Second carbon
of revised
lecture

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

Maxwell Air Force Base

29 September 1950

SECRET

~~SECRET~~

This is the original transcript of the voice recording made on delivery of the talk on 29 Sept 50. The transcript was made by secretarial staff of the School and then sent to me for corrections and editing. W.F.F.

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 Sheetz, Gentlemen, first I want to assure you of my appreciation of the opportunity to come 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 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 Simarlus. She took an interest in cryptography, apparently, and she died. Presumably she went to Heaven, or perhaps to the other place, but she had left instructions as to the disposition of her remains, and they built for her an imposing mausoleum in which her sarcophagus rested. On the outside of the mausoleum there was carved a message, and the message said, "Stay, weary traveler, if thou art footsore, hungry or in need of money, unlock the riddle of the cipher graven below, and you will be lead to riches beyond all dreams of avarice." Then underneath it there was this cryptogram. For several hundred years all the experts tried their hands at deciphering this message without success, until one day, presumably, a long-whiskered, bespectacled individual came along and after working at it for a considerable length of time, solved the message, which gave him instructions as to a secret entry into the tomb. He got inside and then found

~~SECRET~~

an instruction to open the sarcophagus, but he had to solve another message, which he did, and opened 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 monster, 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 thirty years I have had occasion to wish that I knew the old gal's address so that I could put as a first indorsement to the basic communication the single word "concur." Well, anyhow, it's been an interesting life, if not financially lucrative.

Now I am going to read you a little paragraph from Time dated December 17, 1945. "Magic is the Word for It" is the title of the article. "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." Well, General Marshall continued the story of "Magic's" magic. And then it goes on to say what that story was, and I hope I'll have time to come to it a little bit later on.

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 - this was before the war - and to avoid naming names I will simply say that there was a chap in a certain capitol 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. He said, "You know, these many exchanges that we are having dealing with this matter in hand have made it necessary to be very voluminous in our correspondence, and I am a little bit afraid that perhaps some third party might be able to read the communications." Well, we read that, and we were very much upset for fear something would happen, and so we were on tenterhooks and pins and needles for two or three days until we got the reply from headquarters. To paraphrase the reply, it said, "Well, you southern extremity of a horse's anatomy, don't you realise that what you are saying is out of line? Don't you know that our system has so many permutations and combinations it's inconceivable that anybody should be able to read these communications without having the key? Now, don't you worry any more about it. You tend to your own mission, and we'll tend to ours." We were very happy when we read that one.

I hardly need to give you a definition of communications intelligence. I think that Major Morrison has already dealt with it, and I will simply cite the 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 communications intelligence, which is based upon the science of cryptanalysis, forms a very interesting history. It is inextricably bound up with the history of cryptography. The two are but opposite faces of the same coin. Progress in one inevitably leads to progress in the other. Hence, while my talk is to be devoted largely to cryptanalysis and communications intelligence, I will have to deal also with cryptography and communications security to a certain extent. 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 this field of work by our enemy, security rules prevent my saying very much about them. I can only give a fairly good background of U.S. activities, and even then I will not be able to say very much about meaty activities, because I don't know very much about that background and prefer not to give any information that 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 the same vice versa. In the course of my talk I will give illustrations, many 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 show an instance of cipher in the Bible. In Jeremiah 25:26 occurs the expression "And the king of Sheshach shall drink after them." Also in Jeremiah. Well, for many, many years that word "Sheshach" 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, you set up a substitution alphabet whereby you can replace the letters by equivalents. For example, "she" is represented by "beth" or vice versa, so that "Sheshach," translates "babel", "Babylon." The vowels had to be supplied. Incidentally, Daniel, who was the first psychoanalyst, was also the first cryptanalyst. I say psychoanalyst because you remember how he interpreted Nebuchadnezzar's dreams. Nebuchadnezzar had a dream, and when he woke up he couldn't remember it. He called for his sorcerers and asked them to interpret the dream. They asked him what dream, and he said, "Well, I don't remember it, but that's your job, to find out and then interpret it." That was a pretty good assignment, and they failed. They had a nasty habit of chopping your head off in those days if you failed, so they got Daniel and he, by some means - the record doesn't show just how - was able to reconstruct the dream and then interpret it. Then some years later Nebuchadnezzar's son, Belshazzar, was giving a feast, and during the course of the feast a hand appeared on the wall behind the candlestick and wrote a message, and Belshazzar was very much upset and called for his soothsayers and so on, but they couldn't read it. The message said, "Mene mene tekel upharsin." Well, Daniel was called in and apparently succeeded in deciphering this message, and the 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, the Bible is indefinite - Thy kingdom shall be divided and given to the Medes and Persians."

The next is an illustration of the earliest cipher device history records, which is the spitalae used by the ancient Greeks. They had a baton or cylinder of wood around which they wrapped spirally a piece of parchment, and they wrote the message across and took the piece of parchment then and sent it to its destination, where the recipient, having an identically dimensioned rod or cylinder, would be able to reconstruct the message. This diagram, incidentally, is not correct. The writing was done along the edges of the parchment. Incidentally, the baton which the European field marshall carries as one of the insignias of his high office derives from this instrument.

Caesar, of course, is well known in history to have used cryptography, a very simple method, no doubt, because all he did was to replace each letter by the one that was fourth from it in the alphabet. Cicero was the inventor of what is now called short hand. He had a slave by the name of Tero who wrote for Cicero his records and so on in Terronean notes, as they are called.

The beginnings of modern cryptography are to be found in Venice in the Papal states about 1400. I show next an alphabet of the period of 1400 which is interesting merely because it shows that in those early days they already had a recognition of the weakness of what we call single or monoalphabetic substitution. A solution, of course, is accomplished by frequencies. I don't have to go into that. I think all of you at some point have had some contact with that sort of thing. But here is a method of disturbing the normal frequencies by having the high frequent letters represented by a multiplicity of

SECRET

of characters. Now, the earliest tract that the world possesses on this subject of cryptanalysis is that which was written by a Neappolitan whose name was Sico Simonetti. It was written in 1474. He describes the methods of solving simple ciphers, no doubt, but in a very clear and concise form. The first book, extensive treatise on cryptography is that by a German abbot named Trithenius, who wrote his monumental work in 1531. He planned to write four volumes, but he quit with the third one because somehow or other he got charged with being in league with the Devil, and they burned his books, as a matter of fact. We are going to jump a ways now to some examples from history. There is a cipher alphabet and system used by Mary, Queen of Scots, in the period 1545, or thereabouts. There was an Italian cryptographer whose name was Porta who wrote a book published in 1563, and in it he shewed certain types of alphabets which have come down in history now as Porta's alphabets. That's an example, taken not from his book but it shows one alphabet with key letters, a or b, another alphabet with key letters c or d. 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 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 probably, 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 the earliest of the men to solve a system of key substitutions where the key is changing constantly. Porta's table was actually used in official correspondence. That is a picture of a table that was found among the state papers of Queen Elizabeth's

SECRET

time, communicating with the ambassador to Spain.

The next slide I show is the so-called Vigenere square or Vigenere table, a set of twenty-six alphabets, all displaced step by step with the plain text letters at the top and the key letters at the side, and the method of using is to take a key word and the equivalent change in each alphabet according to the manner in which the key changes. Now, Vigenere also has an interest to me because although he is credited with having invented that square, he never said he did, never made any such claims. That's a picture of it as it appears in his book, and it goes considerably beyond what the ordinary references say about his table. I won't go into those differences. They're technical and perhaps of no great interest to us today.

The next cryptographer I wish to mention is a Frenchman, Francois Vieta, an eminent mathematician, founder of modern algebra. In 1589 he became Counseler of Parliament at Tours and then Privy Counseler. While in that job he discovered the key to a Spanish cipher of more than 500 characters, and then 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. There is another example. Here are the alphabets and a sliding card which could be shifted up and down was used as a changing key, a method of changing the key. Here is another called the two square cipher, two alphabet cipher, using coordinates again, but there is one complete alphabet and ther is another one, and the coordinates are used to represent those letters. That was actually used in Charles I time, 1627, communicating with France and Flanders.

I want to jump now to the Revolutionary War period 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. It appears that there was an American whose name was Lovell who was the cipher expert of Congress who 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 a two-part principle. This is a section of the decoding volume. 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 in the encoding section the words are in alphabetical order, and their equivalents are in random order, a system which even today sees 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 indecipherable treasonable Cow Letter, which has never been deciphered. It reads, "I have bought a cow and calf from Gen. John Joseph Burleson," 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 landmark in the history of cryptography. About 1821 a Frenchman, Champolio, startled the world by beginning to publish translations of Egyptian hieroglyphics. This is a picture of the Rosetta Stone, Egyptian hieroglyphics decoded to Egyptian and then Latin, and it was by means of this inscription that this was finally solved. It represented a cryptanalytic problem. In the hieroglyphics there are things that we

call cartouches, that is, things surrounded by a graven line. Here are some few examples. This was on an obelisk, and this one was suspected of representing the name Cleopatra, and I suppose the reason for suspecting it 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 was Cleopatra, it turns out that by taking the letters and substituting its equivalent and putting them in the proper places, bit by bit Champolio was able to establish other names, like Ptolemy and Alexander and so on. That's the way in which the Rosetta Stone and Egyptian hieroglyphics were finally read. It was very fortunate that the early studies on Egyptology had not realized that the Egyptians used cryptography. Some of their writings are not only hieroglyphic, but they are also cryptographic, and this 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 American period of the Civil War or the War Between the States. Here is a picture of a cipher device used by Confederate Army captured at Vicksburg, one of my treasures. The method of use of this is a cylinder covered with a sheet of paper bearing alphabets, the Vigenere table, in other words, a pointer that you could slide and a thumb knob you could turn the alphabet according to the key letters.

There is one person I passed over in getting to the Civil War period. Edgar Allan Poe in 1842 or thereabouts kindled an interest in cryptography by his story of "The Gold Bug" and by a couple of articles in journals dealing with cryptography. Here is a picture of a message, authentic, which was sent by President Lincoln to Gen. Burnside, and it's very simple. It reads this

way, of course, but if you read it backwards, "If I could 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. This is a photograph of a page or two from the code book and cipher system used by the Federals. They had what is called today a route cipher, that is, you had a matrix with indications of route. Here's how you write the message in, the first word, second, third, fourth, fifth, sixth and so forth, and then take it 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 famous names of officers of that period. I have with me today the complete set of books used by the Federal Army during that period, and after my talk those of you who wish may come up and examine it, together with certain other exhibits. Next is a picture of a message sent to General Grant in that route cipher. I shall not take time to read that. 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 they were completely cut off, and the message was then photographed down, and it was the first and earliest example that I know of of micro writing used for military purposes - photographed down and sent out by means of carrier pigeon, and this is a copy of one of the examples.

After the Civil War or War Between the States the use of cryptography in the United States military affairs went into a decline for a long period of peace, and was broken only briefly by the Spanish American War. The War Department published a code called "Codes to Insure Secrecy of Telegrams" in 1885

based on a small commercial code, almost word for word. I'm sorry I don't have a copy of that with me. In the Spanish American War there was very little cryptography. They used that code which had no secrecy whatever, but then there was no such thing as radio. 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, War Department Telegraph Code was published and printed by a commercial house in Cleveland. We come now to the World War I period with Hertz's discovery of these 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, because these were used in preference to code systems, which came later. Here is a picture of a cipher system used by the Russians. Nothing but the Vigenere system all over again, but using numbers instead of letters. Here is a case involving a set of 7 or 8 alphabets used for substitution. This was the deciphering table. The next one is a picture of a front cipher system, a transposition system, the key columns being here and in addition certain disturbing elements by taking off the letters in diagonals. And that is a picture of the system used by the Italian army in World War I. Again, it is only a variation of the Vigenere system. And here is a system used by the Germans, invented by them, or really, I should say, it was a combination of two methods put together in a

very clever way. We called it the ABSGBX cipher because the cipher text consisted exclusively of those letters. An alphabet in here arranged according to some keying order with the coordinates ABSGBX, you enciphered your message by substituting the coordinates with the letters as you see here. The letter r is represented by B and so forth, and then you write a key developed from the key word over your X's and A's and so forth and take the letters out in columns according to the key order. That was a brand new thing in military affairs and caused no end of headaches until it was discovered just how the solution could be achieved. In that case, the solution was not a general solution but depended upon special instances, and I don't have the time to go into that. That cipher was used by the German high command and consequently someone soon discovered that you made a chart based upon the number of ABSGBX messages intercepted, why you could disciver certain things about the tactical situation and especially about what might happen. This is a chart which we got up in the AEF based upon the ABSGBX intercept. This, gentlemen, is the first illustration that I know of in history of traffic analysis, traffic intelligence. The next slide gives a picture of the sort of thing that we put out, a bulletin that we put out when the ABSGBX messages were read, and there are a set of messages from November 20, 1918, of course the war was over, but this gives very important information about the withdrawal of McKenson's army. There is the German text and there is the translation, an authentic message. //The British and Americans used a cipher known as the Playfair cipher, invented allegedly by Lord Leon Playfair, but he didn't invent it - Sir Charles Wheatstone invented it. The method of encipherment is to have a key word, then the rest of the letters of the alphabet, and if you wanted to encipher "at" the equivalent was

"vr" by diagonals, and so on. There is an example of a message enciphered. In those days, 1914, that was regarded as pretty hot stuff. In fact, an officer of the American Army later became Chief Signal Officer, Maj. Gen. Moborne, wrote a little treatise published in 1914 in which he dealt with this Playfair cipher system, and the title of his work is "An Advanced Problem in Cryptography." Today our most elementary students are given things of that sort to solve. The British Army proposed a cipher device in World War I, and they had manufactured a great many of them and distributed thousands, and they proposed to the French and the Americans that they use the same thing for tactical communications, but it was never put to use for reasons that I hope to tell you later.

Now, I'd like to say a few words about code and code systems used. I think you all know that a code system is simply a sort of dictionary in which the words, phrases and sentences are representable by arbitrary groups of letters. Here is a page from a commercial telegraph or commercial cable company's codebook that they offer to their customers. You'll notice that each of these code groups differs from every other code group by at least two letters. We call that the two-letter differential. The reason is that if an error is made in transmission, the liklihood of making two errors in the same group is not nearly as great as making a single error, and their methods of correcting automatically a group if it has a single error in it. Now, code books and codes are made suited to all kinds of business. They are specialized or generalized, like a shipping code, or a code for the automotive industry, and so on. The next one is the highly specialized code. You know, there are certain people who believe firmly and implicitly in the power of healing by suggestion and

and what not, and here is a picture of a code book put out by a gentleman who was a professional man in that field. You'll notice that the purpose of it was, of course, that if you went on a trip and you wanted to consult your practitioner you could send him a message and tell him what you thought you were suffering from. Of course, you thought you were suffering from this, that or the other thing. It was English and French, and you would simply represent your illness, or alleged illness, by code group. 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 differed by at least three letters each, and the reason, of course, is that it would be a pretty serious thing if you sent a message saying that you were suffering from coma but got treated 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 question of large scale reproduction of code boods. On compromise, I don't think they thought too much about the possibilities of solving code, but early in 1916 the Germans began to use Field Code, and the Allies soon followed suit. I had slides to show you pictures of pages of the code books of the various belligerants, but I have exhibits and those who would like to see what they were like are welcome to come up after this talk and examine them. The only one that I really would like to show is one that will give you a picture of American inadequacy in World War I for code work. This is authentic - I didn't make it up - I found it in the records. It's a code gotten out by the 52nd Infantry Brigade dated 17 April 1918 and it is what we called the baseball code. If you wanted to say kill, strike out, base on ball, hit by pitch ball, and so forth - very elementary.

Now I am coming to a very interesting example of World War I period, a cipher message which was taken from a German spy in the United States, and he was sentenced to death. The message was found on his person, and that's a picture of the code groups, and after some weeks it was deciphered by the code solving organizations in Washington, MI-8, as it was called. Here is the German text, and this is what it said, "The Imperial Consular officials of the Republic of Mexico strictly secret the bearer of this is a subject of the Empire and travels as a Russian under the name of Pavlo Baverte. He is a German agent." And so forth. His sentence was commuted to life imprisonment, and he was out in a year. Here is a message which is probably the most famous message in cryptanalytic history to date. This is the message which brought the United States into World War I on the side of Britain. In 1915-16 it was very much catch-as-catch-can as to which side the Americans were going to join. Our British friends and later allies did certain things that we didn't like, and there was a good deal of talk about it, but this message, solved by the British, brought us in. It was the straw that broke the camel's back. It is known as the Zimmerman telegram. It went to the German legation in Mexico City from Count Von Bernstadt, the German ambassador in Washington. The method of solution I won't to into. The handling of the case shows how astute diplomatically our friends were in bringing the Americans in by means of that message. Here is the translation of the thing. It was important because they were going to resume the unrestricted submarine warfare and this, dealing with a deal with Mexico, was the straw that broke the camel's back. People in the Middle West were very luke warm toward the idea of war, but when they began talking about giving back to Mexico, Texas, New Mexico and Arizona, that was something else again. So

we got into the war. Here is an example of another type of code we solved, this time by the United States group in Washington, a sabotage message talking about who was reliable and what they should do, and that figured in a long, long trial before the ___?___ Claims Commission in which the Germans were charged with certain acts of sabotage, notably the Kingsman fire and the Black Tom explosion, and it resulted in a decision in favor of the United States, claimants, some $40,000,000. This is a message in secret ink that figured in the Black Tom Case, a page from the Bluebook Magazine in which there was secret ink writing inscribing on the pages of one story.

Now I come to a case in which I was involved. In 1915, no, 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 it would draw out British troops from the Western front, and these Hindus were negotiating for the purchase of arms and ammunition in the United States and sending it over to India. Here is one page of a long, seven or eight page message that was intercepted between the Hindu in the United States and his chief in Switzerland. The message consisted of groups of figures which were interspersed with words. I recognised immediately that this represented the page of a book, this the line number and this the letter in the line, and all I needed was the book, but, of course, the message itself didn't say what the book was, so I had to go ahead and try to solve it. This was solved, and I'll show you very briefly the method. As I said, there were words, plain text words, interspersed, and I would make a guess. Here, for example "Form day, something, with, something." I assumed that this would be the word "committee," and that meant that on page 65, the fourth line, the second letter in the line was a C.

Well, the third happened to be O, and the fourth an M and the fifth an M, but the sixth was not indicated, and so on. Well, by substituting some of these guesses in their proper positions and tabulations of this sort, I found that this word committee came from the word communication on page 65. Then this word is "Attention," and so on. And by working back and forth, building up the pages in the book and building up the message - one helped the other - and I finally came to the conclusion that it was a book dealing with the history of German political philosophy or what not, and I hunted and hunted and hunted. I finally found the book, all right. It was Price Collier's Germany and the Germans. This message figured in a trial out 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 himself in bad 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 proceedings shot the Hindu who had turned state's evidence, whereupon the United States Marshall, a great big fellow six feet 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 dramatically.

I'm going to pass that one up. That figured in the oil scandal in the days of 1924. I was government witness in that case, solved the messages and showed some of the facts that lead to Mr. Fall's going to prison, the Secretary of the Interior.

The rum runners in those days 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 number for that group into another book and

then adding a constant value to those numbers, and this was the message. All I had to do was to find the books.

There were some interesting things, working on the job we would get messages from various government agencies to solve. Here is one that came to the White House and sent to Secret Service. It was addressed to the President and had this stuck in and after this figure and all it was was if you read it backwards and alternate letters it says "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 effect of the invention and distribution of radio and its effect 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 came inventions of cryptographic devices and machines. The brief history of these will therefore be useful. That is a picture of the earliest cryptographic device on record, except for the spitalas. This is taken from a book by an Italian named Alberti published in 1470 and is just a cipher wheel, one revolving concentrically upon the other so that you could change the relationship of the alphabet. This wheel is represented also in the Porta book, and, by the way, I have a copy of the original edition of Porta with the cipher wheel 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.

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 the the Chief Signal Officer of the Army at that time, Major Myer. It was the same

thing used by the United States Army 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, so every once in a while a thing that is as old as the hills gets through the patent office. Now we come to a device, I mentioned 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 is interesting. Here is a picture of a device invented by Sir Charles Wheatstone, the eminent British mathematician, physicist and electrical engineer. The principle is a little different from the preceding one. This had an alphabet of 27 characters and an inner alphabet of 26, with an eccentric motion depending upon the letters that you were actually going to encipher. With this hand, you see, you go around this way, and the fourth revolution, for example, if the letter H is represented by E on the next revolution H would be represented by the next letters, which happens to be a victor. Now the British took that basic invention, and you'll notice that the first slide had the alphabet on the outside in normal order. What they did was to add the idea of a mixed alphabet on the outside. They changed the form of the device itself, but the cryptographic principle is identical. They had a great many of these manufactured. I was at that time working at the Riverbank Laboratories, and this thing had been approved by the British, the French and the Americans in Europe. It was sent to Washington, approved there by the MI-8 people, and somebody there said, "Well, let's see that this fellow out in Chicago thinks about it, so they sent me a set of five test messages in this device. All I knew was it was based upon Wheatstone principles, and my employer came to me one day and gave me these five messages, each message 35 letters long only. He said, "I want you to solve this

thing." I said, "But I can't solve anything as short as this. 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 those, you will start work orders 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 word on which it was based was the word "cipher," and I thought, "Well, there is no way of reconstructing this." At that time I hadn't invented the principle. I later did. There was nothing to do but try to guess what this might be, by trial and error, and I tried on this basis. If a fellow was foolish enough to use a word like cipher as the basis for mixing one, he'd be likely to use an associated word for the basis for mixing the others; and I tried every word in my mind associated with the word cipher, one after the other, and it took minutes. Then finally I exhausted my efforts, and 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?" 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 comes to your mind." She said, "Shoot." I said, "Cipher." She said "Machine." That was it. In about ten minutes we had reconstructed the alphabet and solved the messages. The first message said, "This cipher is absolutely indecipherable." We sent the solution to Washington, word got to London, and when I got to 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, made

by a Major Lucius Wadsworth, who was aide to General Green of Revolutionary fame, and it bears on it - this is a very poor picture - the date 1817, while Wheatstone devised his and described in 1870. I come now to a cipher allegedly invented by a Frenchman, Bazarie, called a cipher cylinder. This consists of a shaft on which are mounted discs which can be arranged in keying order, each disc having a different alphabet on it. You line up the letters of your plain text message "Jesuis ____ ? ____, I am indecipherable," and for your cipher equivalent you can take any one of the other twenty-five horizontal lines. Looks like an excellent principle, but quite readily solvable these days. The principle, however, was not invented by Bazarie; it was invented by our own Thomas Jefferson, and there is a picture of his description of a thing called the wheel cipher, exactly the same principle. I had an interesting time with that in connection with the definitive additional checks and works being published now at Princeton. In 1915-16 a United States Army officer by the name of Hitt invented again that same principle, this time not in the form of discs, but sliding strips, you see, and this is the original model. Mrs. Hitt came to Riverbank, with this thing and said it was pretty hot stuff, and she put up a challenge message, and I solved the challenge message by hocus pocus. I thought to myself, "Well, this lady, 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 strip? Well, she might use the word 'Riverbank Laboratories.'" 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, is mixed alphabets; you can take them off and put them on in any order you please, exactly the same principle. We used that for quite a number of years

with some success. It was not produced in time, however, to be used in World War I.

This, gentlemen, is a picture of the very first SIGCOT 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, there you perforate your plain text message, here you have a keying tape passing through a transmitter, here is another keying tape, both different, their loops, their differential diameters. This one is a thousand characters in length and the other 999. You start them out at a given point, adjust the positions. Those two points won't come together again until you have enciphered 990,000 characters. A pretty good principal, but, again, on a challenge, this was after I came back, was demobilized and then back to Chicago to the Riverbank Laboratories, on a challenge, this was supposed to be absolutely indecipherable, said so in writing by a letter signed by the Director of Military Intelligence, but I was able to solve the thing without having the tapes, without knowing how long they were, or anything. There is another 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 Hebron out in California came forth in about 1922-23 with a keyboard, rotor, a comutator switch and comutator really, the current from the keyboard depressions going in this side, a fixed comutator going through a wheel here, they switched those circuits, coming out and going through a typewriter. Now that 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 positions, you see, and these are the types of rotors that he used,

pretty high security. The Navy was about to adopt these things. They had a contract for $75,000.00. God, how that hit me! I didn't even have a dollar for that sort of thing. Well, they asked me what about it, and I said, "I'll study it." I came over and I sat before this thing for about six weeks before I had a really good idea. So I went over to the chief of the section, and I said, "I think I can solve messages," and he said, "Show me." I said, "All right." He said, "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. I was getting dressed to go out; of course, it took weeks of making distributions and finding my way around. I had one assistant at the time - he was a veteran, ex-prize fighter, cauliflower ears and all, and he wasn't much help except in typing. I got to a point where if I could only solve or read - I had reduced these billions and millions of alphabets to a place where I had one line of about 18 letters. If I could solve that I would have a start, and I went home that evening from work, and I had a picture of this one line, and all I knew was that the first, the seventh, the ninth and eleventh were the same letters; the second, the twelvth, and the eighteenth were the same letters. All I knew was the letters that were identical. As I was getting dressed to go out to a party that night, fiddling with my bow tie, it suddenly dawned on me. The phrase that would fit was "The President of the United States." That was it! The next day I came in and in a couple of days I handed the Navy a solution; they killed the order. The firm went to pieces, the inventor and president of the firm wound up in San Quentin for a couple of years because he sold stock that went to about four dollars a share on the basis that a Navy order was coming through, and when the Navy order didn't come through, the stock dropped to about $2.00 a

a share, and he had picked up some of the $2.00 stuff, went to a different part of the state and sold it for $10.00. They 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, Commercial Enigma. Here are the rotors, you see, four of them here, a keyboard and the light bank. You press the keyboard, the rotors step, and they light up. You position these things according to keying letters. Now, also in Europe after that time there were other inventors. Here is a machine called the Grehowe which was held as being 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. You could have everybody in the world provided with a machine and a key and nobody else would have the same key, and so on. Well, gentlemen, the number of permutations and combinations that a given cipher system affords, like "The Bird that Sings in the Spring," have nothing to do with the case, or at least very little. It all depends upon how those permutations and combinations are basically cryptographically. Here is a picture of a Swedish machine of about the same period, keyboard, light bank, with rotors, a little different type of rotor in that case. Of course, the light bank 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 box itself from the outside, and there is a picture of the internal workings. There is the keyboard.

It's, of course, turned around, and here are the switching comutators with pins that you could put in and out effective position like on our converter M-209. These pins drive a certain lever here which drives the switching comutators which are in here, and you could also switch around the effects of the comutators. Here is the printing mechanism. This style you'll recognize as being very similar to the style in the Converter M-209. It printed on a tape.

Of course, in those days considerable thought began to be devoted to the encipherment of teletype communications, and this was, aside from that 1802 machine that I showed you, this was the first of the teletype cipher attachments, an invention of Col. Parker Hitt, who retired from the Army and joined the International Telephone-Telegraph Company and devoted himself for two or three years to producing this thing. This was finally, there's the internal mechanism. It had keying wheels which affected the bands of the teletype character. These wheels were of differential diameters. This one had 101 places, 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. That thing was put into test usage in the State Department, and they called upon the War Department to make a security evaluation. I was assigned to the job, and I had an interesting time with this. The State Department put up a series of messages. They were stamped in at a certain hour, 10:00 o'clock in the morning, let's say, and about 10:30 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

when I got up there, he said, "I'm sorry. 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, "Have you got the plain text to those messages here?" And he drew himself up closer, and he 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 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 promptly sat down on the floor. That was only 35 minutes or so after it had been received. The ITT Company burned its fingers on it, gave up the investment and never tried again. So we have the AT&T Company studying the code, the IT&T Company, and later on I'll say a word or two about the IBM Company, who also tried their hands at it and failed. The reason is that without cryptographic and cryptanalytic guidance nobody can invent a thing that is going to stand up under cryptanalytic attack.

This is Converter M-209 which we adopted, a Swedish invention. It is pretty good. The only thing we came across at that time for our field use. Here are keying wheels. Here is a valve which is affected by the keying wheels which affects a print wheel, and there is the tape. A very neat gadget but not too secure when you have two or more messages in the same set.

Now, the rest of the time I would like to devote to a brief discussion of cryptanalytic gadgetry. This is a picture of, to my knowledge, the first cryptanalytic aid, something I got up at Riverbank way back in 1916, I think it was,

a pair of glass plates with stripe and guides, grooves. You could slide these things up and down to align letters and study them for what not. I don't know why the hell I put down the United States War College. I had no relations with them, but it was nice to hand them a present, so I did that. I made it with my own hands. This was a wheel with rubber letters that I could arrange in any order I pleased. They were removable, there's another view of the thing, and here's a whole bunch of them put together for whatever purposes you want to make of them.

Now, from that early start have come a great many very interesting developments. Here is a picture of a thing dated October 30, 1934, where I sent a memorandum to Captain King and Major Akin, now Chief Signal Officer, in which I made some remarks. You can see some tear drops or maybe 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 get this across for me. If you do, we can really begin to do worth-while cryptanalytic work." Well, the plea was successful - we got it. Here's a picture of part of the contract, you see, the 12th of November. It only took a month. And here is what we were getting, and see these prices. When I think of the millions of dollars which we spent in World War II on this sort of thing, I am amazed that from such lowly beginnings should have come that great establishment. This is a room, just one long wing in our headquarters during the war, with tabulating machinery, here, just one after the other, tabulating IBM machines to do special purposes, special jobs.

You know the picture the average person has of a cryptanalyst. He's a long-hair. He has thick spectacles and whiskers and crumbs in them and so on and 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 sort of thing. Cryptanalysis of modern systems has been facilitated, if not made possible, by the use and applications of special cryptanalytic aids, including the use of high speed machinery of the type pictured here, standard, also modifications of those machines, but more importantly by the invention and development of electronics gadgetry. As I said before, the number of permutations, well, I'll get to that in just a moment. The number of permutations and combinations in itself isn't too significant. It's what they are basically. In modern cryptanalysis what you are up against is a great multiplicity of hypotheses that must be tested out, one after the other, until you find the correct one. This can be done more easily by these machines and high speed aid's combined with statistical methods. I want to show you what some of these look like. I showed you a tabulating section. Here is just one gadget which we call a machine deciphering gadget. That's a specialized thing, but you know what you try to do in a cryptanalytic practicing center is with a few people duplicate what thousands of people on the enemy side are doing. It takes thousands of people to put the messages up in the various headquarters and so on. They all flow into one place, and you can only have a certain number of people to read those messages and process them. If you have the key, then it becomes a problem of production line deciphering, so we devised special machines to take the messages and decipher them. This may not have any resemblance whatsoever to the enemy's cryptographic machine, but it's an analogue, it duplicates what their machine does, and at a high rate of speed. So that's a picture of such a device. There is a tabulator, standard tabulator with a

special attachment devised by our own engineers susceptible of what we call doing "brute force" operations, where you are trying to solve a thing on the basis of repetition. Well, if you've got millions and millions of letters, the location of those repetitions is a pretty laborious thing if you have to do it by hand, so we speeded it up. A machine of this kind will locate those repetitions, say, in one-ten thousandth 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 certain differences, and it does it automatically. These relays are set up according to certain circuitry, and you start the machine, and low and behold, it produces a printed record of the message that you get.

Here is a machine which I personally call "Rodin." Rodin was the great French Sculpturer who sculpted a piece of engineering known as The Thinker. This machine thinks. What it does is, you give it a certain number of hypotheses and you tell it, "Now, you examine these hypotheses and come up with an answer." The machine takes the first hypotheses, let's say, and it examines that, and if 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. One after the other at a high rate of speed, an electronic speed. That's only one small section of the thing.

Well, we've got left here a few minutes in which I should say something about the current employment and manner of employment. You see, I've devoted two hours to talking about the background and development and haven't said anything about the manner of employment. Well, we could discuss that under various headings, but it is obvious from the disclosures of Pearl Harbor that the manner of employment in World War II must have been very efficacious. I

wish I had the time to read you the whole of the Marshall-Dewey correspondence that this article in Time was based upon, but I think that what I am going to say next is perhaps a little bit more 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 interception of the intercept traffic has got to be transmitted most expeditiously to processing centers, and after processing the result must be promptly transmitted to the people who evaluate it from an intelligence point of view and to other intelligence personnel and in some cases where it makes a difference, a great difference - seconds perhaps - transmitted direct to operational commanders. The need for trained communications personnel, intelligence experts, radio engineers, electronics technicians, mathematicians, linguists, and 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 an idea what it takes, aside from millions and millions of dollars for equipment, both communications equipment and this type of equipment that I'll give 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 the communications intelligence processing is essentially complex and a large activity, and much of it 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 have a concentration of the personnel. There are only a limited number. You can't find people trained in this field in civil life because there is no need for an activity of cryptanalysis in commerce or industry, and when war comes we don't have a pool of trained personnel in civil life 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.

Now, I want to say a few words about the very great importance of coordination of communication intelligence activities with the general intelligence and 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 reconnaisance or other 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?" You see, you make cover for that. Another aspect of coordination between operations and communications intelligence is to be mentioned. The communications intelligence people should be carefully oriented to give optimum coverage of operations in progress. There are just so many facilities and people devoted to cryptanalytic studies in communications intelligence work. There's just so many available, and there's a great deal of traffic, an

enormous amount. Only so much of it can be processed. You've got to neglect the rest. Well, it's essential, therefore, that the cryptanalytic and communications intelligence people be abreast of the current situation so that they'll know where to put their maximum effort. Their knowledge of the tactical situation is also essential to a proper interpretation of certain materials. It's important to correlate the communications intelligence work with operations because if in exuberance our aircraft knock out radio stations, the very success of that operation has repercussions upon communications intelligence. You see, knocking those out makes unavailable to us a lot of traffic, so that has to be coordinated. There is another reason for being very careful to coordinate, and that is that these code systems and cipher systems are usually world-wide or area-wide in distribution, and if you don't coordinate your operations with your CI so as to cover up your source of information, there may be suspicions of compromise which would have far-reaching consequences. You see, a commander who gets some of this stuff and seeks a minor advantage by using it in one locality, may deprive other commanders in other areas of much greater advantage if you don't compromise the source of information. So while knowledge and experience point to the necessity of exploiting every possible advantage that the situation affords when you get this stuff, and the temptation is, of course, very great in the heat of battle 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 possible compromise of the source must always be borne in mind and the danger weighed

against 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 right here. I welcomes you to examine the exhibits and perhaps if I can answer a question while you are doing it, I will be glad to do that. Thank you very much for your courtesy and your attention.