foreign office -- and he had the pads that were going to be distributed both to Washington and in other places in the Western Hemisphere, ~~and~~ When he got to San Francisco

and he got on a boat I believe ~~and~~ so maybe he was headed for San Francisco anyhow I know he passed through the Panama Canal and when he got to the Canal the FBI was standing there waiting for him and asked him for his diplomatic credentials. He had failed to ~~secure~~ procure these before entering the canal and the FBI, discovering this, immediately took over his luggage and held it because he didn't have the credentials. He raised hell about it. He the Germans got livid and made a lot of noises and you know tried to stop this but the FBI ~~said~~ just stood (?) stolidly you don't have the credentials therefore we have to do it this way, We're sorry. And so they held it overnight and photograph it and then of course it didn't make any difference ~~if~~ whether they violated it or not. They hoped they'd get by with it but they didn't care because they assumed that because they'd held it overnight the Germans wouldn't use it anyhow so they just photographed it. Next day when his credentials were validated and received they very graciously turned it all back over to him. Now ~~the~~ copies of those photographs wound up in Kully's German outfit and then we had ~~the~~

reorganization where the Kully personally got involved ~~in~~ with the military thing but we kept a small group. Kully took all of his old Floradora people and this was the proper thing to do and put them over on the Japanese military because the Japanese military was of the same stripe as the, well, it was additive applied to numerical code and his people were trained in the IBM techniques and everything was set up to make an examination so the Floradora was a damn good staging ground for our G2 -- for our B2 operation to work on the Japanese military and ~~for~~ in that we were fortunate. And we were damn lucky to have Kully and Frank Lewis and the others who had been conditioned ~~to~~ for this kind of a problem ready to assign to ~~for~~ it. Well we were so intrigued with these additive pads that had been recovered that we kept a small effort going on ~~it~~ them. I think there were three people, Tom Wagner and a couple of gals, and it took several months before they found the clues for the breakthrough which was needed for us to look into the the possibility of these being generated by some kind of a machine. Well, Had we not had this key generate~~d~~ or for the SIGTOT we probably

wouldn't have been able to visualize ~~the~~ an installation dedicated to the generation of one time pads but you look at it and you say "Oh, they must have done something like we did with the one time key tapes. They must have had some kind of a device." Well what happened once that ~~the~~ that ~~the~~ Wagner and his group had discovered this attribute and they just weren't sophisticated enough or advanced enough in their cryptanalytic understanding to know what this meant. That I got into the position of doing a P1 on them, ~~see~~ I mean performing the operation which P1 is designed to do. I had a small group of technicians. Now Farner and Small who had been so well, deeply involved in the Japanese thing of course had to be multiplied several times and their ~~scale~~ skill spread out over a great ~~deal~~ many people ~~and~~ and with them as a cadre and some other individuals like Dan Dribben, Walter Freed and John Seaman, and I believe Dale Marston was closely associated with this group, these formed a sort of a ~~test~~ task group concept that would go down and help each one of the sections by finding out what the cryptanalytic problem and

making recommendations to the cryptanalysts on the job as what to do, come back and tell me what kind of ~~a~~ priority since I was chief of B3, what kind of ~~a~~ priority ~~was~~ put on the machine requirements you see and sort of act as a technical liaison ~~in~~ and fertilizer if you will for ideas, to help stimulate people to find out weaknesses in our training structure and so we could remedy those, to find out what other kind of training was needed so we could get that and they were just again it was a team concept and they were mature enough people, fine enough people so that they respected the sensibilities ~~ty~~ of the people they were working with and thereby ~~would~~ were completely accepted ~~that~~ if they had gone in a high handed manner and put the people down, ~~if you~~ to use a modern day expression, I think they wouldn't have been successful but they very skillfully developed the right public relations set-up and people ~~would~~ wanted they'd come and actually sit outside waiting for an opportunity to talk ~~to~~ with this group, and this group was immediately put on to the German problem ~~and~~ to tr~~ied~~ to find out what had been done by the Germans which caused

these phenomenon to appear in the text. Well I think it might be useful to mention that instead of bringing the problem down to the technical staff, the technical staff ~~and the~~ in a body went down and became members of the problem, became members of the section and were assigned to it. This was a psychological gimmick but in effect the problem was removed from the section because it was just too much for the competence of the people there, but we left it for psychological reasons and we were able to ~~get~~ give it the support and everything that we (it(?)) needed. Well once the phenomenon was explained and the concept that there was some kind of a generator there and the necessary statistical and other analytic runs from the IBM unit were provided the problem just fell apart. I mean it was an amazing thing. ~~I~~ everyday you could see significant progress and finally when the device was actually recovered it was just sort of like recovering the wiring of the Purple machine or the wiring of a bunch of wheels in an Enigma or something like that. I mean it was became a real cryptanalytic success story and all of it was against the background of our

concept which we'd employed in our COMSEC and I think this is what you want an example of. Where ~~our~~ ? COMSEC concept lead to some promotion of the cryptanalytic aspect. Had we not developed this thing on our own in terms of the COMSEC key generator we might have never recognized that the Germans had indeed had some kind of device which was fabricating this key and I think while we might have found out the phenomenon and learned to exploit it I think and probably in due course would have realized that this was a key generation thing, we wouldn't have gone into it with the concept that it was a key generation problem so this is one of the rare cases where some contribution has been made to cryptanalysis by the COMSEC requirements. The statement that will probably be quite adequate to enable us to generate the other pads that had been produced by this German machine which the Germans never suspected we would be able to reproduce because you know it was sort of a step beyond the [actual accession ?] of the pads. They thought that if we got the pads that we'd be stumped and we'd never find out how they were

generated. Well there we we fooled them. We did. Now in the domain of key that we had it was the total domain that could be produced by this machine. Whether or not we reproduced it all I think is beside the point. We could have. The idea was to know it was there and penetrate it and find those portion of key which would decode the messages that we intercepted. Now the Germans had another practice. Instead of making a total scramble of these pages, evidently and I almost I think this is about the way they did it, as I remember we reconstructed it, that the machine would run and it would produce the sheets in a normal order of succession so you got them in a proper order as they appeared as they were produced by the generator. The Germans evidently distributed these in piles on a table. They didn't have too many piles. Sometimes they'd have seven piles, sometimes nine piles, and so on and so forth. Then what they would go do is to, and the pad sheets came off of this sort of printing press affair that was producing them. They would just go and drop each page into a pile and walk around the table and then when they got

to the first pile they would go on. Sometimes they would skip a pile. Sometimes they wouldn't skip a pile and so there wasn't a total ~~schmearing~~ smearing of the order of pads. Once you found part of the key, once you got close to the key by finding a ~~new~~ pad, a sheet in one of these pads, then you could sort of, you didn't have to look so far. You'd just look at a few places for the next key because you'd have to go around the table again sort of and so you knew the next one was just a little bit further on and so you just did a little skip jump and you'd find maybe pile one had been put in some pads that had been used between Berlin and Tokyo and pile two would have been used between Berlin and Buenos Aires but you knew that by the second message from Berlin to Tokyo what the Berlin-Tokyo pad I mean message number one if you used it to identify what pad was used you knew that message number two would be about seven or eight pages further down ~~on~~ from the [redacted] stream produced by the key generator even though it was the second page. Once you began to find these little niceties the problem of search was refined a point

where it wasn't nearly as big a task. GEE report has all these fine things in it in a much more accurate presentation than I can reproduce here from my memory but these are the high spots and the general concepts that we operated under and my recollection is not going to be as good about this as would be some of the Japanese problems where I was personally involved in the work ~~but~~ because I was sort of remotely related to this. My job was to make sure we got the skills there and the support for this. The British also participated once we'd got ten into this thing. They were really delighted. I mean it was just as much fun to them as it was to us because we divided up the pie and they went ahead with it. Really ~~it~~ there was no need for them too, but I think they had a bit of the same impulse as we. They had to keep their techniques and their talents sharpened up.

Q: This concept eventually stops doesn't it? I mean learning from one, applying to the other, and vice versa, after the war, the creation of NSA and the huge expansion of everything it becomes more difficult to work or to learn like you all did.

HS

A: It shouldn't and I'll tell you why. I think one we used to have a [Pl in Prod] when I was here earlier. This I think was the Raven group wasn't it and the idea behind that was to take your people with greatest gifts and spread them over the place. Well now and I'll be very blunt with what I'm going to say. The success of that concept is a function of the personalities involved in it. Farner and Small and that group I have mentioned were ideal personalities for this kind of a thing because not only did they go out and help people but when something new like this pad problem came up they brought it back and spread the word, the gospel, around in other places where this kind of a problem might be encountered and I want to assure you that we looked over all the key that we had to see if we couldn't figure out how these were generated and I think with some luck. Problems escape me right now. I remember one but I can't remember more than one I ought to mention. But This key generation principle was recognized and we looked for other places where we might be clever enough to recover the key generation of the

system. I don't think we were ever found another case where it was so startling and satisfying as in the case of the GEE and I can't help but feel like that's one of the one of the most well maybe it wasn't significant technically but it was sure a very satisfying development to be able to announce that you had ~~found~~ solved the one time key.

Q: I should think that the people who are being put into or choose to go into the career of cryptanalysis or in a career of COMSEC should be trained in the other one as well and much more than some one week introductory course in the other discipline.

HS

A: Your ideal, you didn't ask this question but I'll watch it? ~~your~~ The ideal type for your COMSEC operation is the guy who has mastered every known cryptanalytic technique that can be applied and has had the deepest possible experience in it. Now he is the guy that can probably do more to insure your total cryptographic security. That is he tests, he can -- to simplify it, He can flash the princples of, the cryptographic principles, involved in a system against his experience and make an

evaluation and determine what actual tests should be made of the use of these things. That is how you would attack the traffic if you wanted to prove whether or not it could be read better than some guy who is dryly been trained in COMSEC because I think everything I've said here in this, the last, well, in this discussion, shows that you've got to keep people on top of both sets, both sides of ~~the~~ this field of cryptology if you're going to advance your COMSEC to the ultimate and that sometimes the COMSEC pushes the SIGINT ahead a little bit. I think its not as apt to give it the impetus, that is the flow ~~to~~ from the COMSEC advance the SIGINT is not going to be as noticeable as the what your cryptanalytic or SIGINT pack does to the COMSEC field. I I'm not surprised and I'm not unhappy that that's the case. It's just a law of nature.

..... the cryptologic center of the US government and that was our dream. The price that we had to pay is that we had a military Director which rotated among the three services and what you find I think is only a natural result. Now I'm not trying to

run down Pat Carter and ~~the~~ your present boss and others but it would be impossible to achieve the kind of thing you're talking about unless you had one dedicated almost omnipotent and omniscient guy to head the agency. Now I think if I ran the agency one of the things that I would require right quick is I'd require each one of my major outfits to be qualified in both COMINT and COMSEC and with some intelligence training and some business management. If they weren't a good COMSECer they couldn't be head of PROD and if they weren't a good COMINTer they couldn't be head of COMSEC because I would want that guy to think that the head of COMSEC, to think like a COMINTer because he needs that, for his counterintelligence attitude makes him the most proficient protector of of the information that he's responsible for securing. I said that exactly right. Now on the other hand I think the COMSECer and now of course I want these to be just almost twins, both of them well trained, but the COMSEC requirements in a COMINT type of a thing is got to be one that recognizes techniques which identify weaknesses in the COMSEC things that

we're using so that we can reject them just as I told you about some of the things we rejected. Now this is the ideal. We're, you and I, aren't going to live that long friend (laughter).

(I might recognize that)

No, but I think what we're saying is essentially the same thing. I'm looking at it from one side of the heap, you're looking at it from another side of the heap and we can both think of a half dozen actual examples which would prove our point. You say why do we tolerate this? I don't know why. I have no answer to that, except I think we're a ~~beaura~~bureaucratic organization and you just don't change government and this is one thing that's going to ~~hurt~~ whup Jimmy Carter if he gets whupped because he's going out here and swear to God that he is going to change the government and most of us, particularly those of us who were raised in the government, know he ain't going to do that. And I think the country at large knows he's not going to do that. If Jimmy Carter says that he's going to lose. I wish he could but I don't think he knows what to change really and I'd just as

DOCID: 4223202

soon we we didn't have somebody changing that didn't know what he was doing as I'd just as soon put up with what we got. (laughter) Now I'm not saying I'm against Jimmy Carter but this is what scares me about Jimmy Carter when he opens his mouth. Maybe I don't hear what he's saying and that could be a problem in semantics.

End of Tape 6, side 2

Tape 7, Side 1

associated with the Arlington Hall operation and was he kept apprised of the technical situation on sort of a day to day basis? Did you get that? and the answer is Clarke was right on top of it. Not only was he on top of it because of the chain of command but he had personal links like his friendship with certain of us particularly myself and also as our collaboration with the British developed he had his own force over in GCHQ under the requirement for getting the end product and he carefully selected the individuals who were assigned to GCHQ with an idea that they would keep him currently informed of any kind of development, technical, political or otherwise over there, and he had a mania for staying on top of all angles of the problem. Now Clarke's I think we might stop here and explain a little bit about Clarke's role in respect to Arlington Hall Station at that time. We had a sort of a Siamese twin situation over in G2. There was the Director who was in an overall sense responsible for the intelligence activities

and then there was the siamese twin concept which was Al McCormick of Chicago newspaper fame and Carter Clarke who was a dedicated Signal Corps officer and a born intelligence officer. Leader He he didn't need to be trained. He was by instinct an intelligence officer and Clarke I think was one of the motivators to get ASA out of the Munitions Building complex and keep them away from the Pentagon and put them in Arlington Hall Station. He insisted that we ought to buy the school over there and turn it into the cryptanalytic organization of the Army. Well cryptologic organization is the proper term because, ~~well~~ while obviously he was greatly interested in intelligence, He was also a counterintelligence man and automatically embraced the COMSEC as being an important well he felt as some of us old timers do that the first priority is good COMSEC and then COMINT comes after you've satisfied your 100% requirement for total cryptographic security, If you can have a 100% total. Now Clarke did stay on top of the technical things. He would get the reports. He would read them and he would call in some of his friends like myself

and I've done this many times to interpret these and what does this mean sort of Frank? and I would try to tell him and he would understand. He was very able in his comprehension of the technical aspects. He I don't think he could have broken the mono alphabet but he knew what it meant to break the monoalphabet.

Q: Could you ask a follow-up question? In negotiations with the British, in terms of collaboration, Carter Clarke was fully aware of all the technical developments that had taken place in cryptanalysis?

A: Yes Sir, unequivocally and the reason was because he wanted to know what we might lose if we he was a suspicious type of an individual and I think he was the one that put in concrete the concept not to release to the British our US cryptographic principles that I mentioned earlier. And I think I told you that Carter Clarke instructed me to get and he used sort of Carter Clarke language to get off of whatever it was I was sitting on and get over there and get all that stuff back and get people working on it so they could understand it in and apply it when we won the war. That he didn't want to miss this opportunity

of taking every advantage of the British long years that OB40 and other places. He wanted to get that as a part of the trade but he wanted to make sure that we knew what to do with it. He didn't want a bunch of photographs and carbon copies in the file cabinet. He wanted a live operating Middle East organization. He wanted every country in South America. He wanted a little section ~~of us~~ that was working on that traffic because he said there will be no German and no Japanese and no Italian traffic to work on. What you are going to have to do is have jobs for all these people and you better train them now and not wait until after the war is over because they'll get discouraged and go home and he says you've got something here to challenge your good people and anyhow we got to have a cryptanalytic organization that's competent and can deal with any traffic that we might want to intercept so let's get it now while the getting is good and I don't know anybody in that

timeframe that was so dedicated to this principle of the perpetuation of the effort which had been built up and which had been so valuable during the war and as I look back at some of these discussions which followed well the discussions at the beginning of the war right after Pearl Harbor and I'll compare the Army and Navy now and Carter Clarke was over at the Army and there was no Carter Clarke at the Navy. There was the Redmond boys. Two Admiral Redmonds. One of them was directly in charge of the Navy outfit that was responsible for working on the Japanese and German, the naval ciphers. Their idea was that they would concentrate exclusively on the Naval intercept and they did and I can remember distinctly the group working on the Japanese diplomatic, the Navy group working on the Japanese diplomatic, who came over to see me one day and said what can we do with our files. We've been

ordered to get rid of them and we don't think they ought to be destroyed and they will be lost if we leave them here. What do you think should be done with them? And I said you bring the materials. I'll get the file cabinets, and just bring them over here. I'll find a place for them and so next day here came a whole bunch of sailors, each one with a two wheel truck and a file cabinet on it, coming across from the Navy building, into the elevator, up to the third floor and there ~~were~~ was about oh a great number of file cabinets that I had to put in the area outside, the hallway outside of my office, which was a secure area and they sat there almost without being moved until we found a place over at B Building ~~over~~ at Arlington Hall for them. Now the Navy attitude was "Let's concentrate particularly on the wartime situation." Clarke's attitude was "Let's concentrate on the wartime situation but let's take something and dedicate it to the concept that we

will win this war and we want to have a viable cryptanalytic-COMSEC organiz ation after the war is over and we got to have intelligence." If you're ever going to produce intelligence ~~we~~ you get it from a system that's used under wartime stress because people tend to make mistakes and this is the time to exploit it so let's don't put all our eggs in the military basket. Let's keep these diplomatic problems moving along and it was well worth while because we got a lot of good information, wartime information out of this effort. I think this is worth noting and I do believe that Carter Clarke should be given credit for being the most, well the word that I want to use here is hard to find but he should be given credit for having the proper kind of foresight and to be willing to risk the probability that his judgment ~~might~~ may have been bad in not putting all the effort on the military problems as the ~~Redmon~~ Redman philosophy was, but he was willing to take the gamble for the future effort and I'm sure glad he did because when the war was over it was wonderful to have problems that people could be assigned to after they cleaned up ~~ed~~ the documentation

of the Japanese and the German effort and it gave us a chance to pick out the ones we wanted to keep. That's when the Kirbys and the Buffhams and the Marstons.... We twisted their arms to stay on and if you look back in the people who ~~are~~ have really promoted ~~at~~ NSA you'll find that this group supplemented by others like Herb Conley, Jack Connelly and just great numbers that I could name if I wanted to take the time. These, that's how we got those people. We had something for them to do s you see and if we hadn't had a challenge for them I'm sure they would have gone away so I just can't give too much credit to Carter Clarke. I think that it was terrific what he did.

~~Don't~~ I think maybe people might be puzzled by in some measure by the difference between the Army philosophy and the Navy philosophy because here I've really outlined this in the in describing Clarke's attitude where he was willing to gamble for the perpetuation of the activity against the ~~Redmon~~ Redman's concept that we go all out. Now there was probably a reason for that and I would rationalize it as follows. We started out with a

civilian, Billy Friedman, and I think G2 recognized, Col Albright and the Chief Signal Officer and the Director of Intelligence, Military Intelligence, recognized that it would be a very difficult, difficult to get Army officers to dedicate their careers to cryptographic and cryptanalytic matters and they had seen much closer than the Navy had what could be produced by a civilian organization because the Army was a party to the Yardley Black Chamber and the Navy was not and it may be that the Army was conditioned by their understanding of how Yardley, civilian type group, might operate in the military establishment. Now the Navy didn't have that experience and therefore had no insight into it but the Navy had a philosophy that these secret matters had to be dealt with by commissioned personnel and that you could employ non-commissioned personnel but that the decision, ~~of~~ that the more critical things could be handled only by an officer. I am not sure where that philosophy arose but I have encountered it many times. Now there was a great deal of that in the Army because I know that I was excluded from many discussions simply because I was a civilian but the officers

would come back and tell me what was said because I was a civilian in a position of trust and I had to know about it otherwise I couldn't function. Now I think maybe these two things, one the exposure of G2 and the Chief Signal Officers representatives to the Yardley concept where they could appreciate how civilians could be employed as the long term continuity thread in the organization and that coupled with the concept in the Navy of having officers only deal with highly classified matter lead the Navy into use Navy personnel, uniformed personnel if you will, whether cryptanalytic organization supplanted only by civilian linguists in the early days because now Mrs. Driscoll was of course over there but I think these few exceptions, Woodruff, Driscoll and Kate. Kate, is Driscoll was cryptanalytic type, Kate, Woodruff, and some of the others were civilians were translators but that's because the Japanese language was so difficult that the Navy officers couldn't learn it well enough in the short time they could devote to it. Now Kramer was the top Japanese linguist over in the Navy but I have no feeling for how competent he was in Japanese. I don't think he was near as good as Johnny Hurt

or Paul Cade or the Erskine, Hugh Erskine over at the Army. He was better though than Joe Shere and Merrit Booth and the Army officers who had studied in Japan but I don't think he was as skilled in the language as the civilians so the Navy I think because there was no other way of getting them had to go to civilians for certain skills. The Army though was dedicated to the idea that the civilians could continue in the business without any interruption by rotation of assignments and I think that is the substantial difference between the Army and Navy organization and I think if somebody makes the judgment that we were able to accomplish more in the Army than maybe the Navy had and I assure you nobody in the Navy would agree with that, that you might attribute the reason to what I just said. Did I deal with it? (That's exactly right).

....part of which I observed in the Army and Navy and I'm going to contrast a little bit with the way common end product is handled today. In terms of the diplomatic translations which were made and I'm talking now in the time frame just before Pearl

Harbor, maybe 18 months before the Pearl Harbor strike. The function of G2 and the Navy officers was simply to carry the translations up to the President or the Secretary of War or the Secretary of Navy and let them read for themselves what was being produced. Now this was fine because well for example the Japanese officer in the State Department, Japanese desk in the State Department, was currently talking with the Ambassador and he was very anxious to know the precise words that had been sent back to Tokyo about his conversation. He didn't want that to be strained through somebody else's brain. He wanted to drink it from the cup himself. Now ~~that~~ the President got that kind of an attitude too and he wanted to have that cup ~~to~~ at his own lips. He didn't want to have it digested for him by somebody else so now you see the pressure, the attitudes of the recipients was I want the word of God and give me nothing less. Now the same thing was true, I think, in the Navy because the commander wanted the decode. He wanted to make his own judgment about the the information contained in the translation. He didn't want Kramer to act in his capacity of making this judgment. Now I think this conditioned us to a way of handling information, the

end product that's entirely inconceivable today. I think we can imagine giving Mr. Ford an occasional translation but to have Mr. Ford confronted with something like the magic summary of years ago I think would be totally unacceptable so there's been a difference. One, also keep in mind there was no other intelligence worth mentioning in the pre-Pearl Harbor days because Americans just weren't good intelligence, had no feelings of intelligence. I think it was a sheer accident that the COMINT thing developed like it did because if you probably ask G2 officer in those days what would be a good intelligence organization he would give you an answer that you had to have some kind of a field organization. [You would not have the national concept of intelligence as now exemplified by the CIA in the post war philosophies which have developed.] I think it would have been pretty pedestrian and pretty low and I think our great luck in dealing with the Japanese systems in the sense that we were able to exploit them gave a reason for this concept of national intelligence to grow up well in advance of the war and that's been the president's (?)... of course was

looking at the translations. It I would say it would be hard to conceive today of one of our sections over in PROD having a direct line up to the White House and thats what we had in the Japanese section over at Arlington Hall Station and I thought that's what the Navy had. That useful?

I think a related consideration to what I've just said is worthy of noting that I've heard some of my good friends in ~~their~~ our bull sessions about intelligence and its growth. I've heard them and I agree with this, because I've assisted them in their thinking, that we suffered in our intelligence development because of the great success we had in the COMINT business. That the people in the War Department and the Navy departments were so amazed at the type of information being produced, the security with which it was produced and the practical avoidance of all the nasty business of running a spy organization, they ~~had~~ have concluded, and I would agree with them, that our success in COMINT inhibited the development of the cognate intelligence activities which we now are getting blamed for running in this government. In other words we

had no spy rings in G2. Navy had done a little clandestine work but the Army's capability for clandestine work was zilch,nil. It wasn't. The Navy clandestine work though worried us. I know one of the things that bothered us considerably about right after we'd had found out what the J19 type of system was the Navy had burglarized a Japanese foreign office installation in the US and produced the photographs of the system and ~~their~~ the first question that I had to answer G2 and the Chief Signal Officer when they found out about this - Did they break into a place that held the Purple and Red machine and if they did we'll have,we'll have them on the mat for it because we don't want those to be violated. Fortunately the breakin was not at a cipher machine installation but I got strict instructions to go there and tell those folks in the Navy not to do this unless they got Army concurrence and our folks were right because you see being able to do it cryptanalytically we didn't want to lose the cryptanalytic advantage ~~of~~ by having them change ~~the~~ their system and what Mauborgne and the others were afraid of is that the Navy or whoever was violating, breaking in,would leave traces of that would make the Japanese change their system

and they might do, put in another machine that's more complicated than the Purple and then it would take 36 months rather 18 ~~and~~ or maybe never before we got the answer and so they were very nervous about this. Also when you're intercepting a message it's you leave no trace but if you crack a safe you might, so if you can read the message by cryptanalysis the enemy has, and you keep your activity and your success secured, properly secured, the quote enemy unquote has no capability for making a judgment, whether he has no evidence, that you're reading his message and this was a bothersome thing. I still have that kind of a feeling even though I worked over CIA I think its better if you can read by cryptanalysis than to steal it. Now I don't want that to get out to the press because they give another... I'm not against stealing it either if I need to.

Not answering promptly as I'm having to think about and try to recall what happened. I met McCormick about that time frame but there were a lot of things going on and most of all I was converted from the civilian to military. I was come in as a Second Lieutenant and when most people looked at anybody in uniform they didn't look

at who it was they looked at what was on his shoulder and you know a guy going around with a Second Lieutenant's insigna is not going to be listened to and not going to be called in to discussion to somebody going around with a pair of eagles on his shoulder so I did meet, I did meet McCormick. I could sketch a picture of him because I was much interested in him for other reasons but Carter Clarke is the one that did most of the contact with McCormick. I think Carter Clarke was dissatisfied with Minkler and I don't think he admired Bullock either because they knew each other very well and I don't know whether it was Clarke that put the skids under Minkler or whether it was McCormick or whether Minkler just didn't have it and he just went out because he was really a frustrated man.

In this context I think we ought to, except we didn't record that story about Minkler did we?

(No)

Well Let's do it because its on top of my head and I think I think the question is roughly this - What could I say this morning about the circumstances of the delivery of

14 part message which has been discussed so much and which really is the key to the COMINT which was obtained in reference to Pearl Harbor?

Here's what happened. The I think it was on Wednesday which would be the 3rd of December we got a message from Tokyo to Washington which instructed Washington to destroy their codes. We called it the code destruction message. It's in the file of translations ~~or~~ that are attached to the Pearl Harbor report and essentially it said destroy all their systems except one machine system and make sure it's working good because we got an important message we're going to send in it. Now this message was picked up by Col Sattler who was a Signal Corps officer and very able man and it excited him ~~to~~ no end because he came, he just almost ran from his office when he got the message and he just banged through the doors and I was the first breathing body he could find down in the SIS and so he came in and he says "What does this mean?" and I just looked at the message and I said "I don't know. I just got it but it looks to me like they're either going to change the codes or there's something real critical

happening and they've ~~had~~ never sent a message like this because they usually changed the code and then sent the message. And he says "This is a different one there, isn't it?" and I said "Yes sir. We just ~~haven't~~ never seen anything like ~~it~~ that". Well he says ~~Well he says~~ no government is going to destroy its codes unless its going to go to war. He said this is an indication of war.

He said something terrible is going to happen. He said I got to get this down to G2 and the Chief of Staff. So he turned around and ran. I mean this was Wednesday afternoon I think. Well there was a lot of flurrying around and of course the President got interested. I don't think the President or the War Department or the Navy Department any of them looked at this message like Sattler did because it was that was all Sattler needed and if you'll read the Pearl Harbor report you'll find that he got kicked around a little bit because he was so anxious to get a message out to the Hawaiian department and Philippine department and I think that's all the motivation Sattler required. Now I think because the people in G2 and ONI didn't know what to expect I think they were waiting for the Japs to tell them and the only

way the Japs could tell them was ~~to~~ be by sending a message telling the Ambassador or send ~~the~~ a message, a circular message, out on the on the Japanaese diplomatic network throughout the world. Now I'm not talking about the Far Eastern diplomatic network but to send out a circular message to all Japanese ambassadors. They had this practice and followed it pretty frequently. Most of the people then were anxious to read every message from Tokyo to Washington. Then we got another message I think. I don't remember that of this. It probably was, well the real message that got everybody on the alert was ~~the~~ a message that came through Saturday morning. This was called the Pilot Message. It says we're sending the 14 part message. Now in that sense the Japs told us what to expect and since everybody was waiting for the Japs to tell them they were anxious to see what the Japs were going to tell them, say, and so the the 14 part message was a big target. We had closed up at noon on Saturday because we'd been working too much overtime and the Civil Service regulations required that

we be given credit for any overtime hours we spent and so a decision was made from somewhere up in front, probably from Minkler's office, that we wouldn't have any more overtime and everybody would be sent home whether the work was done or not so we were actually sent home. Shucraft and I locked up the office, turned off the switches for the cipher machines and did those things that the security check always did. I left last because I was I was boss so the boss always gets off the shift last even if you're working in the Signal Corps. We left together and then we got called in about 2 o'clock and I came right back and we got the force going because what had happened, the translation of the pilot message had just been sent over as the last piece of paper well sent over promptly but the timing was that it was in the last batch of translations that we carried over from the signal office to the Chief of G2 so the G2 desk which didn't have this overtime problem that the Signal Corps had did what was natural. They came and said Signal Corps have you got this message

TOP SECRET

and then the Signal Corps says we're closed down. We don't know. They said well you better get them in here and get a-cracking to Minkler and that's when we got called you see. So we came back and went to work and of course Shukraft and I we were anxious to get the 14 parter because that's why we were called back really. To find that 14 part message. Now to get down to what was done with that message. The Japanese came on I think it was later on in the day about supper time when we began to get information that, about the message, but it was around the wee smallies of the morning after midnight that we had everything except the last part and so we just sat there waiting and waiting and waiting and the 14th part of the message came in about well sometime after breakfast and of course we cranked it out right fast. Well what happened, it was this delay of the Japs in sending the 14th part that caused the hangup in delivery of the information to Marshall and to the President

TOP SECRET

and to others because both G2 and O~~&~~NI didn't want to take an incomplete message, an incomplete translation, up to that level and so they took the decision they would wait until the message ~~it~~ was complete before they delivered it. This was I don't think too bad a decision because as I recollect the message, and I read it very carefully, and there was no translation involved because the message was in English. The first 13 parts was simply a resume of all that had been discussed between the Japanese and the US authorities and really really didn't make any difference because they knew it anyhow. The puzzle was why were they recapitulating it and then when you got down to the 14th part I think the best thing to do is to read it because it says essentially the Japanese government cannot tolerate the US attitude~~s~~ and actions and therefore ~~we~~ will do as ~~we~~ it sees fit in these circumstances which is about as tight as the declaration of war ~~and God~~ got. Now there were some other messages that bothered us and that was the instructions as to when and how to deliver the message

to the US and if you look back you can see that the time of Pearl Harbor is identified but there's nothing to identify the place of Pearl Harbor and of course 7:30 Honolulu time is ~~13:00~~ 1 o'clock Washington time I believe and that's the connection that was observed, noted. I think some people talked about what might be happening but nobody ever dreamt that the Japs would bomb Pearl Harbor. They just didn't think in those terms. To go back a little bit and discuss the results of throwing these lines into operation. I was calling Monmouth and Shukraft was calling San Francisco. I couldn't raise Monmouth. I kept ringing the bell on the teletype trying to get them up, never did get an answer. Shukraft though got quite a quick response from ~~Psidio~~ the Presidio and the first thing that came through is "~~You're~~ We're not suppose to use this line. What are you doing on the other end?" and he said this to Shukraft. "Now I want to get this line in operation. Where is the, who is in charge?" Sergeant Martin is in charge and he says "Get ~~Sgt~~ Martin on the teletype. I want to talk to him." So he

told Martin what he wanted when Martin finally got there. I don't know where Martin was. It took about fifteen or twenty minutes and Martin said "I'm sorry. Our intercept, he was talking to the intercept station now, not ~~at Psidio~~ to the Presidio but at the intercept station right down where the receivers were. This was just off to the side of them, just like over there in the corner and the Martin said "We don't have any copies we ~~could~~ can teletype to you because we sent all our ~~xxxxxxx~~ copies down to the ~~Psidio~~ Presidio mail room to be mailed to you. And Shu~~c~~kraft says go get them and put them on this line and these are the ones we want. And he did this in the clear. We didn't fool~~i~~ guard in ciphers no with that because we didn't have time. We found out later that it wasn't that the non-comm in charge up at Monmouth intercept station hadn't been told exactly what to expect from this teletype thing but he'd been instructed not to use it until he had been he was given the word officially and when the thing started

banging over there he got up and pulled the plug to keep it from bothering him.

Did you get that?

Q: So the 14 parter really came in, was in that batch they'd sent to the mail room at the Presidio ~~Psidio?~~

A: Put it back on. No the 14 parter was I think we got a copy from Hunt, Fort Hunt, and the Navy had a copy. We got it from all over because the Japs bounce it through and of course all these intercept stations and then Hunt and the nav~~al~~y intercept stations were looking for it and so as quick as it got on the air we picked it up and so it was really foolish about the lines to San Francisco and Monmouth except we started using them immediately and from then on they never did close. I don't I don't think those teletypes stopped until we moved over to Arlington Hall Station. We put in some more but the copy of the 14th part was decoded promptly as soon as it was intercepted. It was only a matter of getting it through the cipher machine and into

hard copy.

Q: Was the communication~~s~~ from Fort Hunt, the line from Fort Hunt, as efficient as the one from ~~Psidio?~~ the Presidio?

A: We didn't have a line from Fort Hunt.

Q: How did you get your intercept~~s~~ from Fort Hunt?

Schukraft

A: Shu~~c~~k~~r~~aft took his personal car and went down and picked them up and the S~~a~~ergeant down there called him ~~when~~ that he had a ~~bunch~~ batch of intercepts.

Q: My question is, If the line to ~~Psidio~~ the Presidio had been in effect say from December 1 or at least before December 6 would you then have gotten any of ~~the~~ those 14 parts quicker than you did?

A: Yes Sir. We would have gotten them just as they came off the air. They would have come right in on that teletype line and we could have decoded them immediately and we wouldn't have had to scurry around between us and the Navy to make sure we were finding them and that we had the word out to the intercept station and Shu~~c~~k~~r~~aft wouldn't have had to go get in the car and sort of look over their intercept operators

Schukraft

shoulders hoping he would find it. Martin and his group out ~~at Psidio~~ the Presidio were the best in the Army and I think if and I'm sure those 14 parters, some of them, were in there. We can check this by going through the files but I'm sure we got them from everybody, from every intercept station, because these were good signals and everybody was listening and what would have happened is, as the Japanese diplomatic intercepts were collected by the operators, the intercept operators' copy would have gone over the teletype and they would have used the teletype to make a record copy and it would have been delivered in real time into this, into the Purple room, where the teletype ~~is~~ was installed so we all we'd have to do is to strip it off the teletype, ~~and~~ go over and check the indicator and put the starting point on it and run it through the cipher machine. I believe we'd already recovered the key for the -- there was no delay in recovering the key for that day.

Q: Do you recall approximately the time, the average time, it took from the time of intercept ~~before it went~~ at Fort Hunt to the time that you received it.

A: There were it was a very close relationship. When Shucraft maintained very close liaison with the Fort Hunt group and he had told the operators what to look for and the kind of things we were interested in so Shucraft would call up on the telephone and double talk with the ~~those~~ people and if they had any thing Shucraft thought we ought to have he'd get in his car and go down there and pick it up. If they didn't have it he wouldn't go. It was that simple.

Q: Can you give us a time, a rough time, for the whole operation? From the time they would intercept it until you had it in your hands?

A: If they intercepted one that they thought Shucraft wanted they would call him up and this is on the assumption it was an identifiable item. Shucraft would drop everything, get in his car and the time lag was what it took Shucraft for driving time and .....

End of Tape 7, Side 1

Tape 7, Side 2

The question is what do I remember about the ~~objective~~ attitude of people in the Signal Intelligence Service toward the work, whether we were dedicated to the technical aspects or whether we were dedicated to the product, intelligence. Well ~~since~~ I think this varies a little bit with the personalities ~~then~~ and maybe I should take each one of ~~them~~ us separately and express how we felt. I ~~get~~ think the, we could lump all the military, the officers who were involved in this, under into one category. They were certainly end product oriented and they wanted to get as much end product as we could produce but a few of them realized, and the few of them included Akin and Mauborgne specifically, realized that the way you got end product was ~~to~~ make an investment in developing your technical capability and so they were willing to abide by Friedman's judgment as to whether or not he should put all his effort on ~~this~~ the production of end product or divert some of it to cryptanalytic research and of course we had the cryptographic problem too and they left pretty much the disposition of the personnel group to Friedman

so far as the technical work was concerned. Well obviously the G2 people cared very little about the technical progress. They I think grossly realized we needed to have good cryptanalysts but they were anxious to have this cryptanalytic effort put on the production of end product and so they get a little petulant if they found out that somebody had been transferred from the Japanese section to some place else and I assure you I used this to my advantage. Now then I think the important thing to talk about is the attitudes of those of us and I'll I'll I'll deal with four, Friedman, Sinkov, Kullback and myself who were the senior cryptanalysts at that time in the Army. We had some other people who later on well who at that time I think Feiner and Small have to be mentioned too so I will talk a little bit about them. Let's start with Friedman. Friedman had a good appreciation of the importance of end product and he knew that the greater the volume of end product we produced and the better it responded to G2's requirements the better he would be able to get resources like IBM machines and other things to forward the cryptanalytic and well the cryptologic if

you will because we still had the code making problems to solve. He realized it was a good way of achieving his resources and so he had proper appreciation of this aspect of it but his instinct was to find a solution and his goal was a general solution to almost any problem so that you could just crank it into a sort of assembly line program and the answer would come out on the other end if you didn't have to do any deep intuitive analysis or anything. You just knew precisely in advance every step that had to be followed and out would come the answer and he liked to devise these kind of programs and once he had satisfied himself that that kind of a situation had developed he was then ready and anxious to go on to some new problem and I think Friedman was unique in that regard because I don't think anybody over at the Navy had that kind of motivation and I think it was a wonderful thing for the government that Friedman had this. I mentioned it not in the sense of complaint about Friedman but in admiration of him because he had enough other people beating him over the

head to get the end product out so somebody had to stand up for the technical advancement and he did that ably. Abe, Dr. Sinkov, I think was closer to Friedman in his attitude toward the problems. He realized too the importance of the end product but he just loved the Italian problem and he could get so steeped in it that he didn't want to be bothered with anybody else. Now I think Kully was a little closer to Abe and Friedman than I was because both, remember, both Abe and Kully were needed sort of intellectual stimulations. They were both PhD's in mathematics pretty soon after they came and so they liked the research aspect of it, I think, because they were conditioned to it by the fact they had gone on in mathematics as far as they had. But Kully was a lot more pragmatic, I think, than Abe or Friedman and somewhat closer to me because I looked on cryptanalysis. I wasn't. I enjoyed it. I thought it was a tremendous occupation to be in but somehow or other I had an instinctive desire to find out what people were talking about. I was curious. I was nosy and there was more of that in me I think than in the other three. Now I admired what

Friedman did. I like to do this same kind of a thing but I also realized that you couldn't put the problem aside, and I think I introduced one thing that maybe the other three didn't have if I can talk about myself. I think my attitude was now I've got this program. Can I improve it? Can I make it more efficient? and I would work very hard you see at trying to make find an easier way of solving a problem, and I was always looking for the golden solution and I think I had this motivation which probably Friedman also had but didn't seem to be as prominent in Friedman's discussions and his actions as mine did to me and that's probably because I was closer to me than I was to Friedman. ~~He felt~~ He'd tried (?) other judgements and I felt this personally but I can remember many cases where Friedman was real pleased to let me go ahead with the operation of the Japanese sections when things were pretty well under control because that gave him a chance to do the other things that he liked to do, ~~mainly~~ namely improve our cryptographic systems, find new devices, speculate about improvements in the application~~s~~ of our IBM and all sorts of avenues into a broader

domain of cryptanalysis. Of course as I sit here today I can't help but think of how strange this may sound in terms of the present concept of intelligence because we have really complicated the situation because we formalized it into intelligence requirements, and intercept requirements and mission objectives and all the fancy words that you bump into ~~on~~ in staff papers but nonetheless it the process boils down simply to the technical skills and actions which are required to reduce the intercepted traffic to some basic intelligence form, translation I think is a good example of what I'm talking about, and the dedication to that segment of the operation ~~is~~ as contrasted with the quote consumer impulse unquote which we find in the intelligence agency, as. The people who receive the information then the final consumer, not who is the man, and I would say that Kissinger is a pretty good example of this, Kissinger and his hungers for information and I'm sure Kissinger doesn't have any idea of what's involved in the earlier steps ~~of~~ -- interception, processing, solution of the system and its translation. I think he would be familiar with that thing closest to him

namely the people who evaluate the information and digest it for him. I think he would understand that but I think he would have very little patience with a man that said well the end product, the end goal here is the solution of the system not the information we're going to give you Mr. Secretary, and in those days you see of course the whole thing was telescoped into very short path because G2 was just over there and there were only a few people we talked to. We could clearly see the cryptanalytic organization and how it was working and then we were immediately close to the intercept operation and there was no competition, no strong competition for intercept time. Our biggest competition was for machine time because the geographical location of our intercept stations took care of the requirements, intercept requirements, problem. They listened to what they could hear and that's what they sent in.

Q: In through the 20's but from then on it gets very very hazy.

A: Well I'm might tell you what I remember about the 1930's on up until we got involved in the war and I think the during the war and post war story about and lets call it the cable traffic here for an easy handle. It is pretty well documented. I doubt

though if the intercept of the early 30s has been treatly adequately in any historical records and so I will just tell you what I remember. Now lets talk about the state of the intercept in 1930, sometime in the early or late spring April-May 1930 time frame. The Second Signal Service was just being put together and so the amount of intercept which we received from them was just the result of sort of accidental, an accidental thing which maybe one of the officers or one of the operators had produced because he was practicing and I think we got a lot of that type of material but it wasn't much use. In the first place we didn't know what to do with it. We were still too young in our training program to be ready to deal with that kind of material and second it was ~~pretty~~ poorly organized because the Second Signal Service hadn't set down the rules and the format for proper preparation of intercept which is vital I think to being able to use the material efficiently because it's got to be pretty well sorted out and identified before it gets, before you can even decide which is

items are going to be transmitted because a lot of it is crud and you don't want to waste your time with it so we find that the Second Signal Service, the great hope ~~for~~ of the Signal Intelligence Service for intercept in the future, was just now coming into being and was in the preproduction ~~stage~~ state. Yardley, to go back and sort of cover up that side of, uncover that side of the picture, Yardley was relying mainly on cable drops and I think that's pretty well told in his book the Black Chamber and I think that's pretty accurate. I dont think he says so in so many words but somebody who understands the business can certainly see this and on my own recollection I can remember a lot of cable drop traffic obviously picked up from cable offices in this country, which ones I dont know but I would guess ~~in~~ New York and Washington because the nature of the traffic. I can remember a lot of that but I remember very little if any intercept except the World War I traffic like the ADFGVX material ~~which~~ that I talked about earlier and that obviously was from the field intercept stations that had been provided for support of intelligence in WWI. Now since we

in the SIS were not actively engaged in COMINT production we didn't need any traffic at that time so probably the security of the operation was such that it seemed like we would be prematurely rocking the boat if we went out or G2 went out and tried to begin to collect cable traffic because there was no point. It would have cost us more in terms of security than we would have gained in terms of advantage, and now there is one other sort of area interest that I think I should mention. The US Navy had and I learned this later. I didn't know it until about 34 or 35 or certainly not before 1932. The US Navy had developed a very effective intercept service and had been covering the Far Eastern circuits particularly the Japanese Far Eastern diplomatic net which was a special net set up with headquarters in Tokyo and several points throughout Asia I believe. I think there were four major stations in it. Thats my recollection and I caution anybody to quote me but I remember four stations. This could be wrong but there were certainly a headquarters

and some stations in Asia, Manchuria and the parts of Asia that the Japanese were occupying in those days and this was I think some of the best intercept copy I saw until we got the Signal Service organized and were using mechanical aids such as undulator tapes ~~that were~~ for recording the signal and then we could always go back to the tape~~s~~ and check it. The Navy intercept copy was almost a hundred percent perfect. I know it was a Navy intercept copy we worked on when Kully and I broke out the first Red machine traffic. It was a Navy intercept, Far East net. It was December and I believe it was December 1930 was the date of the message. Now of course we didn't have access to this Navy material but I mention it to round out the picture. Well a couple of things should be noted in connection with the Second Signal Service and its intercept efforts. One of the things that the Signal Intelligence Service was responsible for grew out of the WWI concept of, I will call it a SIGINT organization, because the secret inks in WWI had been a great source of intelligence and in the

concept of the Signal Intelligence Service ~~in~~ of the 1930s it was envisioned that there should be a secret inks laboratory attached to the Signal Intelligence Service and be a part of it and Friedman had was a very good friend of John McGrail who at that time was a captain and a professor of chemistry at one of the eastern universities. I dont remember which one and John came down a couple of times on active duty. John McGrail one of the things he did on his active duty trip was to design and layout ~~the~~ a laboratory for secret ink~~s~~ treatment. One purpose of it was, one, to have a laboratory in being so that we could train people in secret inks and believe it or not I took a course under John McGrail in secret inks, manipulation and flap and seal work and other things which I found great, right interesting because I had a chemistry major in college and of course I was pretty well conditioned for this and I thought it was great stuff. Now as a part of this secret inks laboratory John had set up facilities for microdot and that required a dark room

and in a corner of the dark room we had developing facilities for 35mm film and a 35mm enlarger and so sometime on in the 30s and I cant put the date on this but I assure you it would be about somewhere between the date of the solution of the Red machine and the Purple machine when G2 began to find out that we could in fact process and exploit the Japanese diplomatic intercept so rapidly that they began to figure on ways of cutting down the time of receipt of the material because that was now the bottleneck and arrangements were made with the local cable office here in Washington for one of the officers to go up and photograph the selected traffic and bring the film down where it would be developed in this little secret ink laboratory and now it was really part of the intercept service because we were so busy with other things we lost interest really in secret ink and we were using this facility as a way of getting prints of the messages and that had been filed (?) up in Washington. Now this pickup

had to be done in the early morning hours. I believe I'm correct in this recollection that the, some fellow came in very early in the morning and got the messages in a little package at the RCA office or whichever cable office it was in Washington. Then one of the officers, and Earl Cook did most of this, would go up go into this little room where he had a camera that could be set up with some lights, photograph the messages, put the film in his pocket, lock the camera back up in whatever compartment he stored it in, come on down and either he or one of us or a sergeant would run the film through, develop it and make the prints and this, just sort of to interject something that's historically out of place and chronologically out of place but so it doesn't get lost, we found it extremely interesting and sometimes valuable, I can't think of anywhere it was of inestimable value but it did enable us to learn a lot of things about coderoom practices and in fact some of the messages from, that he had brought down, the photographs showed clearly that that well the

Scandanavians I believe certainly were using Hagelin cryptograph that produced a printed tape and they simply paste the tape up on their message blank and that was a very good confirmation that they were using Hagelin you see, and other times, particularly in J19 domain we'd find a code clerk would make a mistake and he would copy the wrong column and then type the message up and check it back from the message and he'd scratch out the column and write in the correct text so on occasion when you found a message that had been editorially corrected by the code room producing it and that the copy date correctly been filed you could pick up a little clue as to, would help you in your exploitation thing. I dont think any of these, for example J19 transposed code corrections, we ever got the key out of but I think we I can remember maybe you were on this but I know Farner and Small and I, Sammy, When we got one of these we would just see how much help this could give us if we hadn't recovered

the key and I think our conclusion was this could be a very good clue and if ~~it~~ we had this material before we had understood the system as well as we did it might have been the difference between breaking into it early or not breaking into it at all.--

Just these little clues from looking at the original messages. Now as the interest in intercept and the further development of intercept capabilities sort of lagged until we got actually engaged in the COMINT business and G2 became interested in our end product and began to put the pressure on us for faster servicing of them for particular messages. As a practical example of the kind of thing they were interested in was any message dealing between Tokyo and Berlin and Rome in which dealt with the negotiations of this tripartite type pact called the Axis Pact and the key to this their interest was to discover the precise wording of the secret codicil which had been drafted for this tripartite pact ~~in~~ and which had never appeared in the press or the

public domain. I think we had the text from open sources of the basic pact but the secret codicil to it was never revealed in the open press and that was their primary interest so you see they were anxious to get this dope as quick as they could and this stimulated G2 who placed the requirement on us with the result that the Chief Signal Officer and the head of the War Plans and Training Division, which was responsible for both the activities, the SIS and the Second Sig, keeping in mind the SIS was a cryptanalytic organization and the Second Sig was the intercept organization. Since the War Plans and Training Division was responsible for both of these then they dealt with the requirements for more rapid service, and this I think gave us ~~more~~ an impetus, the impetus we needed to have, to get on with the intercept. Now the nice thing about the cable drop traffic is that is was clean, it was useful, it was perfect copy, it wasn't garbled by being incorrectly transmitted, typed in the code in the communications office and of course you avoided the garble of the intercept process

which no matter how good your intercept operat~~ions~~ors are there's bound to be some small percentage of error~~s~~ introduced and I would say that's roughly the picture unless Sammy can add something that I've overlooked.

Q: Let me ask a follow up question to that. In the period from 1934 ~~with~~ and the passage of the Federal Communications Act and the actual beginning of hostilities for World War II was there any thought that you know of given ~~of~~ in either the SIS or G2 as to the legalit~~y~~ies of using the cable traffic?

A: Yes we gave considerable thought to it. We knew it was illegal and therefore we better keep quiet about it.

Q: You knew it was?

A: Yes Sir. There was no doubt in our minds but what this was illegal. You want to ask a question or you want me...

Q: Well what we were wondering about is that with the Section 605 of the Federal Communications Act of 1934 it spells it out very clearly that interception of foreign communications was prohibited. Of course that goes by the boards during wartime so

the question was when, as the SIS was using these cable, the cable traffic, from 30 or 31 through 41, beginning of the war, and then from 45 onward, what were the legality the consideration, the legal consideration involved in this?

A: Well if I may answer that in terms of what I recollect and sort of the rationale that I remember as I remember it if you will go back to your law you will find that there is a whole string of things, words end to end, starts out with the interception and winds up with "the publication thereof" so we figured this was the envelope that we hid behind. We figured that as long as we didn't let it be openly published that we were still legal if we intercepted and if we cryptanalyzed and if we translated and ~~if we~~ used it within government circles in an unpublished form, that we we sort of had a little bit of an island to stand on. And that was just about the attitude that we employed. Essentially we recognized ~~this~~ its potential illegality and we knew if it ever

got to court that we would be condemmed and even some of us might be tried as individuals. We were told that by G2 and our bosses that "Look you must remember, and I guess you'll remember this Sammy, but I was told just like I was about ~~Patton,~~ patents, there's a caveat that you were given about any invention you made would be the governments you see but that came on later on but there were certain things, ~~Patton~~ patents was one and the other was the legality and the need for secrecy. We were told that the law was unfair, That this was being done in the national interest and if we had any qualms about it we better get out because if ~~they~~ it ever came to ~~court you~~ issue the law, the legal aspects might be against ~~you~~ us so in that sense I was aware that what we were doing had, could be illegal and I was satisfied in my own estimate of it that it was but I didn't care because I felt so strongly that what we were doing was a proper thing for the US government and I certainly knew that we had to have the codes because I could

not see, for example the UK which was notoriously a successful nation in codebreaking. I couldn't see the British pulling back for some legal consideration if they felt they could get a diplomatic advantage from reading and breaking an American code so this was the context in which most of us approached it and maybe we sort of developed, mutually developed, this attitude and fell into it because it gave us a comfortable feeling but I think if I had to do it over again baldfaced I would go and run the risk and in those days it was indeed much less than it is today that ~~it~~ the thing would be exposed because then you were dealing with people that you knew were honorable. The people in the business were honorable people. They weren't sized by some of these things like Ellsberg was sized with. There just weren't enough of them around so that the probability of an Ellsberg being in our group was great enough for it to actually happen. Now we did have a few people that we were nervous about but as I look back there was no call for nervousness . Its just that they they talked that way rather than believed that way,

and I think today as I look at it I would not feel as easy about my chances of going through that kind of an operation without being caught at it as it was in those days. It was almost 100% foolproof in those days. Now its something less than that because I would be afraid that some of my contemporaries might turn out to be an Ellsberg and that would bother me considerably for what its worth.

Q: The cable companies were certainly agreeable to cooperating, were they not?

HS

A: They indeed were and I tell you I found this. That there were certain people within the cable companies. Now I wasn't involved in this directly so this is second hand and hear-say. Some of the people in the cable companies felt like they were doing a national service and were proud to be involved in this thing because they had enough understanding and had been briefed appropriately by our G2 representative and we of course did this at the higher level when the stage was set for us to pick up this cable traffic they had ~~competence~~ confidence enough in the war department people to trust

that it was indeed something in the national interest and was not going to be used for, as implied by Mrs. Abzug and others, that this is for persecution of the individuals. They they they weren't that stupid, these officials, but they did take pains to ~~make~~ sure that whatever arrangements ~~were~~ was set up well enough organized that the action~~s~~ could be kept secret and not be leaked to the press. We were awful nervous about people from the press. We just avoided them wherever possible, not for that reason but for the whole basic concept of keeping quiet the SIS activity. I think the Navy is just as bad. I don't recall whether the Navy did any, had any arrangements, picking up the traffic because and I think the reason ~~is~~ was this, that the Army got in there a little bit early on the deal and the Navy and the Army both felt if that the Navy ~~would try~~ tried to go in and do the same kind of thing that then this might be too much for the communication companies and might be too much to have too much, make too much of a, make too many waves and therefore be discovered.

Q: What was the situation at the end of the war? Did you go back, did you continue on after the war using cable traffic?

A: Let's put this on tape. Now this is a nervous, but I'm going to tell you what I recollect. I don't think its going to be any worse than what's in the records already. At the end of the war we could visualize a couple of things. One, the certain setbacks were in fact inevitable in our intercept capability. We had hoped to have a world-wide intercept capability but we didn't know whether that would endure or not because in the few months after the war people just couldn't get home quick enough and later on, just to throw in a little bit of a personal observation, when they got back home and after they had been there for a while it didn't look so good so they were anxious to get back into the service. So in that little period when there was a great outflow of people from the intelligence area and I can remember General Corderman giving a speech out on the campus at Arlington Hall Station

He got everybody out there and made a speech to them and in essence what he said was we'd like for you to stay but here's your hat, what's your hurry. I mean he just encouraged people to hurry up and get back home because he was he had been told by the Chief Signal Officer and the people in the Pentagon that we had to demobilize rapidly and look General Corderman you got a lot of people out there at Arlington Hall Station. The sooner you get back to nothing out there the happier we'll be with you and your administration and Corderman was out there trying to effect that rapid dissolution of the outfit which was absolutely contrary to the Carter Clarke philosophy and that was "let's keep the better ones". I don't know what discussions Clarke and Corderman had but I do remember Corderman was mentioned a couple of times by Clarke in his conversations with me and I quote "Why the hell is Red so anxious to get rid of the people?" unquote but there was that. I mean we could see that maybe we could go too far in the dismemberment of the activity and we laid on a plan which

I think got called Shamrock at some time and the object of Shamrock was to continue these practices which ~~were~~ developed under wartime conditions and considerations with communications companies because if we broke them off and then go, had to go start them again you see ~~it~~ that would be just like building the world all over again and we thought as long as these were in being and we could continue them to keep people happy this would be fine and I do know that the efforts expended for the continuation of these things turned out to be considerable and involved people at the highest level. People from the upper levels of the government. The Secretary of Defense, the Secretary of War's office. Actually went up and talked to the heads of the communications companies which we wanted to provide us with this stuff and the arrangments were laid out on that level and it was ~~sent out~~ set up so that the detail pickup arrangements, that is, who would deliver what traffic to whom and the rules and regulations surrounding the way it should be handled were set up at the lower level but the sanctions and

the agreement ~~and~~ in principle was negotiated at the highest levels in the country in the Secretary of War's office. I'm sure that must be documented somewhere around Washington. I don't know whether those documents would be here because this would be done between G2, under G2 auspices, rather than the Director of well rather than the Chief Army Security Agency or Chief Signal Officer. Now this Shamrock operation was considered valuable for these considerations. One, it was a cheap way of getting intercept, realcheap. It was a fast way of getting intercept. It was a secure way of getting intercept because the waves you generated by this somewhat clandestine arrangement ~~was~~ were a lot less than you might expect to be generated by having an intercept station deal with the stuff. That was one consideration. The second consideration was ~~the~~ this attribute of the traffic. You were looking at the copy which had been filed by the coderoom, prepared in the coderoom and sometimes the nature of the system shows through in this and the two things I mentioned are beautiful examples of the kind of

information you can pick up. What was the printer like? Was it a hand system? I think you could make a good guess at it. ~~Always~~ or was it a machine system and most ~~of the~~ machines were designed to print on the ~~page~~ tape and you could by ~~determining~~ examining the type and the external characteristics of the message you could learn a lot about the system and you might get some wonderful clues about it because they scratch out an indicator and replace or, as they did with the J19, they would alter one of the columns and that was directly and accurately reflect the length of the column, the length of the key and some other implications and so it was this technical consideration that was important and I think in my mind almost enough to continue it not for the timely receipt and economical receipt of the intercept. Then there was a third consideration that it had been a very nervous thing to get these companies involved in this activity earlier and we felt if they ever pulled away from it that we might not be able to recruit them to assist us so these were the three considerations. One, efficiency and

economy, cheapness and speed of intercept. The technical plums that you might glean from examining the photograph of the traffic and this was particularly ~~to~~ true in the Washington area because that's where the Embassies were and then finally we didn't want to have to invent the wheel all over again with some later generation of communications company.

Q: I think it's important to reiterate the location as to the decision to do that, was upper level of the government rather than the agency looking at the traffic.

A: The agency generated a requirement and before the operation could be conducted it had to be sanctioned in the upper levels of the government and the nature of the thing was such that some of the negotiations had to be conducted by that level. That was the Gordon Gray level if you want a particular... Gordon Gray being an (?) Assistant Secretary I believe of War at that time. Later on he was Assistant Secretary of Defense.

End of Tape 7, Side 2

.....regard to what [illegible], I'll identify as the secrecy oath where an individual who when he accepts the position signed an oath of secrecy. I don't remember the precise time of that. I know I didn't sign a secrecy oath and I wasn't cleared until about the middle of the war and the reason I wasn't cleared ~~was~~ is [illegible] because ~~obviously~~ I had been in the business since 1930 and was one of the original three or four. Do you remember signing the secrecy oath Sammy?

([illegible])

Now when the war came on I think Kordermann and Jim Slack, Col Slack, ~~was the~~ his Executive Officer, got ~~a notice~~ [illegible] about this and at that time Kordermann issued an order that all people who had access to COMINT and particularly to COMSEC materials would have to have some kind of a background examination. I remember that's about the first time I ever heard the term background examination and I wondered what it was and I wondered what Kordermann meant and so did ~~the men and so did~~ Jim Slack but they kind of figured out something that should be done and that was to look to see if there was

derogatory information in their files and look over their Civil Service record and application and maybe write a few people. We always had three people you knew that we used as references and they would write to ~~the~~ references and from them they would pick out one or two and, one of two names, of I mean this was sort of the second generation that if I gave three references they would write to one of the references and say could you please list some intimate acquaintances of this individual and then they would pick out one or two of the individuals who were, had been recommended, by the fellow I had used as a referral and they would check with them to see if there was any derogatory information. Well this patently is not much of a way of doing a background investigation but I guess it was better than nothing. I don't know whether it was worth what it cost or not. Well that was sort of the first step and then later on when we got more and more sophisticated and got into compartmented problems and particularly after the war they got to be lot more fussy about it and I think the ultimate in this

requirement was the use of polygraph. I don't know that we had even envisioned this

~~after~~ the war but now there is another set of circumstances in the war. It was

I think the basic reason for requiring the secrecy oath when you signed it, was to

keep people from spilling their guts out after the war was over because everybody was remembering the

effects of the Yardley book and they didn't want people to go out and tell all about

their wartime experiences because they were afraid something might spill through that

would be classified, and so I think it was just to inhibit people from making noises

about what they had been involved in and that's about all it amounted to. Now really there

was not too much reason for security investigations during the war because it was a

rare thing, I think, to find somebody who wasn't totally dedicated to winning the war and

certainly the Japanese would be identified by color. I mean there was a race element

there which people now say ignore it now if you want to, but there are times when you

don't ignore the difference in people's skin, the color, and that was a deterent.

The German was a little more complicated question but somehow or other we got through

without any bad luck. Of course though when the war was over and we began to, I say we, I mean the nation now not just the SIGINT types and we as a nation and those of us who were in the intelligence business and subjected to the considerations of security requirements, when we began to find out what the Communist intelligence service were doing why then I think we got real scared. I guess this was a sort of Joe McCarthy concept of it and I think there was something we needed to be worried about, because most of the country had looked on Russia as an ally and it wasn't until the Potsdam Conference had taken place that we began to realize that the new peace we were in was a cold war with Russia. I think that's the first inkling we had and then we began to tighten up, as I recollect, on our security requirements but I would say and I could be wrong in this, but the oath of secrecy came in about war time, and I think we were all required to sign it. Do you recall anything different Sammy?

I dont' remember signing this oath until.. I don't think I had to sign it because I was in uniform. See, people in uniform are a cut above people who are not in uniform in the military establishment. ~~They think~~ I don't know, they are born out of different ~~rooms~~ wombs or something. Something happens to them. At the end of the war the under mobilization, those of us who were soldiers for the duration were given the opportunity of continuing in uniform or reverting to civilian status and I'll talk about my own situation and I believe that's your question.

At the end of the war when I got out of ~~the~~ uniform I was undecided whether I wanted to continue in the SIS work or not, and when I talked to Col. Hayes about this, our big problem, my big problem, was not the grade that they offered me but whether I wanted to continue in this work or not because I was tired. It had been a long war and we had been working, all of us, not just me but everybody, had been working such long hours and under such pressure that we we just wanted relief from it and I think I had had a couple of offers outside. One was with a new computer company that was being

organized and the ~~military~~ monetary offer was ~~not the~~ enough, substantial, and of course my natural inclination was to go back to the mountains and rest a while and that's sort of what I was dreaming about. I just didn't want to be bothered with computers and other things so I had a little bit of a personal problem and finally I think when it came down ~~and~~ that Hayes said Well I sort of got to know about this and I said I'll give you an answer over the weekend, so I went home and thought about it very carefully and I'll record my own feeling about it because it may be of interest to somebody. I was vividly aware of what was happening because people were getting out and going away. I was vividly aware that the government had invested a lot of training, a lot of money in me, and that I represented some kind of an asset that would be hard to replace. I mean I probably was a little bit egotistical about this but ~~frankly~~ frankly, this would be the kind of an argument that I would make about myself. So I was worth something and I was a little bit unique because of this long training. Also at that time and

I thought this was important, and this may be a little bit self-serving but I was had considerable influence. I had made a name for myself and I was listened to when I spoke and I was believed because I sort of as somebody who had been living this thing for a long time was looked on as a sort of person who understood the business and whose judgment could be trusted and that was part of the contribution I might make. Now this may sound very egotistical but I'm just trying to tell it like it was. Well these were the things that persuaded me that I ought to take this job and I still didn't know what the salary was going to be at that time, so Monday morning when I went to see Hayes to give him my answer, Yes I'm going to continue, then I found out what I was going to be paid, which really surprised me because I wasn't expecting this much so this was sort of why I continued in the business. Now I'm glad I stayed on for this for two reasons. One the battle for consolidation, whether we had three services or one NSA came up and I think I was helpful in bringing about the NSA concept. I

shudder to think if we had three competing services right now, because I don't know whether the problems would be covered or not. At least in NSA you can put your finger on NSA if ~~the~~ a problem slips out from under. If you've got three services and I know as sure as I'm sitting here and with all due respect to the officers ~~that~~ who populate these services there is going to be a great business of buck-passing and some of the important problems would vanish just like they did with the in the German SIGINT structure ~~in~~ during WWII. The Germans had a great number of SIGINT operations. They all went around, skimmed the ~~the~~ cream off. They did the easy stuff and left the real gems, they never really uncovered them. They never really made an honest-to-God attempt on the American high level traffic, The SIGABA. I don't think they ever made a proper attack on the lesser SIGCOM traffic and the [Hagelin] traffic. They had some success, yes, but they were all so busy doing the easy ones, that they never got down to the hard. Well that's exactly what I think we would have ~~happened~~ had without the

c

consolidation and I think it would have been a terrible situation for the country. I don't think we would have had the secure crypto system because there would be three experts around you know, each one pulling out his own and I think that would have been terrible so I'm kind of glad that I stayed on but the reason I mention this is I just about committed suicide in my NSA career because I was such a vocal proponent of this consolidation because although the Army and the Navy initially, the Air Force and Navy, I'm sorry, although the Army initially wanted consolidation that actively impact of the consolidation itself had taken place some of my friends over in the Army had told me that they wished they had never had any part of this and this of course was exactly what was found in the Navy and Air Force. Well then I ran into trouble with Canine sort of and he moved me from the SIGINT end of the business where I was real comfortable and happy and he just sort of kicked me around I thought. He sent

me over to the COMSEC side of the business. Well I was doing more good for the COMSEC I thought by being over in the SIGINT end than I could in COMSEC and anyhow I was working for a guy who didn't know as much about it as I did and that was

CIA intolerable so I was lucky enough to get a job over in CIA. This was about, just right after the consolidation took place and you could see why I mention the two things in the same breath because I was having a terrible personal time over there at NSA. Canine didn't like me. I I didn't move fast enough to suit him and I think he sensed I didn't have much respect for the way he was running the business because I was pretty outspoken, and of course my friends in the Navy were damned glad to get rid of me because I had made so much trouble for them for ~~all~~ these many years that

CIA it was a happy decision for all. Then when I went over to CIA, and am I making this too personal, Hank, I think, I found a different world. First place I was sitting pretty

much at the top of the heap and I was great deal in the position that J. Edgar Hoover found himself. You know you become consolidated because you hadn't been moved out and I knew how to maneuver and stay on top of that heap without too much effort but when the heap crumbled down I had to get back and start scratching again and show that I had some merit on my own. This is exactly what happened to me when I went to CIA because cryptanalysts, I mean Dulles put it flatly, we're not going into competition with NSA. We're not going into competition with Canine and his people. We've got enough to do in CIA and we're not going to fragmentize our efforts by going over there and starting a cryptanalytic organization, COMINT organization, which and this is for the record, which I think a lot of people including Canine thought Dulles was about to do. In my conversation both with Smith and with Dulles it was clear they had no intentions whatsoever but they did need something over there which I could provide and that's

somebody with expertise so that they thought they were getting good advice because most of the people at CIA had not come from the technical end of the business. They didn't quite understand ~~the~~ what was required in terms of ~~the~~ a cryptanalytic organization and what was important to pick up and how much, how deeply, they should go in the liaison with the on these third party deals and this was kind of my role over there and but I had to learn how to be a CIA type. I took their training course. I tailed people around through Georgetown, ~~for~~ one example. I went to isolation. I got pretty good indoctrination, you know, a quickie course really but it was a lot of fun and really very tiring because here I was well I've gone up in years, see, starting a brand new job and I had enough personal pride to want to earn my money rather than just go there and take that job because I well it was just the way I was put together. We had a lot of fun over there. Some of the things that at least I had a lot of fun, I think made some contributions because one of the mysteries ~~in~~ to the SIGINT business was what kind of

traffic was going on the landlines, the Soviet landlines, and we were able to ~~knock~~ mount this [Kappel] operation which I think was a pretty good one. It lasted for almost a year, 11 months, 11 days and 11 hours is what I remember, and then George Blake finally got through to the Russians that we had this tap. He was the one who blew it, I'm sure. George Blake was aware of it but for some reason the Russians didn't react rapidly to this and that's the kind of thing I did over there which in itself is just another domain of the SIGINT as we see it today except I would go on record right now as saying that clandestine collection should be something that NSA should avoid like sin. First place the kind of people that NSA would use in the collection ~~would~~ have to be trained in clandestine attitudes and I don't see that in any of the services nor did I ever see that it in the services. Rarely you'll find a man who is instinctively a clandestine operator and you can employ him but your average intercept operator is just, he looks ~~just~~ pretty like an intercept operator, he talks like him and he ratchetjaws

the whole story out if he gets somebody he can ratchetjaw with, so I would say NSA had ~~would~~ better be well advised to let all the clandestine activity to be done by CIA and I guess maybe I wouldn't have to argue too much now because look at what happened to the Bureau when it got out into the clandestine business and got caught so it's just as well to let somebody else front for you. Why did I come back to NSA from CIA? Well first place Sammy had an idea that well ~~you~~ he had to have a new Deputy Director and Billy Friedman had retired and Sammy had an idea that it would be a good thing to get some ~~of the~~ old timers in the business, back in the business, and I think also Sammy rather suspected that his life would be a little easier, not that he mistrusted me but if for his task? that he could show that any possible competition from CIA in the business of SIGINT was removed and he felt that by my coming back to NSA I could bring two things. One, alleviate some of the feeling that CIA might get involved ~~with~~ in the, compete with NSA and two, I think Sammy got to know me well enough in both in terms

of the Regal operation which required a lot of coordination and I talked to Sammy as Chief of Air Intelligence, made the arrangements you know, [redacted] briefed him on the Regal and told him so there was quite a long period of relationship between CIA and he felt like maybe my experience in CIA would be useful as well as the fact I had been in the business a long time and at one time had a reputation so I think this sort of convinced him it was a good thing to come back.

Q: Who was this?

HS

A: General Sanford. Sammy Sanford. Well he offered me the job of, that I took as Special Assistant and I was very happy to come back because I loved ~~to~~ the work. I loved the organization. It was a fun place to work so I came back. I don't remember the date but that was the job and that was the circumstance, and I think this will be interesting. I'm ~~not~~ really making this more of a personal story than answering the simple questions chronology. [redacted] Reynolds, who was the Director of Security, came up to me

and he said "Frank, he says, we would like you to take a polygraph when you come back to NSA", and he was very apolegetic about the thing and I reminded him that I had one over at CIA and it hadn't bothered me. Why was he bothered about this? He says, Well we could actually accept you based on your CIA polygraph but we would like to have it said that you, even an oldtimer in the business, when you came in to take this job, took the polygraph and we'd like to be able to point that people in senior positions have had no objections to this, and I said well this is fine with me so I took the polygraph and quite honestly everytime I get on that polygraph I get nervous and well now with respect to the training program for our second generation cryptanalysts I guess we better delineate the second generation. I can think of several generations and I'd like to define the first generation, setting Friedman aside for a minute, but Abe, Kully, Larry Clark, Johnny Hurt and myself, there were five of us. Obviously Friedman trained us and we had a long training program and this was a combination of on the job training

and classroom and personal research. A self taught training I mean ~~the~~ the combination of those things. Self-taught in the sense that the three of us, I'll leave Hurt out because he was more of a linguist than we were and we were less of a linguist than he was, so you [mix and match] natural cleavage and Abe and Kully and I after receiving from Friedman what he could tell us began to teach each other, ~~and we~~ I mean we self taught the group as a team. Kully and I worked together on the Japanese while Abe was in Panama. I'm sure we learned from each other. I learned from Kully. I hope he learned from me so there was that kind of training. Now when the second generation, the next group came along and I'd like to identify these as the Albert Smalls, the Bob Farners, [Jean Feinstein, ~~later~~ Jean Grochen,] Mary Jo Dunning, Leo Rosen. That's about the bracket. That's the next generation you see. The first group's the children, Friedman being the grandfather and us coming in ~~the~~ lineage behind him. Their training was a combination of two things. They were ~~aware of~~ well

(GENEVIEVE M. GROTJAN later "GENE" FEINSTEIN)

trained. I think much better trained than the average cryptanalyst today, ~~Now~~ half the time they took the courses that Friedman had given us and they worked together in teams except for Rosen whose was kind of unique in that he came in at a time when nobody else was coming in and so he did all these by himself but he didn't have to go through the drudgery the rest of us did because he was just out there but he was a real good guy, sharp ~~and fast~~ so he assimilated this cryptanalytic lore with great facilit~~ies~~y but the others who weren't Rosens and I don't say this in a derogatory sense about them because they weren't graduates of MIT. I mean some of them didn't even have their college degrees. They did it more pedestrian way and half the time they were working and I remember that a lot of their training, a lot of their practical training, on the job type of training that was conducted, was to enable them to understand the operation we expected them to perform. For example in some of our work on the Red machine we used the newer recruits to do some of the clerical work and we would

explain to them what we wanted them to do and we would also take the trouble ~~to~~ of explain to them what we were looking for and why we were doing it and what the implication was, ~~for doing it~~ looking that and I think rightly so that this would motivate them to do a better job and take a lot of the drudgery out of it and it was drudgery because it was all hand methods so it was this close working relation between us, the first generation and the second generation and coupled with their self study course, self study work on the courses that we had taken, and I can remember also acting as instructor at times for a pair of people as they went through the courses and that's how that training was done and then let's take another sort of generation except a different stri~~k~~pe and these were the officers who were selected. The Baldwins, the Rhoads, Bichers, Rhodes, the Beechers, the ~~K~~cordermans and others and these were brought in in twos and they sort of paralleled the work that we did, and Friedman had developed this

because when the four of us, Sinkov, Hurt, Kullback and Rowlett, came in we formed two teams. Abe and Kully worked together and Johnny Hurt and I worked together and we sort of, we had a good healthy competition you see to make... We oh the spirit of competition was tremendous. It was friendly competition but I never encountered anything like this in college. There there were four of us, two teams, and we could see what the others were doing and it drove us. It really drove us. Now this concept of training was followed by Friedman and I think it was a very good one because you ~~to~~ didn't have one instructor you see. You didn't have anything formalized but anybody that knew the answers to the questions could be called on to explain it and sometimes what Abe would tell them and what Kully would tell them and what Rowlett would tell them would make a better answer than if ~~each~~ either one of us individually had told them so I think they probably had a better environment for their training as the second generation th~~e~~an we had as the first generation. From then on I think ~~every~~ other generations came in, except as we got closer

to the war came in faster and it became clear to us in our development of these new people that some of the things that were included in the first course were useless, redundant, and that newer material ought to be ~~used~~ produced and one of the things that came in was the inclusion of some statistical courses that Friedman ~~and I~~ had, not produced but Kully, Kully ~~made~~ pointed out and I think he wrote his more ambitious works based on the requirements for text for this. I think he wrote some statistics maybe ~~it~~ there was a couple of books that he prepared on cryptanalytic, for cryptanalytic training purposes, Statistics and Cryptanalysis I believe was the title of it or something like that and as a specific example of what I'm talking about here, when we were reading that Red machine and we had it cold you see we kind of coasted it. We predicted the keys and ~~it~~ there wasn't much of a cryptanalytic problem so ~~little~~ par. main cryptanalysis was done in terms of ~~well~~ recovering the codes. ~~It~~ There was a regular change of codes and putting indicators to message where the indicator was garbled. We couldn't read it otherwise, you know this

a little bit of a cryptanalytic technique involved in clearing up an indicator and in support of the COMSEC program, to test on our COMSEC systems, and ~~finding~~ possible keys, you know, to ~~and lets~~ test out the use of rotor machines and other things, so we got spread out a little bit there and that in itself is very good training. The type of on-the-job training in a related field, but when we had, we were just real happy about the Red machine and our work on the Japanese codes and then we began to get some messages through the intercepts talking about the cipher expert that was going around from embassy to embassy that held a Purple machine and there was a clear indication that the new machine was about to be introduced and of course as a matter of prudence we wanted to be ready for it so we took a look at the ~~sort~~ kind of things that we might expect the Japs to do and so we picked the group that we hoped would be able to work on ~~it~~ this new machine that came in, identified them as individuals as then looked across the spectrum of systems that might possibly be adopted by the Japanese and started

training the individuals who were designated to work on the Purple in the specifics of machines or types of cryptographic principles that might be used. Of course we didn't know at that time. We had no traffic to test it on but we thought it wouldn't hurt if we let them direct their training in this direction and one of the things we did was to make sure they got these courses in statistics and tabulation, of crypt-analytic data right down to its evaluation. The kind of thing you talked about in your ~~captain~~ Kappa test. The IC kind of thing, and we, I think this was very useful because it was useful for two reasons. It certainly helped to round out, the junior crypt-analysts. Now I'm down beyond the Rosens and the Feinsteins and the Smalls and the Furners, Ferner's and I'm into all just before the Dale Marstons and the Chittendens and that group. Well there were also certain other training, I've spoken here about the Japanese but Abe ~~and~~ in the preparation of his staff for the Italian problem and Kully for the German problem of course had to broaden the ~~basic~~ base of training to include how you deal with additive

systems, how you determine what kind of a code and bookbreaking, which was pretty trivial in the Japanese section because we had Johnny Hurt and there wasn't any use of anybody competing with Johnny and we had the language officers so we didn't worry too much about bookbreaking ~~in~~ on the Japanese group. We worried about language, language characteristics (~~topographical~~ orthographical) considerations if I may put a fancy term on it and the statistical implications of that ~~but~~ it was pretty important to us. Now when the, when the when we called in the reservists, the ROTC people, this is the Dale Marston group we had enough work for them to be engaged in so that most that they got was on the job training and we had some formal courses that we put together and they were inflicted, was inflicted with upon them and this was very good but things were then moving so fast I, I'm really surprised ~~that~~ if they got anything except an opportunity to do some selfstudying in their spare time of which they had very little but I know that well I can talk about Dale. Dale worked in the Purple room and I know

Dale got instructions from all of us, mainly from the people who were ~~recovering~~ running the machine and recovering the keys on a day to day basis, how to do the key recovery and of course Dale Marston being who he was and as clever as he was he was just right where he belonged, so he was a great deal like Rosen. He grew into the problem. Some of the others, Tom Chittenden, I think got involved in the COMSEC operation and arrived at their position through other arrangements but again most of the training was on the job from that time on out.

Q: ~~I think~~ we know that Safford was sending out correspondence courses in cryptanalysis to fellows ~~to~~ that be trained that were still in the service plus courses to students in colleges, correspondence courses devised by Friedman. Did you have the same practice in the SIS of sending correspondence courses out to colleges or to anybody else and if so were they successful?

H.S.

A: Yes We we did quite a bit of that. One, I've mentioned special text 165 & 166 and strangely enough it just slipped my mind here in the last ~~succession~~ discussion we had and I think the reason it slipped my mind, I'll give you the evaluation of it first. This is fine stuff if you want reserve officer credits but you didn't learn much cryptanalysis from it and I put it pretty low down on the ladder in our training operation. ~~You lack~~ It gave people a ~~good~~ vocabulary. They knew what a code was and a cipher but they sure didn't learn how to break codes and ciphers from these training courses. Now they were wonderful things and they set the stage for the on the job training later on that was conducted, and I now remember clearly that we, these were the first on the job, well you ~~worked~~ went through 165 and what part of 166 was prepared at that time and then we went on to these special problems so this was the primer level. Now ~~as~~ it was a matter of classification of these things. You couldn't put too much in them because you sent them through the mail and we could just imagine them falling in the hands of the

Germans and all sorts of things like that so they were kept pretty sanitary and I think this militated against their usefulness. I found it a lot easier though to talk to somebody ~~who~~ that had taken 165 and 166 when he came on the job than somebody who hadn't. I mean it prepared them to receive training. That was the thrust of these courses but so far as making them, giving them skills, no it didn't. And to whom did we give them? At that time we wanted to use them as a screening. ~~Every~~ Any body who wanted to take these things we were glad to let them take them whether it was Army or Navy or whatever because we could tell from the courses they took and how well they did in these courses whether or not they might be a good choice to be hired and I think some of the people we hired through this way turned out to be first class cryptanalysts because it was a very straightforward and definitive way of taking ~~a~~ the measure of the individual and how well he might fit into our requirements.

Q: Do you know that Frank Raven had taken this?

A: Yes. I know that Frank Raven was one of the first guys I trained in the Navy and

in fact recover Purple keys. That's when we met. He and a couple of others instead of coming over to our place we went over there, when we met. I was impressed with Frank. I thought he was terrific because he was one of the sharpest of the Navy students. Brotherhood was another one. Brotherhood was very good. A fellow named Deeley (Ely?) that was good too and one one Navy officer, Brown, we called him Brownie. He was regular Navy but he was assigned about that time and Fabyan, who went with Rex Currier and Abe and Rosen on this junket they made to Britain. They came in about that time but the Navy didn't have much much formal training material and the courses were good for that very low very basic primer type of thing but you could do 65 and 66 exercises until you got black in the face and you still wouldn't be able to recover Purple or Red key or detransposed a code or strip an additive or that kind of a thing. That was specialized training.

Q: At what point did you senior cryptanalysts, not stop teaching because I realize you probably continue, but was there a formal school created to train cryptanalysts?

A: Yes there was a formal school but we never did stop. I think even when I left just before retirement, I was still doing a little bit of, I was involved in the educational programs. Obviously as Commandant of the school, and where I left I mean my performance there I'll not make any mention of but we did when you get to be a senior individual and if you have any impulse as a teacher you'll go back and practice a little bit I think and Abe and Kully and I all had teaching backgrounds and I think they responded more definitely than I did ~~to get and~~ if I can limit the quote senior individuals you mean old timers suits me better for the three.

Q: But there was a point where you couldn't keep up with the influx of personnel could you?

A: Absolutely not and so we had to multiply our talents by, and the best way of doing this, was to set the stage so that people, since we were busy with other things and

since we were in real short supply the way we multiply ourselves and set up training devices. One of the things we had was the training ~~bank~~ where the correspondence courses that we were talking about were handled.

End of Tape 8, Side 1

Tape 8, Side 2

Alright you ask a question and I'll try to answer it

Q: I'll ~~was~~ just ask~~ing~~ you whether Fort Monmouth and Hunt were any good, and then you can just repeat what you just said.

A: You mean Vint Hill Farms.

Q: Oh Vint Hill. Yeah

A: Well about the training that was conducted up at Fort Monmouth and Vint Hill Farms.

This I think was trivial. First place, the security considerations limited the kind of training we could conduct down there and so either the most primitive training and the most primitive kind of things that we could do. This also applied ~~to~~ up at Monmouth but one of the most useful things that came out of this, We could put courses in down there that helped us to determine whether the students that took the courses might actually had the apptitudes that we were looking for so it was sort of an aptitude screening operation rather than a conditioning operation and I would validate it and say it was

worth while just for that reason if for no other. But now after the guy was cleared for a different thing, we used to run, I'm jumping around in time now, but this is a good example. In the B3 organization which was known as the general cryptanalytic branch and which was responsible for everything except the Japanese military systems we found that it was absolutely essential to take the people who had come out of the Monmouth and Vint Hill school, these were the enlisted men. Incidentally some pretty good names came through there and ~~there were~~ the people who were being hired as civilians brought in for language skills and others because ~~be~~ the language skills had to be conditioned and we found even though they might not be good cryptanalysts it was worthwhile to run them through the school so at least they got the feel for what they were doing and learned the language and the bookbreaking, I don't think ~~we had~~ you can have a formal course for bookbreaking. You just describe the situation and then put on a practical demonstration. It's just like painting. Nobody can train somebody to be

artist. What you do is sort of tell them how to do it and then they go ahead and they become an artist themselves. Well now bookbreaking in that sense is an art and I think a very very honorable art because the skill of a bookbreaker is a combination of several skills. Virginia you can check me on this. First its how well you know the language and second how good you are to come to logical conclusions and third is a matter of patience. Well now the theoretical, the statistics and the other knowledge that are required for this, are minimal. I mean its, ~~a~~ the real basis of bookbreaking is the language. I don't know how you can say it otherwise and of course there are a lot of things you can do to simplify bookbreaking as I look at it from a cryptanalytic standpoint and that's the proper catalogues, ~~the~~ and proper techniques, ~~the~~ and proper worksheets and things like that, but The real brains of it is the application of your knowledge of the language to the situation thats, that statistical would cover from the catalogues to produce the answers to the book. Now there was a lot of bookbreaking required in the old B3 outfit because many of the South American and

Near Eastern countries had big books to recover. Now when you get into the more machine type of thing then the problem is no longer as simple as it is ~~for~~ with book-breaking and when you get into additive recovery its more complicated so you had to build on some extra training which we tried to produce. Now at that point you can ~~try~~ begin to make ~~the~~ a division in the kind of training at least in my concept that you conduct. The people who are going to work on additive type systems, it's a good idea to give them some machine training but you've got to let them know what a difference table is like, how ~~an~~ indicator solutions, I mean ~~are~~ its awfully important in my my book to understand message numbering systems and other things because they can give you good clues to the messages and ~~ultra~~ infinitely important is how to use your collateral information facilities. And this you can make into quite a pyramid of activity and you don't want to dilute that type of skills with having people subjected to mathematical statistics in courses like that because that'll go and turn them off with good language people.

Lots of good linguists just don't have the apptitude in mathematics and you scare them right out of the building if you forced them to take a course in statistics. They would patiently submit to it I'm sure but they wouldn't be happy and it wouldn't do them much good so you see begin to direct training them but most of the people who worked on machine problems needed a lot more conditioning particularly in statistics and in mechanisms and the cryptographic exemplifications of the mechanical things. What you look for, how you deal with it and that was a broader base than the language which they carried with them when they came People in the French section always selected because they were proficient in French so we didn't have to train them in that. It was just introduce them to how to use their language capability to produce the answers. Now I don't mean to run down bookbreaking or anything like that but I'm trying to put it in perspective as I saw it. Now when get over here to these people who were going to be trained in machines there were two purposes for that. One is because by that time, I'm talking about into the war, we were aware of

the Enigma type see and we were aware of the use of the [Hagelin] and we ~~got~~ had a lot of requirements for real good cryptanalysts in machine systems to, in the verification of the security our own systems, and we didn't have really much of a need for people skilled in the Japanese machine because that was already satisfied because of the experience we had gone through but we needed to change then so we began to conduct special classes.

Dan Dribben was one of the best training officers I ever had in my organization. He was good. Dan was a sharp cryptanalyst and he was a good teacher and he loved to train people and Dan Dribben just about ran a the school for us but he was a member of the technical staff you see so he didn't get over here and cover his head up with sack cloth or something. In his training program he was out there and he was looking for requirements and he, as the training officer of the technical group, identified the requirements and came back and nobody got in his way when he tried to satisfy them and I think this was a wonderful thing that we enabled Dan to be involved in because

right now we tend to formalize these things too much and we lose sight really of what the training requirements are. But now in that sense since we were small and since there were a lot of things that had to be done and since the time was short and since the instructor staff ~~was~~ were burdened with other things we took a lot of short cuts but luckily we didnt make too many mistakes. Have I answered your question now?

Q: How do you train a cryptanalyst now?

A: How do you train a cryptanalyst now? I don't know. I haven't trained one in so long I've ....

V.V. (I'll tell you sometime, I've trained two analysts -- cryptanalytic interns ....) 135

I would think maybe you might might once have sent him to Calimohos's school.

V.V. (That's at the end (OK-Thelen?) That's at the end
[illegible] the last five or eight years.
[illegible] the [illegible] other things that [illegible] ...

End of Tape 8, Side 2

~~TOP SECRET~~

Tape 9, Side 1

Q: Question is what do I remember about the early work on the Japanese military and was there any interference between the work on the Japanese diplomatic and the work on the Japanese military ~~that~~ which might have resulted in a delay in to our entry into the Japanese military systems, and I think this is a very good question that probably hasn't been dealt with anywhere else.

A: To Quickly dispose of the Japanese Purple. Just about the time the war broke out we were adequately covering it. The intercept of the Japanese diplomatic messages could be done within the U.S, the ones we were interested in, and therefore did not interfere with the interception of Japanese military which had to be conducted as close in as possible and mainly ~~in~~ from the Philippines so in that sense there was really no conflict. Oh there might have been a trivial thing where we assigned an operator to one instead of the other but this was a management thing but they did not stand up and confront

each other. We were doing as well as we could with each so there was no intercept problems resulting from the possible conflict between the two. The big problem in the Japanese military is we just didn't have enough intercept stations close in to pick up the traffic ~~uniformity~~ in the quantity that was needed at that time. Now so far as the processing and exploitation was concerned Purple was dead cold. We had it covered. We were predicting the keys and we were collaborating with the Navy and then split the load between us and the Navy and so most of the Purple people, the Furners and the Smalls, ~~and~~ the others, the Sammy Snyders, were being used in support of other problems such as our COMSEC operation and sort of managing and doing the difficult keys, The ones, well, recovering some Purple keys under certain circumstances could be pretty difficult. ~~None that~~ Normally it was a very easy thing but a few things would come up like the use of a station chiefs code which was then enciphered by the Purple and the average key

recoverer in the Purple wouldn't know what to do with these messages so Farner and Small and the rest of us who had been involved in the recovery of Purple would be called in to deal with these problems. Fortunately these were not numerous so we had a dedicated group on the Purple, split between the Army and Navy and these were ~~still~~ skilled specialists ~~that~~ and could, well, some of their skills could have been used in the Japanese military, they weren't really needed because Kully who was put in charge of the Japanese military had been given a staff of people specially, sort of trained for this kind of problem because Japanese military problem was in the early diagnostic stage. Now it took some time for Kully and the folks to begin to take the measure of the problem to determine t~~he effect of~~ exactly what was used and how to attack it because all they had was a bunch of intercepts and no continuity, ~~Nexxxxxxxxxx~~ no sample Japanese systems and here Yardley's reports were not much good. He mentioned a few systems but

and I'm talking about new special reports that Yardley put together in a contact with the Chief Signal Officer after he had returned from his duty in China and I'm not talking about the Black Chamber reports. I think that's important because these are two different points in time and so we, well, Yardley's information was about as good as we had and it wasn't good. It was trifling, trivial or whatever term you want to put on it and we probably Kully would have done just as well if he hadn't had it really I think because ~~we~~ we'd(?) spent some time confirming what Yardley had reported and we puzzled about it and we had to answer a lot of questions because the Chief Signal Officer wanted to know how good is this thing. Didn't Yardley tell you how to do this? Why can't you do it part of? So but and so it was more of a bother than it was a help but now keep in mind that the Japanese military system was very well designed. It was an enciphered code. A sort of additive encipherred code. I believe initially it used normal arithmetic and then they got into a sort of crypto substitution where instead of

using the normal device of addition they had mixed, mixed numerical sequences sort of like a mixed alphabet problem versus the vigenère square with normal alphabets because the normal additive just to overexplain this thing, the normal additive is nothing but a vigenère square using the ten digits pushed in a forward or backward mode depending on whether its an additive or subtractive and the Japanese did a little bit more to that. ~~For that~~. They scrambled the sequences and they used the vigenère principle so that your recollection of the tricks that you'd learned about two plus two equaling four when we were in kindergarten couldn't be applied so you had to look up two and two ~~and the~~ in a matrix and find out the what the equivalent was. Now this was a pretty I'm talking now about cryptographically, I don't recall how the Japs did it, but the cryptographic effect of this non-normal arithmetic was just what I described. Now this makes a problem of different dimension of difficulty when you do something like that because ~~instead of~~ the normal additive thing because, oh a lot of things. You can set up

your accounting machines to do normal arithmetic and then you have to make a very special arrangement to get them to go into the non~~un~~normal mode so the problem was not an easy one and the breakthrough was based on a lot of examination of material, diagnostic work which if you've got some inspired people around can be very short but if the problem is difficult and the people who are working on it just haven't had the opportunity or you haven't been fortunate enough to cap an inspiration that makes the golden guess you've just got to dredge it out. You've got to accumulate enough traffic, sort of oddball messages, bust and all this other tricks of the trade ~~a something~~ to give you kind of clear indication of just what you're up against and it took some time to establish and accumulate enough traffic. The Japs were pretty clever. They didn't change, didn't hold their keys in use for a long time. They changed them frequently so about the time you get a handhold in one period the it would slip away from ~~them~~ you and you'd be trying to corner another greased pig of a second period. So it was not an easy

problem and was not one which could be done overnight. Now the Purple system which in retrospect is a lot less cumbersome to solve. Remember it took 18 months and we had the background of the Red machine and we had to accumulate enough data and determine exactly how the key system worked for each one of the periods then reduce them to a sort of simple base since the system so carefully defined and diagnosed as the Purple was, having required 18 months to get it under control, you can I would say that the Japanese military problem was much greater magnitude and I think Kully's group, the B2 group which was sort of the early outgrowth of the organizational structure, the idea here being let's isolate the military problem, let's put all the power that we can bring to bear on it, every skill that's needed, let's give it priority. I think that came into being pretty well just around Pearl Harbor and we began to realize it of course when the Japs hit at Pearl Harbor. Well there was no question but what these were

the rules that you applied ~~for~~ to the SIS and you put all, you didn't deny the military problem anything that it needed. Now I remember this latter pretty pretty vividly because I was in B3 and I had certain requirements that I hope I was able to be a good neighbor to Kully and didn't deny him anything we had. We really we really ~~try~~ tried to support this. ~~It was across~~ In the past, the SIS support to the B2 problem that that was the rule of the day. Now I think as we get deeper into the war we find certain other aspects to the military problem that I recall and really the one to talk to about this is Dr. Kullback but I remember this. The GCHQ people early on let it become clear that they were so busy dealing with the German problem that they could not afford any resources to divert ~~the~~ any resources to the Japanese military problem but simply turned that over to the folks down at Brisbane and here again we find that great emphasis was placed ~~on~~ in the support of Brisbane. Akin had gone down there as Chief Signal Officer and he said he wasn't ignorant of what was needed and he certainly knew how to get it and if there had been

any reluctance in Washington to give the Brisbane group any support that Akin would have known how to defeat it. An example of this is early on Dr. Sinkov was assigned and he went down to Brisbane and between Brisbane and Washington I think the bulk of the important work was done on the military problem.

Q: Did you support Brisbane in terms of additional research?

A: We tried to give Brisbane anything that we could as I recollect. I 'm not aware of the details because there was a lot of exchange between B2 the Japanese military. We there was one thing we learned early on in the war and it was a good lesson. You should have no interferring channels or echelons between in in your liaison between technical units. In other words B2 dealt directly. Abe and Kully communicated directly with each other. It was no overview in terms of the supervision of the officer in charge of NSA but Kully and Abe had complete latitude in what they exchanged. Of course they the head of ASA needed to know what was going on and he got appropriately briefed by Kully and

I'm sure Akin had almost daily conversations with Sinkov but the rapport was so good that a lot of this material didn't have to be documented. There was no delay like formal reports ~~or~~ and stuff like that. We usually did the job and then when we got around to it we'd write up the report on it and now inevitably there will be little differences of opinions which if not watched can get out of control. I can remember some cases where it looked like there was going to be a difference but these were usually resolved without acrimony and appropriately and it was more a result of the distance and also we couldn't very well have people ~~coming~~ shuffling back and forth between Brisbane and Washington which I think probably would have been an advantage that might have accrued. [It's so] It was a little (?) different between the navy unit working on the Bombe and our work on Madam X over at Arlington Hall Station because we have people going back and forth between Washington and Britain pretty frequently and this personal insight into the problems on both sides in discussions eyeball to eyeball, sort of enabled us to get along. I can remember

I can't remember any difference between the technical outfits ~~and~~ in Arlington Hall Station and GCHQ. The closest we can to it I think was in the work on the military attache system. John Tiltman broke it sometime after the start of the war. He got the entry into the military attache system which was a very important stream of traffic and the, looking back at the fact that the British had said these words about the Japanese military and this is the military attache - that we cannot divert people from the Enigma problem to work ~~along~~ on the Japanese military. When we got down to the military attache problem which had been broken by Tiltman at Bletchley then there was a bit of sorting out of whether or not the work would be done over in GCHQ or Washington so we were anxious and willing and of course under the Clarke philosophy of what to do about problems why I had no choice but to set up a unit to work on it and so in working out the details of how we would divide the effort which can be a

very complicated problem. I mean do you work on odd days and even days like that stupid arrangement that the Army and Navy made about the Purple or do you take the front end of the book and the last end of the book or do you do it by indicator. We had to work out some reasonable way of splitting the effort out ~~and~~ but we did and in this case I think the biggest advantage well the greatest thing, the greatest help we had was surefire and rapid communications carrying the technical information. We had special system set up between us and GCHQ which could carry all the technical information and then there was another little bit of the same sort of thing when we got into the GEE problem because the UK was just as interested in that German one time pad, both for cryptanalytic advancement and for the intelligence that could be produced so we had to make a similar division in the effort there but these are trivial things and I don't want to leave the impression here to the listener that there was any big problem there. It was a matter of the practical resolution, the

determination that the easiest way of doing something had to be done and of course our national perogatives had to be satisfied. Clarke's requirement that we become involved in every problem, big, little, old or young was a thing that I had to keep in mind and I think there was a similar attitude on the part of GCHQ and I think a very reasonable thing because nobody at that time and I think its important that people today keep what I'm about to say in mind, In terms of WWII we didn't know whether there would be continued collaboration between the US and Britain in the cryptologic field. Most of us expected that the collaboration would end with cessation of hostilities you know kind of break off and then just disappear like... Like it did in WWI, the collaboration between the French and the US and of course we never did get deeply into OB40 but there was a little collaboration. We expected that kind of a principle to apply at the end of WWII. Fortunately it didn't but now people today I'm sure get the feeling that there

has always been this collaboration. It's just like it was in the Bible. There was always God, there was always a church but we were pagans in those days and honestly I I I did a lot of thinking about the wisdom of going too deeply into collaboration with the British and for what its worth I'll try to drag out the three points that were most significant in making the determination to go ahead. First was the geography for intercept purposes. We could see ourselves being pulled back to the continent you see and we remembered vividly the difficulties we had in collecting Japanese military and so I think this is a good point. This would promote which would make us want to collaborate with the British because they had a capabilities for doing intercept in many points of the world. You sort of think of the British empire and how it would sort of delinated in those days and it gives you a pretty good intercept picture. The second thing is we had learned to admire the British technical competence. We found they, we figured that together we could do much better technically

than we could separately and we allowed for the difference in national objectives because we went on the assumption that the British organization would be in support of ~~the~~ UK requirements and ours would have to be in support of US requirements but again the technical collaboration would be important because the emphasis would be found in terms of exploitation and intercept. The intercept based on your intelligence requirements and you exploit the traffic to satisfy the same requirements so we didn't see too much conflict in that regard because both of us would have needed the basic traffic to break into the system and that's what we wanted and then the third point which is ~~an~~ the obvious and simple one that together we could do much better than we could separate and it might be a good thing over the years but the thing that really drove it home and made the decision clear was the attitude of the Russians at Potsdam when it became clear that the war, the world tension wasn't over. The Russians were the

natural target, intelligence target from that point out. When that became clear then I think any doubts about the need for us to continue our collaboration with the British were removed. Now I may have wandered around here speaking the obvious but I think my recollection of the attitude of the discussions is ~~mostly~~ grossly accurate. The details might vary but this was the sense of the discussion and I also think that it was a good thing that we made that decision.

Q: Could you give us your recollections in the whole time period beginning from the 1930s April 1930 through your association with, your relationship with Mr. Friedman and your evaluation.

H.S.

A: Well this would not be very subjective. I'm reluctant to do this but in the sense of putting down how Rowlett feels and in the sense that other people, unfortunately Friedman can't, and that's basically my reluctance to do this but I'll do it because I think it might be useful provided that whoever listens to what I say remembers that this is entirely

subjective and may not correct but is just what I saw. Well I'll just go back to the first time I met Friedman. I was impressed with him and as he went on as our teacher the greater admiration developed as time went on for what Friedman could accomplish and we looked on whatever Friedman said as sort of as being the word of God and that you didn't argue with it and he enjoyed this because Friedman liked to be liked and he liked to be admired and I think he'd had a little bit more of this than people like to see in other people but I believe he it wasn't any worse in Friedman than it was in any of the rest of us except he may have let it show through a bit more than others. He wasn't, he didn't run out of the limelight. He sort of loitered while it was pointing in his direction and I don't hold this against him. I think I would do the same thing and do do the same thing when the opportunity is presented. I guess what happened is that Friedman got more opportunities than maybe a lot of other people so they got a little bit jealous ~~with~~ of the frequency with which he got the limelight. Friedman

was proud and he did have some ~~advantages~~ vanity and I think what I just said is the part of that vanity but he also when he deliberated about a thing ~~he was~~ he could be fair about it but he had to deliberate. He had to think about it. I think his immediate personal reaction ~~was~~ to now this is Dr. Headshrinker Rowlett talking and I got no business being this ~~sub~~ subjective (?) but I'll go ahead and do it. I think Friedman's first thought was the one that usually show ed through and then if he had to back off and think about it he would ~~just~~ assume an entirely different attitude and it was essentially fair. I mean of course it was sort of like in a business deal. You looked out for yourself. Billy looked out for himself but I don't think ~~he~~ Billy was dishonest. I don't think he would intentionally steal and I can't find any place where Billy in my knowledge of him and I knew him a long time that after this deliberation that he had done that Billy was essentially dishonest. Now I know that he was a very thoughtful man and he was a good planner. He could look ahead and he could set up situations which are

favorable to him but don't we all. I mean that's how you live in the jungle so in that sense this is not a derogatory remark I'm making about Friedman but he was a good business man so far as his own interests were concerned. 354 Now I think I've put a pretty good background. My relations with Friedman were pretty direct and personal and calculated because some some personality conflict between them because very simple reason that I had 10 days seniority on Kully and 20 days on Abe and in the military view this was enough to make me the senior of the three whether I had, whether I merited it, whether I had earned it personally or not but so it was an automatic thing rather than something you had to go out and compete for. Well this bothered Friedman a little bit because he wanted us all to be on a par and he didn't like for the automatic selection to be made and about the only thing automatic that Friedman liked was drawing straws where everybody had an equal chance and I think this was fair. Many times I would step back, now I'm being subjective about Frank Rowlett but this is

what I found to be the best way of dealing with it instead of demanding my rights based on this microscopic difference of 10 days I found that the thing I could do was to go ahead and accept the straw drawing which I think was right because well you do like your personal advantage but you don't want, you don't want to lose your integrity in seeking it so in this sense there was always the feeling that I had to be very careful because I might lose something because my experiences by losing this little advantage I had I was always on the short end of the stick you see and my lightning rods went up a little bit faster and so I watched Friedman and the things he did a little bit more closely than would this have not had happened. But I don't know to this day I don't know which one of us would have been selected if it had been true competition but the simple fact is I did have that slight edge and this bugged Friedman throughout because there were certain times when he honestly felt that Abe or Kully ought to be chosen to deal with the problem but I was chosen by Akin and

others because they were in the habit of doing ~~that.~~ this I think Friedman felt a little nervous about this. Now let me say a few things about how Friedman dealt with the advancement of the technical situation for which he was responsible. I think Friedman had more vision, that is good vision about the future of the cryptologic effort in the US than anybody else in that time frame. I think Friedman became impatient with us, his students, and I think he became more impatient with the bureaucracy that he had to battle as he looked toward achievement of these goals. Not ~~at~~ up but because he had great support in terms of the Chief Signal Officer and G2 but I think he did become ~~very~~ impatient with trying to fight the bureaucratic influences which inhibited the prompt response to his requirements or the cryptologic requirements as he saw them and I think this this made him feel, I mean he sensed this and he resented it and he reacted to it and I believe at times this, impatience is ~~a~~ probably the better word, he became really impatient with it, ~~his~~ this impatience would show through and cause him to try to devise

ways and means of getting around the obstructions that he recognized were in his way. If I recall when I get down to talking about some of the cipher machine developments I'll give an example of this but now this is the kind of image that I remember of Friedman and I can also remember sort of the transition from the point where Friedman was the last word in cryptology to where the people he had trained who had come behind him began to become recognized for their own actions. Friedman's overall reaction to this was very good but I think he loved to be the father and to carry the the ultimate an expertise image and I think maybe he did react a little bit personally to the emergence of a group of people and the fact that this had now become a team organization rather than a one man and I don't use this in a derogatory sense. The situation where one person would grandstand which was quite tolerable when Friedman was there by himself but now that the team should get the credit and Friedman worked very hard to insure that the team got the credit but I think he kind of felt a little

bit of lonesomeness that he couldn't you know at times take full credit for some of these wonderful things that were done but let me add right quick he was as fair as he could be about it so there's no element of unfairness here but sort of his personal reaction of I wish I could take full credit for that but I can't really take it so I'll give it where it belongs. I mean I said it right and I wish I could have taken full credit for but since I didn't do it I can't and I'll put the credit where it belongs. I think I have put Friedman's personality reaction to the upsurgence of technical competence in a nice fairly spoken package in those few words and I 'm glad I said them because that is the way it looked to me. Now one of the problems Friedman had and now I'm talking about Friedman's personality is that he did have a well he did have to have medical attention. This came on and I think it's been erroneously presented by David Kahn for example and some of the other writers but Kahn's the one I remember. Actually what happened is that there was a combination of things. I don't know whether there was

anything in Friedman's personal family life that impinged on this. He never talked about his family. We knew Mrs. Friedman but his family problems never he never brought to the office and I wasn't aware of any but there were certain other things. One, the requirements for cipher systems, cryptography, US requirements Friedman bore the brunt of that. The and the pressure was considerable for these reasons. That the Chief Signal Officer and the War Department recognized the requirement for the best possible type of system for US usage. They had imagined that they had this requirement satisfied with the M134T1 but when Friedman had to expose one, ~~of~~ the difficulties of that we had encountered in the simple matter of technical production of tapes and two, that there was a different, alternate idea that ought to be adopted I think he was rebuffed considerably on the upper level and now let me tell the story I promised to earlier. The reason the AB~~B~~A was developed was because it was evident particularly to those of us who were involved in the day to day production of the key tape material

that it wasn't a viable system because one, the job of making the tapes was too great, two, the amount, the sheer bulk of material that had to be stored in each each coderoom where the machine was held was pretty great. It wasn't intolerable but still it was a problem so your physical security problem was pretty great and three, that the material the key tapes were intended to be used over and over again and the flimsy tape that we had to prepare got ~~to~~ torn up after a couple of uses so it was in effect a one time tape system not by design but simply because it worked out that way. The tapes just wouldn't last that long. Maybe a two or three time tape. With care you could get five or six encipherments out of a tape so we had gone to a very thick, hard parchment type of tape and it had a little bit of some kind of abrasive in it like [pulajarets] phonetic or what have you and the the punches which cut the holes in the tape got dull and they would just make indentations in it and one indentation is enough to destroy the usefulness of the tape because then its different from the other tapes. The wheel

doesn't move at the right time and the message becomes ~~un~~ indecipherable and there's not much you can do about it unless you're a cryptanalyst and then it becomes two or three weeks before you could produce the text so the material just simply wouldn't stand up under usage so I think once Friedman accepted this ~~and~~ that he went out and went gung-ho to achieve, to throw out the M134T1 and replace it with something better using a different principle with the key generator which is essentially what the AB~~B~~A was so when he went up to the Chief Signal Officer and presented this alternate solution and requested support, monies, he got a shock and I remember how dejected he looked when he came back. He knew that there was something, a few thousand dollars, something like 2500 dollars or some trivial amount like that, set aside for research and development in the code production program and that this could be expended up at the Signal Corps laboratory up at Fort Monmouth. Well when he went up to request that some work be undertaken to do, to prove the new key generator principle and they said "No. We don't have any money" and he said sort of "Well what

about that budget, the $2500 or whatever sum it was" and they said "Well we don't have that" and his question was "Well what happened to it" and they didn't, evidently couldn't give a clear answer and after a little research and investigation they found out that the money had been turned over to the laboratories and that George Graham, Chief Engineer, up there, I believe it was Graham George Graham the last name was Graham had used it in the development of a field cipher device and that nobody in Washington knew about it. The Signal Corps Laboratory had undertaken this on their own. Well this was a real slap in the face to Friedman because he thought he had a pretty good relationship. He would regularly go up to Fort Monmouth and have discussions with [Graham ?] and when he found out this job had been undertaken and his money, the SIS research and development money, had been used for it he was fit to be tied. I mean he was officially browned off and he was personally hurt by this kind of a thing and I think that it was a dirty trick that they played on him. He was very dejected about

this. It took him several several days to recover from it and the net result was that finally Friedman was sent up to look at this device to insure you know that it was a pretty good thing. Well when he went back and said I don't think much of this device he was told well look there's just no money in this budget and next years budget, its a tight time Billy. I don't think we can afford to go into this new system, this new type of key generator system, and by this time Friedman was dedicated to the replacement of the M134T1. His own brainchild now. He had to reject you see and had to promote something that wasn't entirely his own and I think Friedman should be admired for the way he conducted himself under these circumstances because this could be damaging you know under some circumstances from a professional standpoint. But fortunately the people up at the Chief Signal Officer took the attitude that it was a result of Friedman's development of the SIS and this was an SIS product rather than just being a Friedman product so I don't think he was denied any of the personal

credit that he should have deserved for it and that is the truth, the true situation, as I saw it from where I sat being involved in it and then we, since I was working very closely with Friedman on this improvement of the M134T1, I got a pretty good insight ~~on~~ into how he personally felt about it but it didn't deter us from going ahead and doing the groundwork and examinatio of the principle and working out the logic of the machine.

End of Tape 9, Side 1

Tape 9, Side 2

of course this shock of finding that we had no funds ~~for~~ to develop~~ing~~ this idea which now, by now had seized well particularly Friedman and myself because we were the prime movers of this modification of the M134T1, ~~it~~ was a great disappointment and fortunately within a few weeks after the word had come that there were no funds some representatives from the Navy came over in one of their infrequent but most important discussions, the technical problems particularly of cryptography that occurred in those days between the Army and Navy, it became clear from what the Navy representative said (1) they were dissatified with the prospects ~~of~~ for developing ~~the~~ a cipher machine in terms of the devices or the ideas or the logic of the machines which they were examining and were committed to and they felt like that they had go into into something entirely different to achieve the requirements, to meet the requirements, that the Navy had set for itself,

so that they had nothing on the drawing board that satisfied them and they were looking for new ideas. That's the sum and substance of it and ~~(2)~~ second, that they could immediately ~~work~~ embark on a program because they had plenty of funds and I don't know how true this is but I will tell you like it sounded to me at the time. They had something like a million bucks of no-year money that Mr. Roosevelt, thats Franklin D., as I think one of the Undersecretaries of the Navy had procured for them and if they didn't use the money this year it could be carried over to several years you see. It didn't have to be accounted for and turned back in in term~~s~~ of a one year deal. WEll now these two things (1) the Navy was looking for ideas (2) they had the money and were ready and willing and ready to go if they had a good idea really excited Friedman and I think I think we had some discussion about it. Friedman was intrigued by it and I was a good sounding board to knock it off of so his feeling was that, "What an opportunity." If the Army doesn't have the funds they have the need but the Navy has the funds and if we

could just some how or other get the Navy to test this thing out we'd be ahead, and so he decided to take it up with the Chief Signal Officer and see if the Chief Signal Officer was willing on this ~~was~~ sort of a proposition: (1) We don't have the funds Mr. Chief Signal Officer (2) we have a good idea (3) it needs to be tested (4) We the technical people think its much better than anything else we've seen before. We think that this is the best that's ever been produced and we'd like to have it available ~~over at~~ for the Signal Corps. Ergo, your permission to take this up with the Navy and to encourage them to test it out is requested and when it was presented to the Chief Signal Officer under those terms affirmative permission was given and Friedman was allowed to present these ideas to the Navy on the premise that if the Navy wanted to carry on with the project and use it ~~with~~ in their own cipher machines, the Navy cipher machines, that the Chief Signal Officer would present no objections but that the Chief Signal Officer would want access to all the results and the benefits of the Navy research and this was, seemed to be a very fair prospect. Well now I'm

going to be a little bit personal in the words that follow because I was involved in this thing as the co-inventor of it and I think my personal reactions may be useful from a historical standpoint, whether or not they are indeed subjective, so I'll not apologize for that. I'll just go ahead and be subjective. Well when Friedman got this permission from the Chief Signal Officer, he came back and told me about it and I was delighted because I thought it was a good idea and so Friedman made arrangements then to set up a meeting and brought over well I think he first disclosed it to Admiral Wenger, who was at that time Commander. I was not present at the disclosure because Friedman and Wenger always had these sort of private meetings and they discussed a lot of things and I think this was probably a good thing on Friedman's part because the Navy was very reluctant to talk about sensitive things outside of a selected few people and Friedman already had the entree, developed this rapport with Wenger and for

Abe or Kully or me or all of us to be involved in those very very private discussions would have inhibited the exchange of information, certainly the flow from the Navy to the Army, and so I think this was right and proper and it was in one of those, Friedman set up one of those meetings, and revealed, I'd prepared the drawings and everything else to make sure he had the right kind of a package in front of him so he could put it forward in the best light in the simplest terms. So he gave this to Wenger, presented it to him, and then after the meeting he came in and told me Wenger's reaction. He said Wenger was amazed because the concept is so new and different Wenger wanted to take it back and further discuss it over at the Navy and that we'd be hearing from him in due course. Well we waited sort of. I waited anxiously and I think Friedman did and every chance I got to see him we talked about this and wondered what the Navy was going to do with it because we were really sold on it. It was a damn good idea we thought and it must have been, otherwise things that

happened to it wouldn't have. Then several days later Friedman got a call from Wenger that he wanted to bring over a group of navy officers from other parts of the Navy and have some more discussions about this in Friedman's office. Well Friedman told me about this and that it was going to come up and of course I was very anxious and I helped Friedman get his package of material together for this meeting so Friedman goes out and has to answer a lot of questions. He rebriefs them ~~He briefed him~~ fully on this device and answers a lot of questions and there was considerable excitment evidently because as Friedman reported to me after the meeting that they had a lot of questions. They were very serious about it. They ~~apparently~~ had no words of praise but he could tell from ~~by~~ their reaction they were really carefully excited. They just couldn't bury that and he sort of implied that he didnt think ~~that~~ Wenger had really understood what he was explaining to Wenger and that ~~but~~ now he had had a good opportunity to make a proper presentation because some of the people there were much more familiar with electro-mechanical matters than Wenger obviously was so we were real excited. We were waiting

momentarily to get ~~our~~ the great big check saying that look your article has been accepted. You're going to get full credit for this. It's a wonderful thing. ~~You're~~ We're going to have a best seller sort of. (laughter) But then a week went on, two weeks went on, not a word from the Navy and by this time I began to push Friedman ~~and~~ a little bit; I said "Look why don't you call Wenger up and get a report on this meeting?" and he was most reluctant, not that... I don't know why he was. He just didn't want to demean himself to showing any curiosity. I think he was a very proud man and finally I think it got the better of him and so he made a date with Wenger and put the question to Wenger. Well what do you folks think about it? Well I don't, I wasn't there so I don't know what transpired but the report that Friedman gave to me was that he didn't think the Navy understood it because the consensus which Wenger reported as a result of the briefing Friedman had given the second, the second briefing to Wenger and others not just to Wenger alone

said he didn't think they fully understood the principle because they ~~didn't think~~ said it would be work. It was impractical. Well this was sort of a second order disappointment. Friedman wasn't nearly as disappointed with this rejection of the idea as he was with his original presentation to the Chief Signal Officer and so we, I was disappointed too. We just went on. We had a lot of other things to do so we didn't cry in our beer too long about this. Now I think its important to note with regard to Friedman and his role here that he was able to start out that which was best and find ways and means of getting it adopted even by finding ways of getting around the pretty flat budget limitation in the Signal Corps because he took advantage of the opportunity presented by the Navy's funds to get this idea promoted and as you look back ~~in~~ from history it was a wonderful thing that happened. Well things went on for some time without any reaction from the Navy and among other things Major William O. Reeder joined the War Plans and Training Division and Friedman went on a junket overseas to install the M134T1s and while he ~~was away, this is~~ was I think while we were working on the, it was I

think we were beginning to ~~tap~~ attack the Purple machine. The Purple machine had come into use and we were working very closely with the Navy technical group on trying to get into the Purple machine. Now I bring in the Purple machine here ~~now~~ because this was several weeks ~~several months~~ now, after Friedman had reported to me that the Navy had rejected the idea. Ham Wright and I were sitting at my desk over in the Munitions Building looking at, sort of reviewing, what we had cryptanalytically developed about the logic of the Purple machine and the cryptanalytic attacks that we might mount on it and Ham was sitting there and we were discussing the possible types of machines that might be used and Hamm made the remark. He ~~said~~ says, "By golly Frank he says this might, they might have invented the kind of principles that we are using in our new Navy machine. And I said "Well it might" and you know principles come up. And I said "I didn't know you had a new Navy machine and he says "Oh yeah, I'll tell you about it." So help me ~~and~~ this is the truth now. Hamm ~~sat down~~ there and he developed the logic that,

of the system that Friedman had revealed to Wenger and the other Navy people and clearly indicated that the key generator that was being involved in this Navy machine was exactly the one that we wanted to have involved in the Army machine that we'd been denied the opportunity to develop because the funds weren't available. Well I didn't let on to ~~about~~ Hamm and so I sort of ~~started~~ to asked him, well, ~~I said~~ "Where did you get these ideas?" sort of and he said "Well Wenger got them somewhere." you see and I said "Well what is the status of it?" and he says "Well we're having one built." He says "It'll be down here and I'll see if I can't arrange for you to look at it." and this, well I sort of sat there and kept my cool thinking about this because I wondered my goodness what's going on here sort of. I know where Wenger got the idea but why didn't the Navy tell Friedman about it? Well as soon as Hamm left I go out and seek out Major Reeder who is a very easy guy to talk to and I ask him if I can close the door and

he says "Yes" and I closed the door and I told him what happened and I went back and I said "Now it seems to me that this is exactly the information that Friedman had given Wenger several months ago before you were here and that the Navy had told us that they weren't going to do anything about it". and he says "Well what do you think about it Frank" sort of and I said "I think its a damn good thing. I'm glad they've done it". He says "Well I'd hoped you'd feel that way about it". He said "I was talking to the Navy people a couple of weeks ago and they have invited us to send you and Friedman and Sinkov and Kullback over to look at the pilot model of their new cipher machine in which had been adopted the principles that Friedman had revealed to Wenger and this is part of their reciprocation for the use of these ideas" and he said "The only reason that we hadn't gone over earlier is that Friedman's out of the country and they wanted to wait until he comes back." Well I tell this as an interesting episode but it sort of

TOP SECRET

HANDLE VIA COMINT CHANNELS ONLY

shows how the Army and Navy were collaborating in those days and really the barriers between the two so far as the exchange of both technical and tightly held operational information is concerned. Well later on we went over and looked at the thing and it was a joy to and delight to see what a magnificent job the Navy had done on this. The pilot model was not perfect but it was so much better than any cipher machine that had ever been built yet that I just couldn't keep my hands off of it. I got the opportunity to sit down to encipher and decipher a message and the doggone thing worked and I watched those wheels go round with great glee and enjoyment and so did Friedman. Abe and Kully, poor fellows, they got elbowed out because they hadn't been as close to this thing as Friedman and I had and we just took over. We couldn't leave our toy alone and ~~with~~ the consensus of all four of us, Friedman, Abe, Kully and myself, was that this was a terrific thing. That we had a cipher machine here now that could answer better than anything else certainly and probably better than any other nation could produce

to answer the requirements for rapid encipherment that from Army level on up. We weren't thinking about this in terms of division because of a lot of considerations but this was from Army right on up to overseas commands to headquarters, coderooms, provided the US, both the Army and Navy, and we were thinking not just Army and the government because we were thinking about the State Department too, could provide us with a terrific cipher machine device. Well needless to say Friedman was elated by this and I think felt that he had, that this was a great step forward, that he was personally involved in both from the technical and managerial standpoint and I think he got a lot of personal satisfaction out of this thing and I sit here and attest that Friedman ought to get, that there is no measure of how much credit Friedman should get for this, because I think it was sort of he overcame two obstacles, the technical obstacle and the management obstacle to achieve this, the introduction of this real good principle. Now in todays view this may not amount to

much but in the view of 1938, 39 and 40 this was a terrific advance and I think the WWII experiences bore out the fact that we did have an invulnerable system.

As a part of the follow-on and now that we had seen the importance of the cryptographic idea, Friedman approached me and said we've got to make sure now that this is properly patented and someday we'll have to sort out our contribution and so I went to work writing up, drafting the, or updating the drafts for patent application that we had put in, you see, to make sure that the concepts, all the concepts, were appropriately covered and the particular one adopted by the Navy was effectively protrayed because when you get to the patent you don't want to find youself in the loophole of having the practical device looking different from ~~than~~ what the patent application claimed. So that was the first thrust. Then question of, sort of division of credit, came up on this. Friedman sort of thought that we ought to do this pretty soon. I was most reluctant to do it because how do you sort out a thing like that. Finally we hammered out a paper which we both agreed on and signed and then we used this sort of as a basis for future ~~options.~~ actions.

I think its interesting, and now again this is subjective, that all the things, ~~the~~ you see three of us got ~~military~~ monetary awards from the Congress for what we had done. It was Friedman first followed by Safford and then myself. As I look at it the only thing, the big reason for this, was the work done in communications, cryptography, so I think that Friedman's application for this Congressional award, had it not included the ABBA, would have been most difficult. It would have been a very difficult job for him to receive it but I think with ~~that~~ the ABBA in there it was pretty much assured. Now Friedman broke the way. Then Safford put in an application and if you look at the papers that Safford had submitted the thing that I identify ~~with~~ in my knowledge, ~~my~~ very personal knowledge, of the things ~~that~~ which were presented by Safford, the one of significance was again the ECM, and of course we called it the ABBA and the Navy called it the ECM so then having these two awards presented one to Safford and one to Friedman it would have been kind of stupid for me not to put in for my hundred grand because I was as deeply involved in the ABBA as they were, so I think sort of as an aside it was the work on the ABBA/ECM that enabled three of

us out of the cryptanalytic organizations ~~in~~ of the Army and Navy to to get monetary recognition for ~~a~~ our contributions and I throw that in for what its worth. Actually in my case the thing that bothered me is that the newspapers twisted the thing around and said that this is for the work on the Japanese codes. Somehow or other that ~~thing~~ came out but thats the for the birds (chuckle). It was strictly on the merits of the cryptographic contribution that these awards were made. The COMINT side of it never came into question and the press is in error in that sense. Now I think going into such detail into the development of the AB~~B~~A principle~~s~~ and how that worked out I've gotten away from the main stream of thought here but I do believe ~~that~~ this example was significant of the kind of role that Friedman ~~p~~played in his capacity as head of the technical effort in the Signal Intelligence Service. Now of course we've overlapped in time. Other things were involved while we were working on the is AB~~B~~A/ECM because this didn't happen overnight. It took several months for it to come about. Now Friedman of

course continued as the head of the organization, its Director, and thats a good word for it. He was the Director of the technical effort, cryptologic effort, and that embraces both cryptanalytics and cryptography in the SIS and he was aware of the management problems and dealt with them but most of the administrative problems were dealt with by Akin and Reeder and others who were in the office of the War Plans and Training Division because their concept was to keep Friedman as free of these administrative duties as they could so that he could bring his talents, his rare talents, to bear on the technical advancement of the ~~this~~ activity. Well Friedman, when he came back from this trip abroad distributing the devices to the overseas commands, the M134T1, when he came back he had a little catching up to do and of course we were involved with this business of getting the ECM, once the Navy had produced the pilot model, then we had to go to make sure that this satisfied the Army requirements and would be suitable for the

Army because early on we envisioned a contract for the same chassis and the same wheels but the wiring of the wheels would be different. We wanted the same chassis and the same instrumentation between the Army and Navy because then the contract problems would be greatly simplified and the cryptographic difference could be insured because of the design of the wheels and the critical thing was the wiring of the wheels there, so if we had differently wired wheels we could send out in sets, we could still use the same chassis and the same instrumentation throughout. Probably the major difference was the power supply because in the Navy usage the shore stations and larger naval, what's the word, vessels had plenty of power on them but for Army use and Army headquarters in particular there might not be the 120~~V~~ volts DC which I believe the Navy equipment was designed for, and we had to use maybe a ~~Navy~~ local generator or in an emergency situation run the thing off of a jeep power supply or a truck power supply so we had to provide for the 24- ~~120V~~ vol operation which was permitted by certain vehicles' electrical system and there were

differences like that. The Navy had a thing about, one which to Friedman, Abe, Kully and me seemed a trivial cryptographic thing. They wanted to incorporate some means of shifting the wiring manually which, well, shifting the wiring between the key generator and the rotors, stepping mechanisms, and we finally argued that this was trivial and we'd go ahead and accept the Navy version of it because the Navy was putting emphasis on simplicity of operation and we were putting emphasis on using the best cryptography but the difference between the two was so trivial we finally decided that we would not make a argument about this. The job done by the Navy was so good, though, there was very little we could contribute to it except check it out for its cryptographic, make sure the best principles were used and that some dangerous principle might exemplification of the principle, might not be involved or incorporated in the device when it was manufactured by the contractor, which was IT&T, so essentially we accepted the Navy device and it took a lot of work to get this done and it interferred very little with the work done

by the Purple section because we had Furner and Small and the other group carrying on and we had the Navy people still working on it at that time and also we, it was a lot of routine spade work that had to be accomplished before we could get down and make the big pitch, make the big attack, break through. I guess at that time the thing that was bothering everybody the most was not our work on cryptography but the fact that we had not yet solved the Purple. This was about six of seven months after the, Friedman got back and G2 was beginning to get rested and want, wanted badly, to read the text of the messages in the Purple because the use of the Purple system was, it carri the important traffic between Washington and Tokyo, London, Rome, Berlin. These four capitals. Of course Moscow was important, but these four capitals were high priority and these were, there were seven or eight. I think there was Ankara. Distribution was Washington, Tokyo, Tokyo, Washington, Rome, Berlin, London, Paris, Ankara, Moscow, Warsa I think thats, there may have been one more, but this see G2 couldn't get this traffic

because it was on the Purple and so they wanted this traffic and they said get on with it. So the Chief Signal Officer called Billy in and said drop everything and concentrate on this Purple. Give it everything you need but you Billy, you senior cryptanalysts, go down there and solve the Purple you see. Well Friedman I think tried to explain that he wasn't, he, solely, was contributing everything he could. He had a good team working for him. They said anyhow Billy drop it. I think this bothered Friedman. I don't think it helped his health much, and It put a lot of psychological pressure on him in addition to what he already was experiencing, namely he felt a deep responsibility to get this thing on and he was satisfied in his own mind that he was doing just right about it, making the proper division between his work with the Purple because he was staying right on top of everything we were doing and we were insuring that Friedman was kept up to date on it so there was nothing missing and Rosen and Small and Farner and myself probably, well, we were were a good team and he knew this

and I think he felt ~~that~~ (1) we might be resentful if he came in and sort of the implication that we weren't doing a good job and (2) that there ~~wasn't~~ was really nothing that he could contribute that he wasn't already contributing but there he was sitting in ~~a~~ the vacuum with the Chief Signal Officer pounding on him to get this answer out and there wasn't a damm thing he could do but sit there and suffer. Now I think that's exactly the situation that ~~that he~~ Billy was in and I think if there is any truth in Kahn's book about his statement that Friedman had a nervous breakdown as a result of his Purple assignment that it was an unnecessary and artificial pressures that were brought on Friedman by this simple act of saying put full time on it. That caused Friedman's health to degenerate. Now Friedman was pretty tired, you see, and we'd been working awful hard and he was, he was a little bit older than the rest of us and I don't think this helped his health any at all and I think it was a most unfortunate thing that happened.

Now this, the importance of the Purple and the crying need to get translations of messages between Tokyo and these major capitals of the world, ~~happened to~~ having caused Friedman to be assigned full time to drop all other activities and spend full time, ~~this is a~~ that's the better way of putting it, on the solution of the Purple I think had a pretty heavy impact on Friedman because he knew everything that could be done was being done. It was a matter of collecting more information and more material but he had to take certain actions in response to this new situation, ~~He was~~ him spending full time on the problem, and one of the things he did was to call, in support of the technical effort, all the skills that could be mustered out of the Signal Intelligence. Abe and Kully came in and spent, each left their responsibilities, Abe for the Italian and Kully for the German, and came in and reviewed what had been done. Friedman called in some people from outside. The one I remember distinctly was a reserve officer who was a relay engineer for Bell Telephone Companies up in New York City. His name was Juran, J U R A N,

and he came in for two weeks and I stayed with him for this whole period of two weeks going over what we had learned about the Purple and what we had imagined ~~or~~ about it, our diagnosis of it is a better way of putting it, and to make sure that he was briefed within the two weeks he had available to us for his active duty assignment as a reserve officer, that he was made as completely aware as possible of what our problem was, and I might just dispose of the Juran experience as follows: that about the last two or three days he began to express ~~a~~ some judgments [?], ~~since~~ the first five or six days of his period was one of intense interest in what we were doing and strong motivation to make sure he understood it because he was impressed by the assignment. To be called in to put his skills you see in support of something was fantastic, ~~It was something~~ he had never dreamt about. An attack on ~~the~~ a sophisticated cipher machine used at the highest echelons of

J apanese diplomatic establishment and thats quite a mouthful of awesome words and he was impressed by it. He wanted to find the magic solution to the thing. He wanted to be able to point to something that could be looked on as a contribution to this definitely important piece of work. But I can remember the last two or three days he was beginning to formulate in his mind what he was going to tell the Chief Signal Officer because the Chief Signal Officer wanted to talk to him. He was known. He had a good personal reputation. He wanted to talk to him personally and get his evaluation of this so he sat down and told me what he was going to tell the Chief Signal Officer and he said this. That there was nothing that he or any of his compatriots could contribute to this problem. That we had done a most magnificent job and had gone so far, far beyond any measure that could be expected of us and that what we should do was to continue and probably be left alone because he deplored that he had interrupted our work for the two weeks and had to go away without making any contribution. Now he sort o

TOP SECRET
HANDLE

hurried up and added "Now this doesn't mean that you shouldn't call on us if you think that we can make a contribution if there is any possibility that we can make a contribution but taking into account the security of the problem as well as what has been done here in the Signal Intelligence Service you're better off to go ahead on your own until you need us and that was a sort of a different attitude I found because most people would want to go away leaving the impression that they had helped us a lot but he went up and said very negatively "I haven't done a thing except interrupt." and this of course helped Friedman, Juran's recommendation, because it reinforced what Friedman had told the Chief Signal Officer, that we had pulled all stops on this and that, and I think this eased Friedman's personal ~~attention~~ tension and apprehension somewhat because it was now bugging him. ~~and~~ He was getting tired and you could see the effects of this added pressure because now he had to ~~bare~~ bear the full responsibility for the thing and he

could not shift it off on any of the rest of us nor could we share it with him which we would have gladly done but this was Friedman's nature. He took it all on his own shoulders. Now also sort of to relieve the pressure on Friedman and I think I'm describing the pressure on Friedman more than I am the technical situation but I think this is sort of what you want. Abe and Kully and the others who had been assigned to the problem had come in and reported that they didn't see that there was anything that could be done that hadn't, that we weren't doing you see. They sort of said look we've reviewed this thing. We've reviewed it critically and everything is being done. There is nothing we can contribute and then they said, "Please let us go back and work on our own problems a little bit because we're getting behind there you see and so this added to the the getting back to proper attitude. I think it was a little unnatural to put all that pressure on Friedman. Fortunately Furner, (Small, Rosen) and I who really were bearing the brunt of the work, it ~~really~~ didn't bother us. For some reason I guess

we were pretty well satisfied. We didn't know what else to do and if somebody had come in and solved it we'd been glad because, so there was no tension between Friedman and us because the Chief Signal Officer had put the pressure on him. Maybe I'm overemphasizing the sort of personal reactions here but, these exist today I'm sure and they have a lot of influence on what's done and how the answer is achieved and ~~that~~ they can't be ignored. In due course I think the problem developed, oh one of the other things that happened in this timeframe and I think sort of in some way affected Friedman's attitude is that the Navy had withdrawn both in act and interest in trying to solve the Purple. They I think sort of reached the conclusion that there was nothing in it for them since it was going to eat up a lot of people it was kind of an impossible situation to solve the problem and they had the pressures of working on the navy systems in front of them.....

End of Tape 9, Side 2

Tape 10, Side 1

Now of course it took several weeks sort of for Friedman to work himself out of this position that had been thrust upon him and this came about not only because Juran's reports and Kully and Abe's attitudes and Friedman's own reporting to the Chief Signal Officer but other things came in and had to be dealt with particularly in the COMSEC field and so we began to getting back to a more normal less and well less disturbing situation for Friedman because this wasn't a bad deal that he got I think in terms of getting this special assignment. The other things that came up were in terms of satisfying intercept requirements. We had a lot of problems in regard to the lower echelon~~s~~ systems that had to be resolved and then there was ~~a~~ the continuing problem ~~with~~ of insuring that the cryptographic program which had been established for budgetary and other reasons was being satisfied and to update the requirements for cryptographic systems and Friedman,

this is this is some thing that he loved and had worked with effectively, and so as the situation developed to the point ~~that~~ of where we could go on with our research, with Friedman sort of playing in and out of it I think the tension on him was relaxed. Of course ultimately when the system was broken I think the release of tension, Friedman still felt some of it but when the system was broken and the fact established that we could read the messages I think it was only then that he ~~was~~ could totally relax from this requirement because the outside people who were aware of our effort then were satisfied that the solution had been achieved and that everything that could be done of course had been done ~~and~~ or that everything that needed to be done had been done because we were reading the messages so the pressure let up at that point in time and Friedman relaxed a bit and I think that's when he was able to, well, start back up hill and regain some of his his, well, get out of this more dejected state into a less dejected state because

there was a state of dejection that became evident to some of us at that time. Probably the next thing of significance that occurred which which I think Friedman might have felt was in terms of some problems development of the mechanization of the, of the solution of the Japanese transposed code. Fortunately for all of us, the the magnitude of the problem was not recognized outside of the technical sections. It was a very awesome aspect to recover each day several transpositions keys and not only the keys themselves but the underlying codes without a knowledge of either. Early on in this introduction of the transposed code the Navy had made some photographs of the code and the system and had given us copies of them and they, well, both Friedman and the Navy had the same conclusion, that this was practically impossible. We might have limited success but we never could exploit it you see and the system was just that overwhelming in nature and Friedman made a judgment and I think expressed himself that this was the case and then later on when the SIS was able to develop the GEEWHIZER in a mechanization of this I think

Friedman may have felt a little personal some of his personal reputation ~~may have~~ had suffered because of the earlier stand he took but I don't think this should have bothered him because he should have regaled himself in the fact that he had set the stage for the emergence of this approach and if he hadn't (1) had the vision and foresight to get the people acquainted with the principles which ~~had been~~ could be applied in this case and (2) had gone a way out on a limb to get the IBM equipment which was an essential part of the solution on board, and I think Abe receives more credit than those of us who were more deeply involved in the particular development that resulted, and I'll identify it here as the GEEWHIZER approach, the GEEWHIZER being the cover name or the short title or handy title of a device that was constructed to be used in conjunction with an IBM tabulator and by the use of this combination of things together with certain things introduced by Small (Shor) like the use of the logarithm instead of the the absolute frequency and some of Furner's (FERNER'S) concept, mathematical, and contributions made by

others of us which finally culminated in the production of both a program and a primitive mechanization of cryptanalysis. I think it was that incident and I think probably the thing that bothered Friedman most though was the outbreak of the war. The imminence of the outbreak of the war was beginning to bear down on him and I think the records will show here that a team was selected to go to visit GCHQ. Denniston had been over to see us and we had been, the SIS and the Navy group, had been invited to send each two representatives so Akin had selected Friedman as senior man together with I believe Rosen was selected early on because everybody had great respect for what Rosen could bring back with his engineering background as well as his own personal sharpness. He was, he was really on top of this so we thought that would be the best deal and then Friedman went into uniform and I think the act ~~on~~ of going into the uniform had a serious ~~dramatic~~ traumatic effect on him. I don't think he was too disturbed about going to London because I think this, he would have been right out, he would have been doing exactly what he liked

once he got over there but I think just going into uniform shook him up so he had to take a breather ~~away~~ from the activity and get away from it and get some help, ~~some~~ medical help, and from then on I think Friedman's career was overtaken by the pressure of the war. Things were just happening too fast. Friedman could never keep up with them and so he finally paced himself until where he acted more in the capacity of an advisor instead of being involved in the administration and he, in this capacity he got involved in several things. One of them was the development of the 228, the SIGCOM, and I also got involved in that and worked with him and I found that he was beginning to realize that he was going to have to turn over the reins to the rest of us because ~~H~~e just couldn't stand the pace. The requirements were just too great for him and he began to relax in his attitude somewhat, except he would feel pretty badly at times. He'd, I don't like

to use the term fits of depression but that might pretty well describe it because I think he wanted to produce more. He wanted to give more than he was able to give and I think that bothered him and I think he reacted to it and finally he was put in a position of senior consultant and of course in a way was insulated from some of the greater pressures, organizational pressures and wartime pressures, and he pretty soon accepted this but it was only an overt acceptance I think. I think from then on Friedman had a pretty traumatic existence. Fortunately though, the officers in charge of the Army Security Agency knew Friedman and his reputation of what he had contributed and they didn't make life any more unpleasant for him than the situation [?] was.] They were aware that this was bothering Friedman. They tried to help him and they tried to do it in such a way that it didn't look like charity but every now and then it would show through and I'm sure it bugged Friedman. But he continued in so far as his interest in the activity was concerned. He was just as intensely interested. He was always

intensely interested. There was never any diminishing of his interest in the thing. It was just that he didn't have the physical stamina to respond and to do all the things he thought he ought to be doing, and I think I've accurately described what was wrong with Friedman, that he thought he ought to be doing more than was required of him and since he couldn't provide this I think he felt like he was being deficient and he downgraded himself and he really shouldn't have because I think anybody who had done as much as Friedman could have sat back on their laurels at that time, but he just absolutely refused to do it. Now I've said this very well and I think its right and its just about the way it was. I've left out the details but this is my impression and to just sort of requote it a little bit, I think Friedman felt that he should do more than he was able to accomplish and it was the difference, his incapability of doing all that he thought he ought to be doing that bothered him.

I might describe some of the organization implications which resulted and which had a bearing on Friedman and his contribution which conversely Friedman had a bearing on and it was this. We've now gone from about 1938 right into the period shortly after the war had started, and my last few sentences were directed at Friedman and his role during the war. But that period of transition I think needs a little attention in these remarks and I think we find it here. In the first place with the advent of Bullock, Col. Frank Bullock and Col. _____, who had no real experience in cryptology before their assignment. They were a straight first class signal corps officers but not aware, as aware, of the Signal Intelligence activities as Akin and Reeder and Mauborgne were. I mean we had a new climate now. A new attitude. A new, bosses came in and also with the burgeoning awareness that the war was imminent and with the influx of a great many more officers in the Chief Signal Officer and the calling in the reservists some of the rather happy environment that we had enjoyed was suddenly lost and this became a

bothersome thing and one of the things that I can remember distinctly that I think would have had a bearing on Friedman's feelings about it. It certainly had a bearing on mine was that the senior officer, language officer, who was assigned who was put in charge of the Japanese, well, he was put in charge of the signal intelligence activities -- that's Harold Dowd, and then other officers who had been assigned to the Japanese, other sections, assumed the responsibilities for them. The senior language officer in the Japanese section was Capt Svenson and he replaced, just overnight there was an order issued that said Svenson is responsible for the Japanese section. Rowlett is his technical assistant you see and this was sort of the way Friedman was treated. Well it didnt' bug me because I'll say it because I believe it. Svenson was known as the "Charging Swede" and I think was the football hero up at West Point when he was there. He still was a football hero as far as I was concerned but he didn't know anything about the technical end of the business. I'd, I'd make peace with him

but I ignored him other than just making peace with him; ~~because~~ nobody listened to him. I issued the orders and if he didn't like them he'd come and argue with me because he couldn't argue with the fellow who was doing it. I usually was able to out talk him and I'd even make trades with him, you know, to change priorities and things like that. if ~~He~~ wanted to do something and he knew he couldn't do it unless I helped him. I'm really describing how I solved my problem. I don't know how Friedman solved his. I don't think he ever solved it but I accepted Svenson and I just sat down and outfigured the bastard. That's exactly what I did because that was the only way of getting on with it and maybe I was smart or maybe I was stupid but there was that kind of a thing that we had to deal with and Svenson ~~was~~ is the one that drove us out of the Munitions Building on the 6th of December after we had information about the pilot messages because he was applying Minckler's instructions about the overtime and that was a terrible thing to ~~have~~ happen to us

because I think it would have bothered ~~my~~ me more if I hadn't sort of accepted it. You know this is a necessary evil and how do you get around it. I just wasn't overwhelmed by it at all. Now it was that kind of a thing that we had to accept and adjust to in our transformation from the earlier, well, the earlier kind of saturated technical attitude until we got in this pseudo-administrative mishmash that nobody understood and most of us who had any concept of the true mission of the SIS, most of us just ignored it. I think I said enough about that didn't I?

Comments about some other things that happened. I think I might better make a comment about some other things that _____. I've been talking now in terms of just ~~a~~ the few people, the old timers but one of the other problems that we all had to solve was how to deal with the increase in personnel requirements. Fortunately we didn't have to go out and recruit. There was a large body of skilled people on tap. These were the ROTC people that ~~which~~ of which Dale Marston is a good representative and Tom Chittenden,

They came in as a body and were assigned to positions of, well, Charlie Heiser (?) was another one that I remember. They were assigned to positions within the Signal Intelligence Service. At that time we began making the division between those who would be dedicated to the COMINT side and those who would be dedicated to COMSEC because it became pretty evident to almost everybody that (1) war was imminent (2) whether war was imminent or not there was going to be a greater effort at mobilization and (3) that we had to have a cadre. Had to expand our cadre of knowledgable people if the full mobilization took effect so this problem had to be solved in that time frame and I think this probably was behind the concept of putting the, of sort of removing the responsibilities from the civilian workforce and turning it over to the military. Then there was another thing that most of us in key positions were reservists and so we would eventually be called to active duty and there was that, that overtone that had to be considered. Of course Abe and Slet Rosen had already gone into uniform to make

the trip to London and they were the first and I think some of the, I didn't get into uniform until sometime after Pearl Harbor. I was still a civilian and I guess I always was a civilian because I never got to be an officer. I was a very poor officer. I wasn't trained. I didnt have the dedication~~s of~~ to the military code and principles that you get if you have some sort of formal training. All we did was, I think Kully was a great deal like I was. We just wanted to get on with the job and it was easier to do it in uniform than out of it. It didn't really make any difference and I think rank was something that was held pretty ~~safely~~ sacred at one time but I can remember Walt Jacobs and Dan Dribben as sergeants bossing majors and captains around. Not, not ordering them but directing them. They were the essential directors of the activity. It was great bit of topsyturvyness in the military structure within the SIS and this instead of, well, it just created uncertainties and oddities rather than generating obstructions.

End of Tape 10, Side 1

~~HANDLE [illegible] ONLY~~

Side 2 is blank

THE END