This is the lecture as corrected and edited by me. The original copy was sent to the C.E. Staff Officers School for deposit in the archives of the School.
W.F.F.

~~SECRET~~

~~SECRET~~

COMMUNICATIONS INTELLIGENCE

A Presentation by

MR. WILLIAM F. FRIEDMAN

to the Faculty and Students of Class 50-B

Air Communication & Electronic Staff Officers' Course

29 September 1950

~~SECRET~~

~~SECRET~~

~~SECRET~~

COMMUNICATIONS INTELLIGENCE

A presentation by Mr. William F. Friedman to the Faculty and Students of Class 50-B, Air Communication & Electronic Staff Officers' Course, on 29 September 1950

Colonel Sheets, Gentlemen: First I want to assure you of my appreciation of the opportunity to come here to talk to you on my subject. In inviting me to speak on the subject of Communications Intelligence, it was indicated that "the objective of the presentation is to create an awareness of the background, development, and manner of employment of this vital military weapon." Communications Intelligence was not always regarded as vital. I am reminded here of a story that I read some years ago in an old book, and the story may be apocryphal, but I give it for what it is worth. It seems that about two thousand years ago there was a Persian queen whose name was Semiramis and who took an interest in cryptography. Whether it was because of that interest or other unnatural circumstances, the record doesn't say, but anyhow she met an untimely death. Presumably she went to Heaven, or perhaps to the other place, but

Stay, weary traveller!
If thou art footsore, hungry, or in need of money-
Unlock the riddle of the cipher graven below-
And you will be led to riches beyond all dreams of avarice!

O, thou vile and insatiable monster! To disturb these poor bones!
If thou had'st learned something more useful than the art of deciphering,
Thou would'st not be footsore, hungry, or in need of money!

[illegible] For several hundred years the possibility of [illegible] served as a lure to all the experts who tried their hands at deciphering the message, but they were without success, until one day, [illegible]

along came a long-haired, bespectacled individual who, after working at the project for a considerable length of time, solved the cipher message. It gave him detailed instructions for finding a secret entry into the tomb. When he got inside he found an instruction to open the sarcophagus, but he had to solve another message in order to do so. Possibly it involved finding the correct combination to a 5-tumbler lock! Well, he solved that one too, after a lot of work, and which enabled him to open the sarcophagus, and found a box. In the box was a message in plain language, and this is what it said: "Oh, thou vile and insatiable master, to disturb these poor bones! If thou hadst learned something more useful than the art of deciphering, thou wouldst not be footsore, hungry, or in need of money!"

Many times in the course of the past forty years I have had occasion to wish that I knew the old gal's address so that I could write her on a first indorsement to her basic communication, the single word "Concur." Well, anyhow, it's been an interesting life!

Now I am going to read you a short paragraph from a long story in Time Magazine of December 17, 1945, under the heading NATIONAL AFFAIRS, with the subheading PEARL HARBOR and the sub-heading "Magic" is the word for it" TIME said:

"U.S. citizens discovered last week that perhaps their most potent secret weapon of World War II was not radar, not the VT fuse, not the atom bomb, but a harmless little machine which cryptographers painstakingly constructed in a hidden room in Washington. With this machine, built after years of trial and error, of inference and deduction, cryptographers have duplicated the decoding devices used in Tokyo. Testimony before the Pearl Harbor Committee had already shown that the machine known as 'Magic' was in use long before December 7, 1941,

had given ample warning of the Japs' sneak attack if only U.S. brass hats had been smart enough to realize it (TIME Dec. 10). Now General Marshall ~~now~~ continued the story of "Magic's" magic." It had: [Insert here. Copy from TIME. See me]

And then ~~it~~ TIME goes on to ~~say what~~ give more details of that story. ~~was. I hope I'll have time to~~ We shall return to ~~it a little~~ bit later ~~on~~ in this talk. ... [Stop]

I hardly need to stress the necessity for secrecy in this business. Hope for future success depends to a very great degree on maintaining secrecy with respect to past achievements. Changes as a result of suspected compromise of cryptographic systems are easy to make and very hard to follow. The effects of leakage or compromise are not local — they are widespread, because of the widespread use and distribution of particular cryptographic systems. During World War II, I might say, the continuance of our success hung by a very slender thread. I am reminded at this point of an instance of this sort which happened just a short time before 1941, and to avoid naming names I will simply say that there was a chap in a certain capital of the world who sent a message to his home government in which he said that he was getting a bit worried about their communications. In substance, he said: "You know, these many telegraphic exchanges that we are having, dealing with this matter in hand, have put a great strain on our cipher system because they have made it necessary to be very voluminous in our correspondence, so that I am afraid that perhaps some third party might be reading our communications. I think we ought to do something about this right away." Well, we read that, and we were very much upset for fear that they would take the hint and that something would happen. So we were on tenterhooks and pins and needles for two or three days until we got the reply from headquarters. You can imagine how agog with anticipation we were

until the message was processed to the point of intelligibility. To paraphrase the reply, it said, "Well, you southern extremity of a horse's anatomy, don't you realize that what you are saying is way out of line? Don't you know that our system and the machine has so many permutations and combinations it's inconceivable that anybody should be able to read these communications without having the machine and the key? Now, don't you worry any more about it. You 'tend to your own business, and we'll 'tend to ours." We were very happy when we read that one. The thread was indeed a very thin one that time because it was possible to do quite a number of things to "soup up" the system, any one of which would have occupied us for months to get back into a state of readability.

I hardly need to give you a definition of communications intelligence, or COMINT, as we call it for short. No doubt Major Morrison has already dealt with it, so I will simply cite its three main objectives. First, to provide authentic information for policy makers, to apprise them of the realities of the international situation, of the war making capabilities and vulnerabilities of foreign countries, and of the intentions of those countries with respect to war. Second, to eliminate the element of surprise from an act of aggression by another country. Third, to provide unique information essential to the successful prosecution, and vital to a shortening of, the period of hostilities.

Now, the background of COMINT, which is based upon the science of cryptanalysis, has a long and very interesting history which is inextricably bound up with the history of cryptography. The two are but opposite faces

of the same coin, for progress in one inevitably leads to progress in the other. Hence, while my talk will deal ~~is to be directed largely to crypt-analysis and COMINT, I will have to deal also, to a certain extent,~~ with both COMINT and COMSEC. ~~cryptography and communications security or COMSEC.~~ Now, because of the secrecy or cloak of silence which officially surrounds the whole field of cryptology and especially cryptanalytics, it is obvious that authentic information with reference to the background and development of the science in foreign countries is quite sparse; and although after World War II we learned much regarding the accomplishments in this field of work by our enemies, security rules prevent my saying very much in detail about how good or bad they were in comparison with us. Suffice it to say we looked pretty good. I can only give a fairly good account of U.S. cryptologic ~~COMINT~~ activities up to a certain point of time, and even then I will not be able to say very much about them simply because the story is too long to give in a lecture or even a series of talks. the U.S. Navy's COMINT activities, because I don't know very much about that background and prefer not to give any information which I can't document. In any case, I might say at this point that our relations with the Navy in the early days were such as to preclude my knowing very much about what they were doing, and vice versa. In the course of my talk I will ~~give~~ present a number of illustrations of cryptography and cryptanalysis, some of which form part of my own experience. Modesty would dictate their omission, but because of their possible interest I will use them and will here and now make a general apology for the use of the personal pronoun.

Now may we have the first slide, please. Cryptography and cryptanalysis go back to the dawn of the invention of writing, and here I
1 show an instance of cipher in the Bible. In Jeremiah 25:26 occurs the

expression "And the king of Sheshakh shall drink after them." Also in Jeremiah 51:41: "How is Sheshakh taken?" Well, for many, many years that name "Sheshakh" remained a mystery. There was no such place. But then somebody discovered that if you write the twenty-two letters of the Hebrew alphabet in two rows, eleven and eleven, like this, you get up a substitution alphabet whereby you can replace the letters by those standing opposite them. For example, "Shin," is represented by "Beth" or vice versa, so that "Sheshakh," translates "Babel," or "Babylon." The vowels had to be supplied. Incidentally, mentioning the Bible, one might say that Daniel, who was the first psychoanalyst, was also the first cryptanalyst. I say psychoanalyst, because you remember how he interpreted Nebuchadnezzar's dreams. In the Bible's own words, "Nebuchadnezzar dreamed dreams, wherewith his spirit was troubled, and sleep brake from him." But when he woke up he just couldn't seem to remember them. One morning he called for his magicians, astrologists, and Chaldean sorcerers and asked them to interpret the dream he'd had during the night. They asked him: "What was the dream?" and he said, "Well, I don't remember it, but it's part of your job to find that out and then to interpret it." That was a pretty stiff assignment, and they failed to make good, which irked Nebuchadnezzar no end. Kings had a nasty habit of chopping your head off in those days if you failed; so in this case it comes as no surprise to learn that Nebuchadnezzar passed the word along to destroy all the wise men of Babylon, including Daniel. Well, when the King's guard came to get Daniel, Daniel asked that he be given a bit of time. Then, by some heavenly guidance - the record simply says that the secret was revealed to Daniel in a night vision - Daniel was able

to reconstruct the dream and then interpret it. Some years later, Nebuchadnezzar's son, Belshazzar, was giving a feast, and during the course of the feast the fingers of a man's hand appeared on the wall behind the candlestick and wrote a secret message; Belshazzar was very much upset and called for his soothsayers, chaldean sorcerers, magicians and so on, but they couldn't read the message - apparently they couldn't even read the cipher characters! Well, Daniel was called in and succeeded not only in reading the writing on the wall: "Mene, mene, tekel, upharsin," but also the meaning of the words. His interpretation was "Mene" - God hath numbered thy kingdom and finished it. "Tekel" - Thou art weighed in the balances and found wanting. "Upharsin," or rather "Peres," (apparently the chap who did the hand-writing on the wall knew a thing or two about cryptography, because he used "variants!") - Thy kingdom shall be divided and given to the Medes and Persians."

The next is an illustration of the earliest cipher device history records, a device which was called a scytale, used by the ancient Lacedaemonians or Greeks. They had a wooden cylinder of specific dimensions, around which they wrapped spirally a piece of parchment; they then wrote the message across the edges of the parchment, unwound it, and sent it to its destination, where the recipient would wind the parchment around an identically-dimensioned cylinder, and thus bring together properly the bits of letters representing the message. This diagram, incidentally, is not correct. The writing was done along the edges of the parchment, as I said before, and not as shown in this

SECRET

picture. And, by the way, the baton which the European field marshal still carries as one of the insignia of his high office derives from this very instrument.

Caesar, of course, is well known in history to have used cryptography - a very simple method, obviously, because all he did was to replace each letter by the one that was fourth from it in the alphabet. Cicero was one of the inventors of what is now called shorthand. He had a slave by the name of Tiro who wrote for Cicero his records and so on, in shorthand or Tironean notes, as they are called.

The beginnings of modern cryptography can be traced back to the days of the early years of the 15th Century, when the science was extensively employed by the princes and chanceries in the Papal States, about 1,400. I show next an alphabet of that period which is interesting merely because it shows that in those early days they already had a recognition of the basic weakness of what we call simple or monoalphabetic substitution. Solution of this type of cipher, as you all know, is accomplished by using data based upon frequencies. I don't have to go into that because all of you, at some time or other, have read "The Gold Bug," and understand that sort of analysis. But this slide shows that the early Italian cryptographers introduced a method of disturbing the normal frequencies, by having the high-frequency letters represented by more than a single character. I will add that the earliest treatise that the world possesses on the subject of cryptography, or for that matter, cryptanalysis, is that which was written in 1474 by a Neapolitan, whose name was Giacco Simonetta. He sets forth the principles and methods of solving ciphers -- simple ciphers no doubt, but he describes them in a very clear and concise form. The first book or extensive treatise on

cryptography is that by a German abbot named Trithemius, who wrote his monumental work in 1531. He planned to write four volumes, but he quit with the third one because he [purposely] wrote so obscurely and made such fantastic claims that he got charged with being in league with the Devil. They burned his books, as a matter of fact. This may be a good place to present a slide which observed that the necessity for secrecy in high business was recognized from the earliest days of cryptology

We are going to jump a ways now to some examples from more recent history. This slide shows a cipher alphabet and system used by Mary, Queen of Scots, in the period 1585, or thereabouts. There was an Italian cryptographer whose name was Porta and who wrote a book, published in 1563, in which he showed certain types of alphabets that have come down in history and are known now as Porta's Alphabets. Here's an example of the Porta Table, showing one alphabet with key letters A or B, another alphabet with key letters C or D, and so on. I don't want to go into exactly how those key letters are used, but it is sufficient to say that even to this day cryptograms using the Porta alphabets are occasionally encountered. Incidentally, Porta was quite a fellow. There are lots of people who refer to his book but have never read it. I took the trouble to have it translated to see just what he did say, and he was, in my opinion, the greatest of the old cryptographers. Incidentally, also he was the inventor of what we know as the camera obscura, the progenitor of our modern cameras. I think also he was one of the earliest of cryptanalysts able to solve a system of keyed substitution, that is, where the key is changing consistently as the message undergoes encipherment. Porta's table was actually used in official correspondence. Here is a picture of a table that was found among the

state papers of Queen Elizabeth's time, used for communicating with the English Ambassador to Spain. It used Porta's alphabets.

The next slide I show is a picture of what cryptographers usually call the Vigenère Square or Vigenère Table; a set of twenty-six alphabets successively displaced one letter per row, with the plain-text letters at the top of the square and the key-letters at the side. The method of using the table is to agree upon a key word, which causes the equivalents of the plain-text letters to change according to the manner in which the key changes. Now, Vigenère also has an interest to me because although he is commonly credited with having invented that square, he really didn't and, what's more, never said he did. Here's a picture of it as it appears in his own book. It goes considerably beyond what the ordinary references say about his table, but I won't go into those differences because they're technical and perhaps of no great interest to you today.

The next cryptographer I wish to mention is a Frenchman, Francois Viete, an eminent mathematician, founder of modern algebra. In 1589 he became Councelor of Parliament at Tours and then Privy Councelor. While in that job he solved a Spanish cipher system using more than 500 characters, so that all the Spanish dispatches falling into French hands were easily read. Phillip II of Spain was so convinced of the safety of his cipher that when he found the French were aware of the contents of his letters to the Netherlands, he complained to the Pope that the French were using sorcery against him. Viete was called on the carpet and made to explain. Here is another example of another old official cipher. Here are

the alphabets; and a sliding card, which could be shifted up and down, was used for changing the key, or as a means of changing the key. Here is another, called the "two-square cipher," or "two-alphabet cipher"; it involves coordinates: here is one complete alphabet and here is another one; the coordinates are used to represent the letters. That was actually used in Charles I's time, 1627, in communicating with France and Flanders.

I want to jump now to the period of the American Revolution, in U.S. history. The systems used by the Americans and by the British were almost identical! In one case, in fact, they used the same code book! I know that there was ~~I have seen reference to~~ an American who seems to have been the one-man NSA, Revolution's hero, for he was the cipher expert to Congress, and it is claimed that he managed to decipher nearly all, if not all, of the British code messages intercepted by the Americans. The next chart shows a picture of a code or "syllabary," as we call it, used by Thomas Jefferson. This syllabary is constructed on the so-called two-part principle. This is a portion of the decoding section. You will note that the numerical groups are in consecutive order but their meanings are at random. They have no alphabetical order at all. It simply means that you have to have another section, the encoding section, in which the words are in alphabetical order, and their equivalents are in random order. This sort of system even today is in extensive use. Jefferson was an all-around genius, and I shall have something to say about him and cryptography a little bit later on, I hope. Here's an interesting slide showing a picture of a letter which is known as "the Benedict Arnold

~~SECRET~~

Indecipherable Treasonable Cow Letter." It has never been deciphered. It reads, "I have bought a cow and calf from Con. John Joseph Dullis," and so forth. The reason that it hasn't been deciphered is that there isn't enough of it to form the basis for a solution.

I am going to say a few words about Egyptian hieroglyphics for the reason that I think that that represents the next and a great landmark in the history of cryptography. About 1821 a Frenchman, Champolion, startled the world by beginning to publish translations of Egyptian hieroglyphics. [Here's a picture of the gentleman and here's a picture of the great Napoleon. This is a picture of the Rosetta Stone.] It is a tri-lingual inscription: Egyptian hieroglyphics, followed by Egyptian script called "Demotic", and then Greek. All three texts were assumed to say the same thing, of course. It was by means of this tri-lingual inscription that the Egyptian hieroglyphic writing was finally solved, a feat which represented the successful solution to a [great cryptanalytic] problem, the major part of which was linguistic in character, for the cryptanalytic part was relatively simple. In the hieroglyphics there are things that we call cartouches, that is, characters enclosed in a rectangle marked by a graven line. Here are some examples. This one was on an obelisk, and was suspected of representing the name Cleopatra. I suppose the reason for that assumption was the repitition here of two characters at a proper distance to represent the two A's of Cleopatra. By taking the various cartouches, writing them out carefully, studying them on the basis that this cartouche was Cleopatra, it turns out that by taking the characters in the cartouches, substituting their equivalent Roman letters and putting them in the proper places in other cartouches, bit by bit Champolion was

able to establish names other than Cleopatra, such as Ptolemy, Alexander, and so on. That's the way in which a start or initial break was made with respect to the Rosetta Stone, and Egyptian hieroglyphics were finally read. It was very fortunate that the early students of Egyptology didn't know that the Egyptians also used cryptography! Some of their writings are not only "plain-text hieroglyphics," but they also had "cryptographic hieroglyphics"! Here, for instance, is an example of substitution. That character in place of this one means "to speak." You see the finger pointing to the mouth, and so on.

~~Now I am going to jump to~~ The period of the Civil War or the "War Between the States," in U.S. history, Next the use of cryptology in a large way. Here is a picture of a cipher device used by the Confederate Army, captured at Vicksburg, one of our Museum treasures. The device is a cylinder covered with a sheet of paper bearing the alphabets, the alphabets of the Vigenère table, in other words, a pointer that you could slide, and a thumb knob with which you could turn the cylinder according to the key letters. You might like to know two of the keys they used with this system and device: COMPLETE VICTORY was the first, and COME RETRIBUTION the second.

There is one person I should mention before coming ~~passed over in getting~~ to the Civil War period. Edgar Allan Poe, in 1842 or thereabouts, kindled an interest in cryptography by his famous story of "The Gold Bug," and by some articles on cryptography in newspapers and journals of the period. For his day he was the best informed person in the U.S. on cryptologic matters.

Here is a picture of a message, authentic without question, which was sent by President Lincoln to Gen. Burnside. It's very simple. It reads this way, of course, and makes no sense; but if you read it backwards it makes excellent sense: "If I should be in a boat off Aquia Creek at dark tomorrow, Wednesday evening, could you without inconvenience

meet me and pass an hour or two with me? (Signed) A. Lincoln." I think the President was kidding a bit, but he may have had confidence in the official cryptographic system in the same way that certain high-level officers in our [illegible] after [illegible]

This is a photograph of a page or two from the code book and cipher system used by the Federal Army. They had what is called "route ciphers," that is, a matrix with indications of route to be followed in inscribing and transcribing the words of the message. Here's how you write the message in: the first word, second, third, fourth, fifth, sixth and so forth; then you take them out according to another route. And here the thing is complicated by the use of arbitrary equivalents for the names of important people. "President of the U.S." is represented by "Adam" or "Asia." It had two equivalents, you see. Here are some of the names of famous or well-known officers of that period. I have with me today the complete set of cipher books used by the Federal Army during that period, and after my talk those of you who wish may come up and examine them, together with certain other exhibits. The next slide is a picture of a message sent to General Grant in one of those route ciphers. I shall not take time to read it.

There is an example of a type of secret writing employed by the French in the Franco-Prussian War. It consisted of code groups written out from a code book. You remember that in the Siege of Paris the French were completely cut off, so that messages had to be sent out by pigeon. The message was photographed down, and — this, I believe, was the first and earliest example of micro writing used for military purposes — the message was, as I said, photographed down and sent out by means of carrier pigeon. This is a copy of one of the examples.

After the Civil War, or War Between the States, the use of cryptography in United States military affairs went into a decline for a long period of peace, and was broken only briefly by the Spanish-American War. In 1885 the War Department published a code called "Code to Insure Secrecy of Telegrams," based on a small commercial code, almost word for word. I have a copy of that with me and if you wish to examine it you'll get some idea of how naive we were in those days! In the Spanish-American War there was very little use made of sound cryptography, for we used that code, which had no secrecy whatever; but then we must remember there was no such thing as radio in those days, either. In 1899 the Chief Signal Officer undertook the preparation of a suitable code. Economy was stressed - the Chief Signal Officer personally did all the work. In 1902 the "Cipher of the War Department" was published by the Adjutant General. In 1906 a revision of that was published, and in 1915 a completely new code, the War Department Telegraph Code, was published. But, believe it or not, that code was printed by a commercial house in Cleveland! As Friedman is what my predecessor in the Office of the Chief Signal Officer told me when I took over from him in January 1921, after he came now to the World War I period. With Hertz's discovery of the so-called Hertzian waves and Marconi's practical demonstration of signalling by wireless, a new era in military communications was ushered in, and also a new era in cryptology. The first wide usage of wireless, or radio, as it soon came to be called, was in World War I, but developments in cryptography lagged a bit, as we shall see.

First, I will discuss the tactical use of cipher systems in World War I, because these were used in preference to code systems, which came later. Here is a picture of a cipher system used by the Russians. You will note

SECRET

that it is nothing but the Vigenère principle all over again, using numbers instead of letters, ~~and~~ it represents only a case involving a set of 7 or 8 alphabets used repetitively, by a key number, for substitution. This was the deciphering table. The next slide is a picture of a front-line cipher system used by the French. It was a transposition system, the columns being here transcribed according to the columnar key; in addition, certain disturbing elements came into the method by taking off the letters in diagonals. And here is a picture of the system used by the Italian Army in World War I. Again, it is only a variation of the old Vigenère system. Here is a system used by the Germans; it was invented by them, or, I should say, it was a clever combination of two methods ~~put together in a very clever way~~. We called it the ADFGVX cipher because the cipher text consisted exclusively of those letters. An alphabet is here, arranged according to some pre-arranged plan, with the coordinates ADFGVX; the letters of the message were then replaced by pairs of coordinates; for example, the letter R is represented by AG, and so forth. Then a numerical key, developed from a key word, is written over the X's, A's and so forth, and the letters are then taken out in columns according to the key order. That system was a brand new thing in military cryptography and caused no end of headaches for the Allied cryptanalysts until it was discovered just how a solution could be achieved. The solution was not a general one solution but depended upon special cases; however, these happened so often that we could bank on these occurring. That cipher system was used by the German high command and consequently someone soon discovered that

if you made a chart based upon the number of ADFGVX messages intercepted, just why you could discover certain things about the tactical situation and, more important, you could, with some degree of assurance, predict what at a certain point of the front. Here is an example of such a chart might happen. ~~This is a chart which we got up in the~~ based upon the ADFGVX intercepts. This, gentlemen, is the first illustration that I know of in history of one of the basic principles of traffic analysis, and traffic intelligence. (Explain chart) The next slide gives a picture of the sort of "communiques" we issued, "Bulletins" we called them, that we put out when the ADFGVX messages were read. Here is one of a set of messages, dated November 20, 1918; of course the war was over by that date, but this gave very important information about the withdrawal of Mackensen's army into Roumania. There is the German text and there is the translation, an interesting and authentic message.

For tactical messages the British and Americans in World War I used a method known as the Playfair cipher, invented allegedly by Lord Lyon Playfair, but he didn't invent it - Sir Charles Wheatstone invented it. By the way, Wheatstone, who is credited with inventing the electrical bridge that is known by his name, didn't invent that bridge - a chap named Christy really did. The method of Playfair encipherment is to have a square 5 x 5, or 25 cells in all, in which you start in with a key word, then the rest of the unused letters of the alphabet. (I and J are treated as the same letter). If you want to encipher "at" the equivalent is "rw", by diagonals, and so on. There is an example of how a message is enciphered. In those days, 1914, that was regarded as pretty hot stuff. In fact, an officer of the American Army (later he became Chief Signal Officer, Major General

~~Retired~~

Lauberge) wrote a little treatise, published in 1914, in which he dealt with this Playfair cipher system. The title of his work is "An Advanced Problem in Cryptography." Today, our most elementary students are given things of that sort to solve after a few lessons.

The British Army developed a cipher device in World War I. They had manufactured a great many of them, thousands in fact, and they proposed to the French and the Americans that all the Allies should use it for tactical communications; but, to the chagrin of the British, it was never put to use, for reasons that I hope to have time to tell you later.

So much for the cipher and the cipher problem. Now, I'd like to say a few words about the codes and code systems used in World War I. That a code system is simply a sort of dictionary in which the words, phrases and sentences are representable by arbitrary groups of letters or figures. Here is a page from a commercial telegraph or commercial cable company's code-book, which they offer to their customers for economy. You'll notice that each of those code groups differs from every other code group by at least two letters. We call that "the two-letter differential." The reason for having such a differential is that errors are sometimes made in transmission, but the likelihood of making two errors in the same group is not nearly as great as making a single error. The 2-letter differential affords methods of readily correcting a group if it has a single error in it; with a bit more trouble 2-letter errors can also be corrected. Now, code books and codes are compiled to be suited to general or specific kinds of business. They are generalized, like a general trade or shipping code, or a code for the automotive industry,

and so on; but they may also be highly specialized in character. The next slide shows a highly specialized code. You know, there are certain people who believe firmly and implicitly in the power of healing by suggestion, and that is, and here is a picture of a code book put out by a gentleman who was a professional man in that field. It's clear you will notice that the purpose of it was, of course, to be able to receive treatment from or by your own practitioner no matter where you were. Thus, if you should go away on a trip and want to consult your practitioner, you can send him a message and tell him what you think you are suffering from, or, of course, what you think you are suffering from. Now, that is the other thing. The code is in English and French, and you would simply represent your illness, or alleged illness, by the code group corresponding to your malaise. Now, note that the gentleman who got up this code was pretty well versed in the intricacies of code and communications difficulties, because these code groups differ by at least three letters each; the reason, of course, for this extra precaution is, of course, clear: be a pretty serious thing if you sent a message saying that you think you are suffering from corns, but the code group, having been garbled in transmission, telling him fortunately gave you the treatment for convulsions. That would be pretty tough!

Prior to World War I the use of code books for tactical purposes was thought to be impracticable, largely because of the difficulties of compiling, reproducing, distributing and protecting the books. I don't think they thought too much about the possibilities of solving codes. Early in 1916 the Germans began to use small field codes, and the Allies soon followed suit. I had some slides to show you pictures of pages of the code books of the various belligerents, but I will omit them and say

that I also have brought exhibits of such books as were actually used for the purpose. Those who would like to see what they were like are welcome to come up after this talk and examine them. The only slide that I will show is one that will give you a picture of the American Army's inadequacy in World War I for code communications. This is authentic — I didn't make it up — because I found it in the records when I closed our office with the AEF in April 1919. It's a code gotten out by the 52nd Infantry Brigade, dated 17 April 1918, and it is what we may call "the baseball code." If you wanted to say "killed," you said "struck out"; "wounded" was represented by "hit by pitched ball," and so forth — very elementary.

move to back of p. 15c

Now I am coming to a very interesting example of the use of ciphers by German agents in the World War I period. Here is a cipher message which was found on a German spy in the United States soon after he crossed the Mexican border into Texas. After some weeks it was deciphered by G-2's code-solving organization in Washington, MI-8, as it was called. Here is the deciphered German text, and this is what it said: "To The Imperial Consular officials of the Republic of Mexico. Strictly Secret! The bearer of this is a subject of the Empire who travels as a Russian under the name of Pablo Waberski. He is a German agent." And so forth. The Court sentenced him to be shot; President Wilson commuted it to life imprisonment; and he was out of the pokey after only one year! We're a lot more severe these days.

Here is the message, now known as the "Zimmermann Telegram," which is probably the most famous message in published cryptanalytic history to date. This is the message which was the prime factor that broke the German's back and brought the United States into World War I, on the side of the Allies.

From the beginning of that war until the end of 1916 it was questionable ~~In 1915-16 it was very much catch-as-catch-can~~ as to which side the Americans were going to join. Our British friends, later our allies, did certain things that we didn't like, and there was a good deal of talk about their nefarious behavior with our mail and our merchant ships. But this message, solved by the British, brought us in on their side. It was the straw that broke the camel's back. It is known as "the Zimmermann telegram." It went to the German legation in Mexico City from Count Von Bernstorff, the German ambassador in Washington. The method of solution I won't go into. [British] Their cleverness in the handling of the case is a good illustration of how astute, diplomatically, ~~our British friends~~ they are, for, as I have already said, it resulted in bringing us into the War on their side. Here is the translation of the thing. It was important because the message said the Germans were going to resume unrestricted submarine warfare and this part, here, dealing with a ~~deal~~ proposal to be made to Mexico, was the straw that broke the camel's back. People in the Middle West were very lukewarm toward the idea of our getting into the War - on either side - but when the Germans began talking about returning to Mexico, Texas, New Mexico and Arizona, that was something else again. So, we got into the war within a couple of weeks after the British gave us and established the authenticity of the translation of "the Zimmermann telegram." A book of almost 250 pages, dealing only with that telegram and parts, was published just about six weeks ago. I brought a copy with me for you to look at later.

Here is another message solved in World War I by the British and made available to our authorities in Washington: a sabotage message talking about who were reliable saboteurs and what they should do. That message figured in a long, long trial before the German-American Mixed Claims

Commission, in which the Germans were charged with certain acts of sabotage, notably the Kingsland fire and the Black Tom explosion in New Jersey. Most of you are too young to remember those incidents. The trial resulted in a decision in favor of the United States claimants, who were awarded some $20,000,000. Here is a message, in secret ink, that figured in the Black Tom Case: a page from the Bluebook Magazine, on which there was a message written in invisible ink, a method we run into occasionally even in modern matters.

Now I come to a case in which I was involved. In 1916-17 the Germans financed a large number of Hindus in their attempts to stir up a rebellion in India, the idea being to cause so much trouble in India that the British would be forced to withdraw troops from the Western front to quell disturbances in India. These Hindus were negotiating for the purchase of arms and ammunition in the United States and sending them over to India. Since the U.S. was neutral, it was against our own laws to permit such undertakings against a friendly nation. So the business had to be conducted secretly and that is how cryptograms entered into the picture. Here is one page of a long, seven or eight-page letter that was intercepted between the top Hindu agent in the United States and his chief in Switzerland. The letter consisted of groups of figures, in which were interspersed some plain-text words. I recognized pretty quickly that the letters of the secret text had been replaced by numbers which indicated specific letters in a book. Each group of numbers represented the page number, the line number, and the position number in the line of the letter. All I needed was the book, but unfortunately the Hindu failed to tell us what the book was, so I had to go ahead and

try to solve the message without it. It was solved; and I'll show you very briefly the method. As I said, there were words, plain-text words, interspersed throughout the cipher text, and I would make a guess at what the numerical group before or after a plain-text word represented. Here, for example: "Forward something, with something." I assumed that this first "something" would be the word "committee," and that meant that on page 65, the fourth line, the second letter in the line was a C; the third to be O; the fourth M; the fifth another M, but the sixth letter in that line was not indicated. Instead, the next group jumped to another page, from which the letters I, T, T, and so on were taken. Well, by substituting some of these guesses in their proper positions and making tabulations of this sort, I assumed that the first five letters of this word "committee" came from the word "communication" on page 65, line 4; the next three, from a word having "TTE" in it, such as "attention"; but the last letter, E, from another page altogether and I could only add more data before making any guess as to what the word on page 72, line 2, might be. By working back and forth, building up the various words on various pages of the book, then building up the words of the message -- one helped the other -- I finally got certain clues as to the sort of book involved -- that it was a book dealing with the history of German political philosophy, economy, or history. I hunted and hunted and hunted for that book. I finally found it, all right. It was Price Collier's Germany and the Germans. This message figured in a long-drawn out trial in San Francisco, where there were about a hundred and five Hindus on trial simultaneously. One of the Hindus turned State's evidence and got

SECRET

himself in bed with the others. They were searched every day before they came into the court, but one day, the day after I testified, one Hindu managed to secrete a gun in his clothes and during the midst of the court proceedings shot the Hindu who had turned State's evidence, thereupon the United States marshall, a great big fellow, six foot four, standing in the back of the court, drew his weapon and shot the first Hindu dead. They were both dead right there, within two or three seconds. That's the way that trial ended up, rather dramatically.

I'm going to pass over the next slide. It figured in the oil scandal in the days of 1924. I was government witness in that case, having solved the messages which disclosed some of the facts that lead to Mr. Fall's going to prison. He was Secretary of the Interior, if you recall. I think he died only recently.

The rum runners in those lamentable days of prohibition, used some very good codes and ciphers. Here is a particular case where a message was enciphered by taking code groups out of one book, transferring the code numbers for those groups into another book and then adding a constant value to those numbers, finding the letter-group equivalents of the final numbers, then enciphering those letter groups! This was such a message. All I had to do was to find the two code books, the additive, and the cipher alphabet. Lightning struck one night and the job was completed in a few hours.

There were some interesting things, working on the job in peacetime, when we would get messages from various government agencies to solve.

Here is one that came to the White House and was sent to us by the Secret Service. It was addressed to the President and had this dagger stuck in after this message. If you read it backwards and take alternate letters it asked President Roosevelt: "Did you ever bite a lemon?"

Now I am going to jump to the question of cipher devices, because they represent the modern trend. I've already mentioned to you the point about the invention and introduction into wide usage of radio, and their effects upon military matters, especially upon cryptology. Traffic in large quantities became available for interception and study, and hence improvement in cryptography had to come. It came slowly but surely. In connection with theoretical advances in cryptographic methods came inventions of cryptographic devices and machines. A brief history of these will therefore be useful. [Here] is a picture of the earliest cryptographic device on record, except for the scytale. This is taken from a book by an Italian cryptographer named Alberti, published in 1470, and is just a pair of alphabets, one revolving concentrically upon the other, so that you could change the relationship of the two alphabets. This wheel is represented also in the Porta book, and, by-the-way, I have with me today a copy of the original edition of Porta, with the cipher wheels in place and in working order. This was published in 1563. They didn't have any children in those days, obviously, or otherwise these things wouldn't be here, and in good working order!

I know it takes a long time to get a patent through the patent office, but Alberti's device was finally patented in 1865, the inventor happening to be the then Chief Signal Officer of the Army, Major Albert J. Myer.

Believe-it-or-not, the same thing was used by the Signal Corps of the United States Army as a new invention perhaps, in the period 1910 to 1918. There is a more recent invention of the same thing. The patent office doesn't have good access to literature on the subject of cryptology, so every once in a while a thing that is as old as the hills gets through the patent office. Now we come to an interesting device. I mentioned a little while ago that the British proposed a cipher device for use on the Western Front in World War I, and a little bit of history of that development is interesting. Here is a picture of a device invented by Sir Charles Wheatstone, the eminent British mathematician, physicist and electrical engineer. He was also a cryptographer of some stature. The principle of the Wheatstone cipher wheel is just a little different from that of Alberti's or the Signal Corps. This one has an alphabet of 27 characters and an inner alphabet of 26, with an eccentric motion influenced by the letters that you were actually going to encipher. With this hand, you see, you go around this way, and, for example, if the letter H is represented by E, on the next revolution H is represented by the next letter, which happens to be a V for victor. Now the British took that basic invention, and souped it up a bit. Perhaps you noticed that on the first slide the outer alphabet consisted of the letters in normal English order, on the inner alphabet the letters were in mixed order. What they did was to add the idea of a mixed alphabet on the outside or outer alphabet. They changed the form of the device itself, but the cryptographic principle is identical. Here it is. They had a great many of these manufactured. I was at that time, in the Autumn of 1917, working at the Riverbank

Laboratories. This thing had been approved by the British, the French and the American cryptographers in Europe. It was sent to Washington, approved there by the MI-8 people, but somebody there said, "Well, let's see what this fellow out in Chicago thinks about it. So they sent us a set of five very short test messages enciphered by this device. All I knew was that a device based upon Wheatstone principles was probably involved. My employer came to me and gave me these five messages, each message only 35 or so letters long. He said, "I want you to solve this thing." I said, "But I can't solve anything as short as this. It's absurd and unfair. I don't want any part of such a test. Besides, I have other fish to fry." He said, "Young man, on the last day of each month you get a little green piece of paper with my name in the lower right hand corner. If you would like to continue receiving these pieces of paper, you will start work on this right away." I said, "Yes, Sir!" Well, by hocus pocus which I won't go into, I succeeded in reconstructing what I thought was the basis for the mixing of these letters in here, the letters of the inner alphabet. The word on which it was based seemed to be the word "cipher," and I thought, "Well, so far so good, but unfortunately there is no way of reconstructing the outer alphabet by analysis." At that time I hadn't invented the principle of doing so, although about a dozen years later I did so. But in 1917 there was nothing to do but try to guess what the keyword for the outer alphabet might be, by trial and error, and I made this assumption: If a fellow was foolish enough to use a word like "cipher" as the basis for mixing one alphabet, he'd be likely to use an associated word as the basis for mixing the other. I tried every word

associated in my mind with the word "cipher," one after the other, and it took minutes to test each guess. I thought of words like "alphabet, secret, substitution, Wheatstone," and so on. Finally, I exhausted my efforts. Mrs. Friedman, who was my right hand man at the time, was sitting in another part of the room, and I said, "Elizabeth, will you stop what you're doing and do something for me?" She said, "What do you want me to do?" I said, "Make yourself comfortable. I am going to say a word to you, and I want you to come back at me with the first word that pops into your head." She made a pass or two with her lipstick and said, "Shoot." I said, "Cipher." She said, "Machine." That was it! In about ten minutes we had reconstructed the outer alphabet and solved the messages. The first message said: "This cipher is absolutely unbreakable." We telegraphed the solution to Washington, word got to London, and they had to kill the project. When I got to the AEF in France I wasn't very well liked by our British friends. That Wheatstone principle is attributed to Sir Charles, but not long ago by sheer accident I came across this device: it's in our museum now and was made by a Major Decius Wadsworth, U.S. Army. Wadsworth was aide to General Wilkinson, of Revolutionary fame, and he later became Chief of Ordnance. How he became interested in ciphers I don't know, but he certainly made this device. It bears on it - this is a very poor picture - the date 1817, while Wheatstone conceived his device and described it in 1870. Hence, credit for the invention of the so-called Wheatstone principle belongs not to an Englishman, but to an American.

I come now to a cipher device allegedly invented by a Frenchman, a Commandant Bazeries, and called the "Bazeries cylinder." The Bazeries device

consists of a shaft on which are mounted 20 discs which can be arranged in keying order, each disc bearing an identifying number and having a different alphabet on it. Having set up the discs in key order, you line up the letters of your plain text message thus: "Je suis indechiffrable" ("I am indecipherable") is what it says on this line; and for your cipher text you can take any one of the other horizontal lines of cipher letters. This looks like a system based upon an excellent principle, but it is quite readily solvable these days — if you have the device. The principle, however, was not invented by Bazeries; it was invented by our own Thomas Jefferson, and here is his description of the device which he called "the Wheel Cypher," using exactly the same principle. I had an interesting time digging up the facts in connection with an article I was asked to write for the definitive edition of Jefferson's writings now being published at Princeton. In 1915-16 a United States Army officer by the name of Parker Hitt independently invented that same principle again, this time not in the form of discs, but sliding strips, you see; this is a picture of his original model. Mrs. Hitt came to Riverbank, where I was then educating myself in cryptography, and she brought along her husband's invention, saying it was pretty hot stuff. She put up a challenge message on the device, which I solved by hocus pocus, you might say, like this: I thought to myself, "Well, this lady, Mrs. Hitt, is beautiful and charming, and so forth, but she doesn't know much about cryptography. What kind of a key would she be likely to use for mixing up the order of the strips? Well, she might use the key 'Riverbank Laboratories.'"

~~SECRET~~

That was it! In 1918 that same principle was adopted by the United States Army Signal Corps; there it is, the M-94 device. This, as you see, uses .25 discs with differently mixed alphabets; you can put them on in any key order you please, — exactly the same principle as Jefferson's or Bazeries' or Hitt's device employed. We used Cipher Device M-94 for quite a number of years after World War I with some success. The Navy, the Marine Corps, and the Coast Guard also used it. By adopting Hitt's sliding strip form, which lends itself better to changing the mixed alphabets frequently, we got greater security in a device we called "the strip cipher" or Cipher Device M-138 in the Army.

This, gentlemen, is a picture of the very first SIGTOT or one-time tape cryptographic transmission machine, produced by the AT&T Company in 1918, too late to be used in World War I. The principle is: here you perforate a tape bearing your plain-text message, here you have a previously-prepared keying tape passing through a transmitter, here is another keying tape passing through another transmitter; these tapes are different and in the form of loops of different diameters. Suppose this one is a thousand characters in length and the other 999. If you start them out at initial given points, according indicators, those two points won't come together again until you have enciphered 999,000 characters! A pretty good principle, but, again, on a challenge, — this was after I came back from the AEF, was demobilized and then went back to Chicago to the Riverbank Laboratories — on a challenge, I solved a set of messages in the system, without having the machine or the key tapes. This was supposed to be absolutely indecipherable; G-2 said so in writing in a letter signed by the Director of Military

Intelligence, but I was able to solve the thing, as I have just said, without having the tapes, without knowing how long they were, or the machine. It was a long and interesting solution, but I haven't the time to go into it.

This is a picture of a new type of cryptographic machine. A gentleman by the name of Hebern out in California came forth in about 1922-23 with a keyboard, a rotor which acts as a switching commutator really. The current from the keyboard depressions enters at this side (a fixed commutator), goes through the wheel here, exits at this fixed commutator, and then to the light-bank or typewriter. Now, this machine had only one rotor. In about three or four years, after collaboration with the Navy, he came out with a five-wheel machine, five rotors, you see, and these are the types of rotors that he used, which gave pretty high security. The Navy was about to adopt these things. They were about to place a contract for $75,000.00 with Hebern. Now that hit me when the chief of the Navy Code and Signal Section, Lieutenant Strubel - now Admiral Strubel in charge of the 8th Fleet in the waters around Formosa - told me what the Navy had in the way of cash for cipher machines! We in the Army didn't even have a dollar for that sort of thing at that time! Well, Strubel asked me: "What about it?" I said, "I'll study it." I studied the matter for about six weeks before I had a really good idea. Then I went to Strubel and said, "I think I can solve messages." He said, "You'll have to show me." I said, "All right, I accept your challenge." He said, "OK. What do you want?" I said, "I want ten messages set up on your machine." He gave me the ten messages, and I solved the thing.

It was a curious thing that happened to me one evening as I was getting dressed to go out. I'd been working at the problem, of course, and it took weeks of making distributions and finding my way around. I had one assistant at the time - he was a veteran, an enterprise fighter, with crossed-eyes, cauliflower ears and all, and he wasn't much help, except in typing. I had reduced a problem involving millions and millions of alphabets to a place where I had one line of 26 letters reduced to a certain form. If I could solve that one line I would have a start. Well, I went home that evening I mentioned, much preoccupied. I had a clear picture in my mind of this one line, but all I knew was that certain letters were the same, certain ones different - and, of course, I kept in mind the specific positions of those letters. For instance, the first six letters were all different, but the 3d, 7th, 11th, 19th and 25th were identical; the 4th, 21st and 26th were identical, and so on. Well, as I said before, while getting dressed to go out to a party that night, fiddling with my black bow tie, all of a sudden it came to me in a single flash, like lightning!! The phrase that would exactly fit the positions of the repeated and the different letters was "President of the United States." That was it! The next day I came in and verified the assumption. In a few days I handed the Navy a solution; they killed the order. The Hebern firm went to pieces; Hebern, the inventor and president of the firm, wound up in San Quentin for a couple of years because he ran afoul of California's "blue-sky laws." You see, the Hebern Company's stock had skyrocketed on the hot tip that a Navy order was coming through; and when the Navy order didn't come through as anticipated, the stock dropped to about $2.00 a share. Hebern picked up some of the $2.00

stuff, went to a different part of the state, and sold it for $10.00. The California authorities didn't like that, so they put him in the hoosegow.

This is a picture of the first cipher machine invented and built in Europe, called the Enigma. It was sold on the commercial market until the Nazis came into power. Here are the rotors, you see; four of them here, a keyboard and the light bank. You press the keyboard, the rotors step, and the lamps light up. You position these rotors according to prearranged keying instructions. Now, also in Europe a bit later there were other inventors. Here is a machine called the Hyha, which was considered to be a very complicated and difficult thing - nobody could solve it. Here is a German professor who put out a treatise on the indecipherability of the thing, showing how many permutations and combinations there were. Everybody in the world could be provided with a machine and a different key, there were so many permutations and combinations available. Well, gentlemen, merely the number of permutations and combinations that a given cipher system affords, like "the birds that sing in the spring," have nothing to do with the case, or at least very little. It all depends upon the nature of these permutations and combinations, that it, what they are basically in the cryptographic sense. For instance, take the principle of monoalphabetic substitution, the principle Poe used in "The Gold Bug." Theoretically, with a 26-letter alphabet you can make 26! cipher alphabets. Now 26! is a large number: 403,291,461,126,605,635,584,000,000, that is, four hundred and three quadrillions, two hundred ninety-one thousand four hundred and sixty-one

trillions, one hundred twenty-six thousand six hundred and five billions, six hundred thirty-five thousand five hundred and eighty-four millions. Quite a large number. So, if you were to try to solve a cipher such as that in "The Gold Bug" and were to go at it simply by trying all those quadrillions of permutations of the alphabet, you'd need lots of time and manpower. Because it has been calculated that merely to write down those permutations it would take a thousand million men working a thousand million years to do the major part of the job - not all of it - and the scroll would reach from Earth far beyond the planet Mercury! Yet, any of you can solve "The Gold Bug" cipher in a few minutes, despite the vast number of permutations that a 26-letter alphabet affords.

Here is a picture of a Swedish machine of about the same period: a keyboard; a light bank; and a set of rotors. The rotors are of a bit different type in this case. Of course, the light-bank type of machine was slow. You had to sit down and copy by hand and so on; so the inventor of this machine hooked it up with an electric Remington typewriter, and that was the first model of a printing cipher machine. He later modified it so as to have the printing mechanism self-contained in the cryptograph, and that's a picture of the machine from the outside; and there is a picture of the internal workings. There is the keyboard. Here are the switching commutators, with pins which are put in and out of effective positions, like on our Converter M-209. Those pins drive a certain lever, here, which drives the switching commutators, which are in here; you can also switch the effects of the commutators by means of these plugs. Here is the printing mechanism. This style you'll recognize as being very similar to that in Converter M-209. The text is printed on a tape.

Years ago, of course, considerable thought began to be devoted to the encipherment of teletype communications. Aside from that 1918-19 A.T. & T. Company machine that I showed you a few minutes ago, this was the first of the teletype cipher attachments developed for security purposes. It was an invention of Colonel Parker Hitt, who retired from the Army about 1925 and joined the International Telephone and Telegraph Company, where he devoted himself for two or three years to producing this machine. There's the internal mechanism. It had keying wheels which affected the five bauds representing the teletype characters. These wheels were of differential diameters. This one had 101 points, this one 99, this one 97, and so on, down, so that it had an extremely long period; but the length of the period, again, like "the birds that sing in the spring," has little to do with the case. The machine was put into test usage in the State Department, which called upon the War Department to make a security evaluation. I was assigned to the job, and had an interesting time with this. The State Department put up a series of messages. They were stamped in at a certain hour, about 10:00 o'clock in the morning; about 10:30, Mr. Salmon, the chief of the State Department communications, called me and said, "The machine is out of order. Maybe you can fix it." I said, "I'll be up there in a few minutes." I slipped a piece of paper in my pocket, and hustled over to the State Department, then in the old State, War, and Navy Building. Upon arrival, Salmon was apologetic. "I'm sorry," he said, "I tried to catch you, but you had already left. It's working again, so I won't trouble you." I said, "By the way, I have a question to ask about those messages." He immediately got suspicious and asked, "What do you want to know?" And I said,

SECRET

"Have you got the plain texts to these messages here?" He drew himself away from me and said, "Well, yes." I said, "Where are they?" He said, "In that safe over there." I said, "Well, I'll sit here. You go over to the safe and dig out message No. 7. I want to ask a question about it." Very reluctantly he got up, opened the safe, pulled out message No. 7, and, with his back to me, the message being held close to his vest, said, "What is it you want to know?" I pulled out my piece of paper, and I said, "Well, does it say ——?" and I read him the whole message. He almost sat down on the floor in astonishment. That was only 35 minutes or so after it had been received. The ITT Company burned its fingers on this development, gave up the investment and never tried again. I've told you about the AT&T Company studying and inventing cipher machines, and the IT&T Company; the Automatic Electric Company of Chicago, and the IBM Company also tried their hands at it and failed. The basic reason for these failures is that without first-class cryptanalytic guidance nobody can invent a cryptographic machine that is going to stand up under organized attack by cryptanalysts with the proper "know how."

This is Converter M-209, which we adopted; it was a Swedish invention and is pretty good. It was the only thing we came across in 1940 suitable for our use in the field. Here are keying wheels. Here is a barrel of movable staves, which are affected by the keying wheels; the staves, as they move to the left, and in number from 0 to 25, affect a print wheel, and there is the tape. A very neat gadget but a bit slow and not too secure when you have two or more messages in the same setting.

Now, the rest of the time I would like to devote to a brief discussion of cryptanalytic gadgetry. This, to my knowledge, is a picture of the first cryptanalytic aid, something I got up at Riverbank way back in 1916, I think it was: a pair of glass plates guides or grooves in which alphabet strips could be slid up and down in order to align letters and study them, for various purposes. I don't remember now why I put down on it "The U. S. War College." I had no relations with them, but it was nice to hand them a present, so I did that. I made those strips with my own hands. This was a wheel with rubber letters that I could arrange in any order I pleased to make up alphabets. There's another view of the thing, and here's a whole bunch of them put together, for whatever purposes necessary.

Now, from that early start have come a great many very interesting developments. Here is a picture of a memo dated October 30, 1934, which I sent to Captain King and Major Aldin, now Chief Signal Officer, and in which I made some remarks. You can see evidences of tears or maybe drops of blood on this thing. I was asking for a little bit of money to get some IBM machines. I said, "Please do your utmost to put this across for me. If you do, we can really begin to do worthwhile cryptanalytic work." Well, the plan was successful - we got it. Here's a picture of part of the contract, you see, dated the 12th of November. It took only a month. And here is what we were getting, and see these prices. When I think of the millions of dollars which the Army's Signal Intelligence Service spent during World War II on this sort of thing, I am amazed that from such lowly beginnings should have come that great establishment of IBM apparatus. This is a room, just <u>one</u> wing of several in our headquarters during the

war, with tabulating machines, here, just one after the other IBM machines, either standard or modified for special jobs.

You know the picture the average person has of a cryptanalyst. He's a long-hair. He wears thick spectacles, has long whiskers with crumbs in them and so on; he goes into a huddle with himself and pretty soon he comes up with an answer. Well, that's far from the picture these days. Cryptanalysis and communications intelligence is "big business" now, and I want to say a word or two about that aspect of the subject. Cryptanalysis of modern crypto-systems has been facilitated, if not made possible, by the use and application of special cryptanalytic aids, including the use of high speed electronic and digital computers, some of which I'll show you slides of to come. Some are standard machines, but mostly we devise and use modifications of them. More importantly, we have recently gone into the invention, development, and production of highly specialized cryptanalytic gadgetry. At this point I must take a few moments to clarify the picture and in simple language tell you what such gadgets do for us. As I said before, the mere number of permutations and combinations afforded by a cryptosystem or so isn't too significant. It's what they amount to or involve in terms of cryptographic meaningfulness and complexity. In modern cryptanalysis what you are up against are complex cryptosystems which generally involve, for their solution, the making of a great multiplicity of hypotheses each of which must be tested out, one after the other, until you find the correct one. The job of the cryptanalyst is to devise short cuts for testing the hypotheses, short cuts often based upon the use of statistics and statistical theories having to do with the relative frequencies. Once

having devised the proper test or tests for each hypothesis, or for several concurrent hypotheses, human labor could be set to work making the millions of tests in order to find the correct hypothesis or to cast out the vast majority of incorrect ones. When each test is complicated, or lengthy, it is obvious that you'd have to have, as we used to say, factorial n Chinamen to do the job, or else the job would take long. But it is our experience that every test which can be made by hand can be mechanized, and it is further our experience that in most cases it is practicable to build machines which will make the tests. I don't have to tell you that machines don't tire as rapidly as humans, they don't need much sleep, or time out for meals, or for recreation or for such things as shopping, love-making, etc. — in short, the "care and feeding of machines" is a relatively much more simple matter than the "care and feeding of human beings." So, we have cryptanalysts who devise the tests; then we have cryptanalytic engineers who mechanize the tests, and then devise, invent, develop, and produce the machines to perform the tests at high speeds. Then we have to have maintenance engineers to keep the machines in good working order; and they have cryptanalytic assistants who examine the output of the machines, and who are usually able to take the correct hypothesis or few correct ones and go on with them to the final stage where a key is recovered. Next we may have to have other machines which apply the recovered keys to specific messages and produce the plain texts from them. But in all these steps, let me emphasize, the machines can do only one thing, they can only perform, at a high rate of speed, processes which the human brain and hand can perform but only at a much slower rate. Let me emphasize that these machines don't, they can't, replace the thinking processes involved in cryptanalysis.

Next we have to have automatic

SECRET

Now, I want to show you what some of these machines look like. Here is a highly-specialized machine for deciphering messages; we call it an "analog" because although it does what the enemy's cryptosystem does, any resemblance between it and the enemy's machine is purely coincidental. To explain, I'll say this: In a cryptanalytic processing center, we try to duplicate with a few people what thousands of people on the enemy side are doing, for it takes thousands of soldiers to encipher and decipher the messages of the many headquarters involved in intercommunication. All these messages, or most of them are intercepted, they all flow into one place, and you can only have a certain number of people to process them. If you have the key or keys, then it becomes a problem of production-line deciphering; so we devise special machines to decipher the messages. As I said before, the machine may not have any resemblance whatsoever to the enemy's cryptographic machines, but it duplicates what their machine does, and does so at a high rate of speed. Here's a picture of such a device. In this next slide you see a tabulator, a standard tabulator with a special attachment devised by our own engineers susceptible of doing what we call "brute force" operations, where you are trying to solve a thing on the basis of repetitions which are few and scattered over a large volume of messages. Well, if you've got millions and millions of letters, or code groups, the location of those repetitions is a pretty laborious thing if you have to do it by hand, so we speed the search up. A machine of this kind will locate those repetitions in, say, one-ten-thousandths of the time that it would take to do it by hand. Here is a specialized machine, again a tabulator, with an attachment, here, that is

used for passing the text of one message against the text of another message in order to find certain similarities, or perhaps differences, or maybe homologies, and it does it automatically. These relays are set up according to certain circuitry; you start the machine, and low and behold, it produces a printed record of the message repetitious or what not.

Here is a machine which I personally call "Rodin," after the piece of work by the great French sculptor Rodin, who sculpted a piece of engineering known as "The Thinker." This machine almost thinks. What it does is this: you ~~set up certain logic~~ feed into it a certain number of hypotheses and you tell it, "Now, you examine these hypotheses and come up with one which will answer all the following conditions." The machine takes the first hypotheses, let's say, examines that, and as soon as it comes to a contradiction it says, "Well, that's no good; I'll go back and take up the next one." And so on. It tests the hypotheses, one after the other, at a high rate of speed, at electronic speed. That's only one small section of the machine.

Well, we've got left here a few minutes in which I should say something about the current employment or manner of employment of communications intelligence. I've devoted two hours to talking about the background and development and haven't said very much about the manner of its employment. Well, we could discuss that under various headings, but it is obvious from the disclosures of the Congressional Pearl Harbor Committee that the manner of its employment in shortening World War II must have been very efficacious. I wish I had the time to read you the whole of the Marshall-Hewy

correspondence that the article in Time was based upon, but I think that just a brief extract will be sufficient to give you a pretty good idea of the contribution ORCON made toward our winning World War II. These are all in that correspondence, which was practically broadcast to all the chanceries and war offices of the world when it was disclosed during the Congressional hearings. General Marshall, you'll remember, in his letter to Governor Dewey, sent during the hot political campaign of 1944, was asking the Governor not to use certain information Dewey got by surreptitious channels. Here are some excellent illustrations of the manner of employment of ORCON:

> "Now the point to the present dilemma is that we have gone ahead with this business of deciphering their codes until we possess other codes, German as well as Japanese, but our main basis of information regarding Hitler's intentions in Europe is obtained from Baron Oshima's messages from Berlin reporting his interviews with Hitler and other officials to the Japanese Government. These are still in the codes involved in the Pearl Harbor events.
>
> "To explain further the critical nature of this set-up which would be wiped out almost in an instant if the least suspicion were aroused regarding it, the Battle of the Coral Sea was based on deciphered messages and therefore our few ships were in the right place at the right time. Further, we were able to concentrate on our limited forces to meet their advances on Midway when otherwise we almost certainly would have been some 3,000 miles out of place.
>
> "We had full information of the strength of their forces in that advance and also of the smaller force directed against the Aleutians which finally landed troops on Attu and Kiska.
>
> "Operations in the Pacific are largely guided by the information we obtain of Japanese deployments. We know their strength in various garrisons, the rations and other stores continuing available to them, and what is of vast importance, we check their fleet movements and the movements of their convoys.

"The heavy losses reported from time to time which they sustain by reason of our submarine action largely results from the fact that we know the sailing dates and the routes of their convoys and can notify our submarines to lie in wait at the proper point.

"The current raids by Admiral Halsey's carrier forces on Japanese shipping in Manila Bay and elsewhere were largely based in timing on the known movements of Japanese convoys, two of which were caught, as anticipated, in his destructive attacks.

* * * *

"The conduct of General Eisenhower's campaign and of all operations in the Pacific are closely related in conception and timing to the information we secretly obtain through these intercepted codes. They contribute greatly to the victory and tremendously to the savings of American lives, both in the conduct of current operations and in looking toward the early termination of the war."

* * * *

What I am going to say next is very important. The interception of foreign communications and subsequent processing requires the services of numerous communications and other trained personnel. In order that the product may be most useful operationally, and not merely historically interesting, the intercept traffic has got to be forwarded as expeditiously as possible to the processing center, and after processing the COMINT product must be promptly transmitted to the people who evaluate it from an intelligence point of view, integrate or collate it with intelligence from other sources, pass the results then to other intelligence personnel, and, in some cases where it makes a difference — a great difference, seconds perhaps — see that it is transmitted direct to operational commanders. The need for trained communications personnel, intelligence

experts, radio and electronics engineers, mathematicians, linguists, cryptanalysts, and other highly skilled personnel, military and civilian, is therefore quite obvious. It takes a large organization. In 1939 or 40, the totality of personnel in the Army and Navy devoted to this work was about 300. In 1945 we had 37,000! That gives you some idea as to what it takes, aside from millions and millions of dollars for equipment, both communications equipment and this type of equipment that I gave you a little story about.

Some of the cryptanalytic and communications intelligence processes can be accomplished in the field to meet certain immediate needs of field tactical commanders, and these have been provided for by each of the three Services in order to meet special needs in this category. But communications intelligence processing involves a rather large and intricate complex of a good many activities, much of which can be done well only at major, large processing plants where the limited number of highly skilled personnel can be concentrated and very special specialized cryptanalytic machinery can be installed and maintained. You see, we have to concentrate the skilled personnel because there are only a limited number of them. You can't find people trained in this field in civil life, because there is no need for cryptanalysis in commerce or industry, so that when war comes we don't have a large pool of trained civilians from which to draw to augment our forces. We've got to take basically intelligent people with good backgrounds, and good education, and train them ourselves. The clearance process alone takes months, and while during that time we can give them some basic training, the more complex phases have to be absorbed largely by on-the-job training.

SECRET

Now, I want to say a few words about the very great importance of coordination of communication intelligence activities with other intelligence operations and the tactical situation. There you've got to have certain cover methods. For example, when a decision has been made to take action based upon communications intelligence, a careful effort must be made to insure that the action cannot be attributed to communications intelligence alone. Otherwise you will kill the goose that lays the golden egg. When possible, action must always be preceded by suitable reconnaissance or other operations which will serve as cover or deceptive methods. For example, if there is a convoy out in the middle of the ocean and suddenly it is attacked by air, the question might well rise, "Well, how the hell did they know we were out here, way off the beaten track?" You see, you make cover for that, perhaps by air reconnaissance — or it seems that way to the enemy.

Another aspect of coordination between operations and communications intelligence is to be mentioned. The communications intelligence producers must be carefully and fully oriented to give optimum coverage of tactical operations in progress, or contemplated. There are just so many facilities and personnel available for communications intelligence work, and there's a great deal of traffic, an enormous amount. Only a fraction of it can be processed, so you've got to neglect the rest. It's essential, therefore, that the communications intelligence workers be abreast of the current situation so that they'll know where to put their maximum effort. Also, their knowledge of the tactical situation is essential to a proper interpretation of certain results they obtain.

It's important, also, to correlate the communications intelligence work with tactical operations in another phase of operations. If in exuberance our bombers knock out enemy radio stations, the very success of such an operation has repercussions upon communications intelligence. You see, putting those stations out of business makes unavailable to us a lot of traffic; so that operations of this sort must be coordinated with the COMINT authorities. There is another reason for being very careful to coordinate, and that is that cryptosystems are usually world-wide or area-wide in distribution, and if you don't coordinate tactical operations with your COMINT authorities, so as to cover up your source of information, the enemy will soon suspect that his cryptosystem has been compromised which would have far-reaching consequences. You see, a commander who is a recipient of COMINT and seeks a minor advantage by using it in one locality may deprive commanders in other areas of much greater advantage; you want to be sure that you don't compromise the source of information — that's the important point in this discussion. While knowledge and experience point to the necessity of exploiting every possible advantage that the situation affords when you get this stuff, and in the heat of battle the temptation is, of course, very great to use the material whenever it is available, nevertheless this often may lead to carelessness in its use, which may lead to jeopardizing the source. Of course, the full value of communications intelligence cannot be realized unless operational use is made of it. However, when action is contemplated based upon such intelligence, the possibility of compromise of the source must always be

borne in mind and the danger weighed against the military advantages to be gained. Minor advantages never alone are sufficient ground for risking the loss of the source.

Well, gentlemen, it's 10:00 o'clock. I'm sorry that we don't have any time to answer questions, but I welcome you to examine the exhibits. If I can answer a question while you are doing so, I will be glad to do that. Thank you very much for your courtesy and your attention.