Obsolete pages

SECOND PERIOD

COMMUNICATIONS SECURITY

Gentlemen, this period will be devoted to the subject of communications security, how it can be established and maintained.

Three or four years ago I gave a talk before the student officers of another Service School on this subject. About that time there was being hammered into our ears over the radio in Washington a slogan concerned with automobile traffic safety rules. The slogan was: "Don't learn your traffic laws by accident." I thought the slogan useful as a title for my talk but I modified it a little-- Don't learn your COMSEC laws by accident. I began my talk on that occasion, as on this one, by reading the Webster Dictionary definition of the word "accident". I know, of course, that this group here today is not directly concerned with COMSEC duties but as potential future commanders of fighting units the definition of the word "accident" should be of interest in connection with what will be said in a moment or two, so I will read Webster's definition if you will bear with me.

> "Accident: Literally a befalling; an event which takes place without one's foresight or expectation; an undesigned, sudden and unexpected event, hence, often an undesigned or unforeseen occurrence of an afflictive or unfortunate character; a mishap resulting in injury to a person or damage to a thing; a casualty, as to die by accident."

Having defined the word, I will not proceed to make the definition relevant to this talk by reminding you of a minor but nevertheless quite would leave Buka for Balalle. They also knew what his air escort would be, and so on. You can see, therefore, that it was relatively easy to bring about the "accident" Yamamoto was to suffer. Our top Commander-in-Chief and his party, on the other hand, journeyed with safety because the communications connected with his various trips were secure. The Japanese Commander-in-Chief journeyed in peril because his communications were insecure. His death was no accident in the dictionary sense of that word--it was brought about. The Yamamoto incident later gave rise to a somewhat amusing exchange of TOP SECRET telegrams between Tokyo and Washington. After the war was all over certain telegrams turned up in the Forrestal Diaries, from which I will now read (Page 86):

> The formal surrender took place on the deck of the U.S.S. Missouri off Tokyo Bay on September 2nd. The mood of sudden relief from long and breaking tension is exemplified by an amusing exchange a few days later of urgent TOP SECRET telegrams which Forrestal put into his diary. In the enthusiasm of victory someone let out the story of how in 1943 Admiral Yamamoto, the Japanese Naval Commander-in-Chief and architect to the Pearl Harbor attack had been intercepted and shot down in flames as a result of the American ability to read the Japanese codes. It was the first public revelation of the work of the cryptanalytic division and it brought an anguished cable from the intelligence unit already engaged at Yokohama in the interrogation of Japanese Naval officers.

amazing achievements of American intelligence, the enemy had succeeded in breaking the principal code then in use by the Japanese Navy. In this way the enemy was able to learn of our intentions almost as quickly as we had determined them ourselves."

And then in the last chapter, entitled "Analysis of the Defeat", Captain Fuchida says:

"The distinguished American Naval historian, Professor Samuel E. Morison, characterizes the victory of the United States forces at Midway as 'a victory of intelligence'. In this judgment, this author fully concurs for it is beyond the slightest possibility of doubt that the advance discovery of the Japanese plan to attack was the foremost single and immediate cause of Japanese defeat. Viewed from the Japanese side, this success of the enemy's intelligence translates itself into a failure on our part--a failure to take adequate precautions regarding the secrecy of our plan. Had the secret of our intent to invade Midway been concealed with the same thoroughness as the plan to attack Pearl Harbor, the outcome of this battle might well have been different."

Lest you infer that our side didn't meet with any COMSEC accidents, let me say that we had plenty of them. These were not attributable, however, to serious weaknesses in our COMSEC devices, machines and procedures, but principally to human failure to follow the rules implicitly or to weaknesses in the COMSEC devices, machines and procedures of some of our Allies. Take for instance the heavy losses that the United States Army Air Corps sustained in their air strikes on the Ploesti oil fields in southeastern Europe. We lost several hundred big bombers within a relatively short time because of weaknesses in Russian communications, weaknesses we didn't suspect. Those big raids constituted field days for the German fighter commands, because merely by traffic analysis, and simple traffic analysis at that, they knew exactly when and where our bombers were headed. We found what the trouble was, but sad to say, it was too late. This incident leads me to say that the COMSEC weaknesses of Allies even today lead to a rather serious illness which afflicts our high level authorities from time to time. I've given the disease a name--cryptologic schizophrenia. It develops when one is torn between an overwhelming desire to continue to read friendly traffic by cryptanalytic operations and the almost certain knowledge that the same traffic is also being read by others and should be made secure against the common enemy. What to do? Thus far, no real psychiatric or psychoanalytic cure has been found for the illness. The powers that be have decreed that the illness will be avoided by the very simple ruling that COMSEC interests will always over-ride COMINT wishes.

It is hardly necessary to tell you that with the advances made in the invention and development of all the many instrumentalities of warfare, including communication systems, the so-called "pencil-and-paper ciphers", the hand-operated small cipher devices, the codes and code systems of former days, even during and throughout the period of World War I, appeared to be and were indeed completely inadequate. Military, naval, air, and diplomatic cryptographic communications had to be speeded up; and obviously the road along which crypto-engineering and development had to travel was that which by mechanical or electro-mechanical apparatus for crypto-communications would at least begin to approach the ever-increasing speed of electrical communications in general, including both wire and radio systems. The need to invent, develop and field test practical crypto-apparatus became obvious even before World War I had ended. It is a truism that as mechanization and automation progresses in our civilization, parallel progress has to follow in communications systems and instrumentalities. And let me remind you that the impetus for devising and developing faster means for crypto-communication came not only from the need for speedier crypto-apparatus to match the ever-increasing speed of electrical communications, but also--and perhaps more importantly--from the need for much greater security in those communications, which were now largely by radio and therefore susceptible of interception and study by the enemy.

A brief history of the invention and development of crypto-devices, crypto-machinery, and crypto-apparatus will therefore be of some interest. We will proceed now with the slides.

First, I show you the earliest cipher device known to history. This slide is a picture of the cipher disk taken from Alberti, who wrote a treatise on ciphers in Rome about 1470. It is the oldest tract on cryptography that the world possesses.

The next slide shows a similar sort of wheel which appeared many years later in Porta's book, which I showed you after the first period, recommends the use of a similar device, if you call it a device.

The Myer disk is next, patented in November 1865 by the first Chief Signal Officer of the United States Army, and the next slide pictures the U.S. Army Cipher Disk, (1914-18), used in the period of World War I. It follows exactly the same principle that Alberti used. It seems to have taken a long time, doesn't it, for the Signal Corps to get caught up with Alberti?

Now I know it takes a long time to nurse a patent through the United States Patent Office, but Alberti's device was finally patented in 1924. Here the device patented.

Next is a picture of the Wheatstone Cryptograph, the first real improvement on Alberti's device. I have the only copy in the United States, maybe in the world and I've brought it with me. Wheatstone interested himself in cryptography and he invented his device in the latter part of the decade 1870. It is not just a simple cipher disk. Of course, as you see, it consists of the ordinary alphabet on the outside and an alphabet on the inside and the latter is a mixed sequence; but there is one additional important feature--the alphabet on the outside contains 27 places, the one on the inside, 26. There is a differential gear in the device so that as you encipher a message and turn the big or "minute" hand to the letters to the plain text, the small or "hour" hand advances one step for each complete revolution of the "minute" hand, just as in a clock. At the close of this period those of you who would like to examine the device may do so.

Now in 1917, in casting about for a field cipher device for use on the Western front, our British allies resuscitated Charles Wheatstone's principle, embodied it in a little different mechanical form, and made thousands of them. Here is one of them and here is an American copy of the British model. It has a 27-unit alphabet on the outside and a 26-unit one on the inside; but there is now one additional and very important feature. You will notice that both alphabets are now disarranged for mixed sequences, whereas before, in the original Wheatstone, only the inner alphabet was mixed. Now I suppose you would be interested in a story about this thing. It was decided to adopt the device for use on the Western front after it was approved by the cryptologic authorities at the GHQ's of each if the principal allies, British, French and American. A copy of the device was then sent to Washington and the head of the American cryptologic agency in Washington approved it. At that time I was teaching school--remember that photograph I showed you of the school for instruction in cryptography and cryptanalysis? Somebody said why not send it out to Riverbank and see what they have to say. So they sent out a set of test messages and one day Colonel Fabyan came walking into my office, handed me a piece of paper, and said: "These are in Wheatstone, I think. Solve them". I took one look and saw there were five messages, just five, and they were all very short--each had about 35 letters. I said, "Oh! It's silly to try this. I have other fish to fry." The Colonel said, looking hard at me, "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 of it. If you would like to continue receiving those bits of paper, you'll start working on these messages right away." I said: "Yes, Sir!" Well, I started in and by means too involved at the moment to tell you, I felt that the outer alphabet, in this case the mixed sequence, had been derived from a rectangle based on a keyword, and it appeared to me, from the distribution of the sequence of about half-dozen letters I'd reconstructed, that the keyword for mixing the sequence might have been the word "cipher". At that time I'd not discovered what later turned out to be an important new principle in cryptanalysis whereby having the one alphabetic sequence the other could readily be found by a process of conversion. So not having this principle I was at a loss as to what to do, except try to guess what the other alphabetic sequence might have been based upon. I sat back and thought: Now, if a chap is simple-minded enough to use as a keyword a word connected with the subject for mixing up the letters in the one alphabet, he would probably use a word associated in his mind with that word as the key for disarranging the inner alphabet. So I tried every word that was associated in my mind with the word "cipher" -- "cipher alphabet", "cipher device", "cipher polyalphabet", and so on, one after the other. This took a little time, because with each guess I had to derive the mixed sequence and try it out on the messages. Finally, I came to the end of my rope and said to the then new Mrs. Friedman: "Elizebeth, I want you to stop what you are doing and do something for me. Now make yourself comfortable," --whereupon she took out her lipstick and made a few passes with it. I said: "Now I'm going to say a word to you and I want you to come back with the very first word that comes to your mind. Are you ready?" She said: "Yes". I said:

"Cipher", she said: "Machine". Machine was the word. You see my male mind didn't regard this thing as a machine at all; but the female mind is, as you know, a thing apart. Well, the messages were deciphered in a hurry by me. The first message, by the way, read: "This cipher is absolutely indecipherable." We sent the solution to Washington, where on arrival there was a to-do; there was also a to-do in Europe. I wrote up the solution and Colonel Fabyan sent it to Washington so that when I got to GHQ, three or four months later, I wasn't very popular with our British friends, because a mere amateur had found something their experts had overlooked. Moreover, what was worse, they had to withdraw the device from users, and thousands of them had been issued.

Now I show you a poor picture of a very similar device, bearing on its face the engraved date 1817. It was invented by a Decius Wadsworth, at that time the Chief Ordnance Officer of the United States Army. The device itself is still in operative condition and is housed in the museum of a little hamlet in Connecticut. I borrowed it for a short time from the curator and unfortunately didn't have a good picture made. Decius Wadsworth anticipated Sir Charles Wheatstone's invention by a good many years.

Next comes the cipher cylinder. A French Army reserve officer, Commandant Bazeries tried to interest the French Army in a device which he called the "Cryptographe Cylindrique", or cylindrical cipher. His device consisted of a series of disks with a central hole so that they can be mounted upon the shaft; each disk bears an alphabet (of 25 letters in this case) in disarranged device; here is the second page. You see his calculations, giving you at the bottom the number of permutations that his particular device affords--a whale of a large number because Jefferson proposed a set of 36 disks.

In studying the degree of security provided by the M-94 I soon came to the conclusion that security would be much increased by the use of variable or changeable alphabets so I had a gadget built on which we could mount slips of paper and fasten them and then change the alphabet as often as was felt necessary. That was the beginning of our variant forms of the strip cipher devices used by the Armed Forces, and later by the State Department and the Treasury Department. Here's the original version of the strip cipher device that used changeable alphabets. Both the Army and the Navy cryptographic divisions proceeded to improve on the system, both as to the form of the device itself as well as the ways of making the strips in quantity. Here is a picture of the final Army type of strip cipher device. You see the channels in which the alphabet strips were inserted according to the daily key, and according to the particular crypto-net to which your command belonged. I mean by this that not all the traffic would be in the same set-up of strips or even used the same strips. The idea was to cut down the amount of interceptible traffic in the same key.

Next we come to a machine called the Kryha, invented by a German, in about the year 1925. The Kryha was the last word in the way of mechanical cryptographs at the time, and Mr. Kryha tried to interest various governments in his machine. I think I should explain it for those who have never seen it.

for it. When there are several messages in depth the solution becomes even easier. And the bad part about this from the standpoint of COMSEC is that with a solution by depth the recovery of the key--the whole setting of the machine--is not at all difficult. Then, of course, the solution of all other messages enciphered by the same arrangement of keying elements is an easy matter.

The cipher machine now used by the Marine Corps is a double M-209 machine and it is an improvement security-wise over the single M-209, but I'm sorry to say that it too has the same weakness of an easy solution when two or more messages are in depth.

for it. When there are several messages in depth the solution becomes even easier. And the bad part about this from the standpoint of COMSEC is that with a solution by depth the recovery of the key--the whole setting of the machine--is not at all difficult. Then, of course, the solution of all other messages enciphered by the same arrangement of keying elements is an easy matter.

~~The cipher machine now used by the Marine Corps is a double M-2Ø9 machine and it is an improvement security-wise over the single M-2Ø9, but I'm sorry to say that it too has the same weakness of an easy solution when two or more messages are in depth.~~

was being built until the final model was completed and ready to be delivered to us. After a quick look I asked the Chief of the Division to put up some messages for us himself, so that there would be no question as to whether I or some of my assistants had gotten any illegitimate help. Well, he enciphered a few messages and I brought him back the answer to the first one in 2Ø minutes, and the answer to the rest of them in 35 minutes. The whole development represented a loss of time and energy and moreover, it wasted what little money we had for such business. I almost forgot to tell you. This was very amusing. When we finally went to pick up the machine, I talked to Colonel So and So, who told me with some pride that his machine was all mechanical and that there was nothing in the way of an electrical machine or operation that you couldn't do mechanically. I asked: "Colonel, can you light a room mechanically?" To which he replied: "You've said enough--get out. That's the machine, take it with you." The power source, which in the model was laughable, he planned to motorize. But I do not regret to say that the crypto-principle was very faulty--it didn't take very much time as I indicated to read the messages--and the laboratories development came to an ignominious end. But I'm glad to say that was an unusual Colonel; those who came later were much more inclined to take advice from persons experienced in the field of cryptology.

Now we come to a development which is of deep interest to us. Here's a picture of a gentleman named Boris C. W. Hagelin, a Swedish engineer, who was responsible for the invention and development of one of the machines that we used in World War II in great quantities. Mr. Hagelin and I became very good friends after the war. I was opposed to taking on Hagelin's device in 1940-41 for reasons that will presently become clear. It wasn't a case of NIH--"not invented here"; but the decision to have them made for and used by the United States Army was a decision on a level higher than my own, and I simply accepted it. It turned out, I think, that my superiors were right, for we at least had something, whereas if they'd listened to me we wouldn't have.

Now just a bit about Mr. Hagelin. He did what I best describe as a hysteron-proteron. That's a four-bit word, not four bit in the sense that you use it for digital computers but in the everyday sense; it's a four-bit word from the Greek meaning to do a thing "ass-backwards". I mean that usually you go into cryptographic work and then you have a nervous breakdown. He did it the other way. He had a nervous breakdown and while he was recovering he invented this machine--and he made several million U.S. dollars. That's why I say he did a hysteron-proteron.

Here's a picture of Hagelin's very first machine and I've brought his very first model, in fact, number one, a present from Mr. Hagelin to me for my museum and, when I've passed on, for the museum of the United States on Constitution Avenue in Washington. It's a very interesting device. From that prototype we built in America for World War II this six-wheel Hagelin machine with American inch-specifications and with American tools rather than European millimeter specifications and tools, the astonishing number of over one hundred and ten thousand of these machines. They were manufactured by the

Smith-Corona Typewriter Company, in Groton, New York, and are undoubtedly known to many of you as Converter M-209. But the M-209 had a serious, a very serious weakness, you know; among other things it had no printing mechanism; but I'm not really concerned with that. I'm concerned with its cryptographic deficiences, about which I'll tell you presently. This is a picture of one of the Hagelin machines as modified by some of our GI's in Italy. You know how resourceful GI's can be; they scrounged parts here and there and they improved their machine to make it a printing model. See, here is the keyboard, and here's the printing mechanism. Inside the cover is a cartoon of a couple of GI's getting ready to test a home-made still for the production of you-know-what. The caption at the bottom of the cartoon says: "Yes, but will the God damned thing work?"

Now, Mr. Hagelin proceeded to improve his machine and this is a side view of one of his latest models--the CX-52. It prints not only the plain text but also the cipher text. It has a ciphering mechanism that represents a very great advance. Now the wheels, instead of being permanently fixed upon the shaft, ~~can be rearranged in 720 different ways and are demountable~~ are demountable and can be rearranged in 720 different ways. The stepping motion for these wheels is complicated and as of this moment we do not know

[redacted]

of all, I will show you how a message which has been enciphered by an intelligible

EO 3.3 (h) (2)
PL 86-36/50 USC 3605

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

[redacted] It will take about a dozen or more messages in this case, and it won't be a particularly easy job at that.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

We are going to proceed with a quick review of the development of what we call electrical rotor machines. The first one I show--a product of the company which was headed by Mr. Hagelin when his father bought out a Swedish cryptograph company in Stockholm--was not a real rotor device of the type we know today but I don't want to go into details. I merely want to show the device. The device is now connected with an electric typewriter, so that instead of writing down letters one by one you can make with speed a printed record. Up to that time devices of this sort were only of the indicator-type of machine. You press a key and the light would light, you would have to write down the letter flashed on the light bank and wheels would step.

The next slide shows a better picture of this machine controlling a Remington electric typewriter. The next step, of course, was made by Mr. Hagelin when he made the printing mechanism an integral part of the machine itself. Here is the keyboard, the printing mechanism, in here, and now the whole assembly is very much smaller and more compact.

Now I show a German machine known as the Engima, a commercial model, invented and put on the market in about 1923-24. It comprised a keyboard, a light bank, a set of electric wheels called rotors. In this case the enciphering-deciphering circuitry is more complicated; it goes from a key of the keyboard, and through these rotors and back through them, to a bank of lights whereon it lights a lamp. This reversing wheel is a very important feature of this machine. Now everytime you press a key, one of these rotors steps forward and the stepping of the rotors is such that the machine had a very short cycle as such things go, about 26^3; it was a little less than that on account of certain factors into which it isn't necessary to go. Now, I'm not going to take the various developments of that machine through World War II. At the moment, I want to go directly to the American developments in these rotor machines. For this purpose I show a picture of a man named Edward H. Hebern, a Californian, who independently, I think, thought of rotor machines. I asked Mr. Hebern one day how he happened to get started on such work and he said, "well, you see I was in jail"; I said: "In jail, what for?" He said, "Horse thievery." I asked him: "Were you guilty?", whereupon he said: "The jury thought so." It was while he was in jail, then, that Mr. Hebern conceived the idea of a cipher machine. Here is his very first model, built presumably after he got out of jail. It has a keyboard, a left-hand stator, that is, a ring of 26 stationery 26 contacts, arranged in a circular fashion; a rotor of 26-points, and an exit stator of 26 contacts on this side. You press a key and a lamp lights. Just one rotor was in his first model, which he built in 1922 or 1923 for the Klu Klux Klan. Here is the first printing model made by Mr. Hebern--still a one-wheel or one-rotor machine--with a keyboard and now an electric typewriter connected thereto. I have among my treasures in my library a brochure which went with this thing and it's a very curious document. Now, one interesting thing about Mr. Hebern's rotors is worth noting. He didn't have absolutely fixed wiring--these are detachable wires, and this next slide shows 13 leads on one side and 13 on the other, showing that he conceived at an early date the idea of variable connections for rotors. This is an extremely important feature of any kind of a rotor machine. This shows his next step. Now we have three rotors in cascade. This, too, was a very important step--the cascading effect was a great advance in connection with rotors. Here I show his next development--a 5-rotor machine. Here are the rotors removed from the machine to show you what they look like. They were still variable--you could take wires and rearrange them; there was a keyboard and still a light bank. There is an interesting story connected with that model. The Navy Department was very much interested in cipher machines for these were things they absolutely had to have for speedier communications from Washington to the Fleet Commanders and, of course, for intra-fleet communications. The Navy was very anxious to have a suitable machine and the Hebern machine seemed like a good bet. This was the machine they thought they would like to buy. They got an appropriation for the purpose, a large sum of money for those days, $75,ØØØ, and they proceeded then to negotiate with Mr. Hebern. At that time, in the code and cipher section, there was a cryptanalyst of parts, who happened to be a lady, and she was quite able. She was the one who got Mr. Hebern ready to move from a three-wheel to a five-wheel machine; and when he finished the development of the latter and he seemed to be on the point of getting a good-sized order from the Navy Department, he offered and she accepted an attractive offer to come and join the Hebern firm in California. I apologize for introducing the first person singular so much, but the fact is that I became interested in this machine as a result of a personal inquiry from the President of the Naval Board that had been assigned to study the machine and I persuaded the War Department to purchase one of them from Mr. Hebern. I sat and studied it for some weeks--three or four weeks. The whole of my outfit consisted of myself and a World War I veteran, an ex-prize fighter, with crossed-eyes and cauliflower ears; the only thing he could do was to type, and I may say that he could copy from draft letters or cipher text with absolute accuracy, but that's all he could do. The rest of it was up to me. As I say, I studied the Hebern machine until an idea for a solution came to me, whereupon I went over to the Navy Section, which was then in charge of a Lt. Struble, who now is Vice Admiral Struble, Retired, with an enviable service record. I said to Struble, "Lieutenant, I don't think that machine is quite as safe as you think it is." He said: "Oh, you're crazy!" I said: "Does this mean that you challenge me?" whereupon he said, "Yes." So I said: "I accept." He asked: "Well, what do you want in the way of messages?" And I said: "How about ten messages put up on your machine?" He gave me the ten messages and with some typing help from that ex-prize fighter I worked on them until I got to a place one day, at the close of business, when I had reduced the text of one of the messages to monoalphabetic terms. By this I mean that I'd reduced it to its simplest terms: I knew that in the first line of the text of that message the had the text of the first message which I was able to solve in that thing. And by the way, you will forgive me if I say, the methods that were devised at that time for the solution of rotor machines and rotors in cascade are practically the same today as they were over twenty-five years ago. The Navy decided that the Hebern principle was still a good one and went ahead with Mr. Hebern after he got out of prison, and Hebern built some more machines for them. Here's a picture of the last machine built for them. ~~Here is a picture of the last~~

~~machine~~
As regards the purely mechanical factors the Navy wasn't satisfied with the power drive and the hand drive; but the crypto-principles seemed satisfactory, but the cautious Navy asked the Army's help in evaluating the security afforded by the machine. It had a different kind of stepping motion in which the Navy had put a great deal of faith. It was a good motion but nevertheless it had weaknesses that we found we could exploit, and we solved challenge messages put up by the Navy. Here's a picture of the last machine that Hebern built for the Navy. He wanted to get paid for it but there was a hitch. When it was pointed out to him that the machine didn't work, he said: "Show me where it says in the contract it has to work", and when they couldn't he was paid off. The Navy then decided that they had had enough of Hebern and went into research and development themselves. They had a laboratory established in the Navy Yard, with a very able young man named Seiler, now a Captain in the Navy, who did some excellent developmental work. Years later the Hebern heirs brought suit in the United States Court of Claims against the United States for $50,000,000, believe

difficult for the Army and the Navy to have any inter-communication at all. The only thing that we had was a disreputable hand-operated cipher using pencil and paper, which had been adopted way back in 1930 by direction of the Chief of Staff of the Army and the Chief of Naval Operations, and that's all there was. The strip cipher device could have been adopted for joint communications but wasn't. Fortunately, the ECM-SIGABA came just in goo time and was used with great satisfaction on both sides, I am very happy to say. I might add in closing that incident by saying that, to the best of my knowledge, this is the only gadget that was withheld from our British Allies. Although they knew that we had a machine of this character and although we knew their type of machine, with which neither they nor we were at all happy, it was our policy on the highest level of the Army and Navy, to withhold this from the British. There was a struggle for several years on this point until the recalcitrant people high up in both services began to see the light. The trouble was that when the technicians assured them that messages put up by this machine couldn't be read without having the rotors and key list--that we ourselves, in Army as well as Navy, had tried very hard to do so and failed--they just wouldn't believe it. One reason is, of course they were daily getting the decrypts that were being produced from German, Italian and Japanese messages and they just didn't feel like taking any chances. "How could the technicians be so sure as they say they are?" they asked over and over again. I don't know how many millions of dollars were spent needlessly in establishing means for inter-communication with the British. By this I mean that we had to make an adaptor for this machine so that it could inter-communicate with the British TYPEX and the British had to make an adaptor for their machine to inter-communicate with the ECM-SIGABA. It was a wholly unnecessary expense, I think, but by the end of 1953 we were able to convince the authorities that it would be all right and finally the British were allowed to have our machines until they could complete their developments and be on their own. I think even at the present time they still have some of our machines. I can explain the basic principle of the machine. Here are the essential elements in the machine: a set of five rotors here, and another set of five here, making a set of ten altogether. These rotors are all interchangeable, so you see that to begin with there can be a great number of permutations from a primary set of ten rotors. It's greater than 1Ø! because the rotors can be inserted right-side up or upside down. Now there are four inputs in this row of rotors and their output goes to control the stepping of the five cryptographic rotors, so that the stepping of these rotors is very erratic according to the output of the control rotors. Here is another set of rotors, five small ones, which are used to permute the output of the control rotors.

We know of no case of solution of this system at all throughout the war. There was one possible compromise and it raised quite a storm at the time. The 28th Division bivouacked for the night in a small city in France and the vehicle containing the cryptomaterial and the SIGABAs was stationed in front of the place where the Signal Officer and his entourage were quartered for the night. Unfortunately no guard was posted to safeguard the van. In the morning that vehicle was missing. Warning messages were sent instantly to Washington and there was a great to-do. The Army set up blockades on all the roads, the idea being to make sure that the truck wasn't being carried off by some German outfit, but nothing turned up. The Engineer Corps even diverted a river, and found the cipher machines and the cryptomaterial in the river. The van had been stolen by Frenchmen purely for the vehicle; its contents were of no interest to them. The episode was one which caused the Signal Officer to be tried by court martial, as were several others. We had very strict rules indeed about safeguarding this gadget, and in mentioning this point I should say that we weren't worried by the thought that our messages could be read if the Germans would capture one. We were worried by the thought that they would learn how good it was and would copy it--thus cutting off our COMINT. One of the funny things about our not giving the machine to the British when they needed it so desperately I can hardly refrain from telling you. I mentioned the strict rules about safeguarding it--who could see the thing, who could service it, and so on and we saw to it that these rules were followed. But there came a time, in North Africa, when our maintenance men were knocked off and there was nobody to service the machines. However, there was a very skillful British Officer, an electrical engineer. He serviced and maintained our SIGABAs there for a while. When he got back to London he built a machine based upon the ECM-SIGABA principle!

Now, I want to show you next the Enigma, the cipher machine used very extensively by the German Armed Forces in World War II. This was a modification as long as possible in order to delay the enemy's real attack on the traffic enciphered by the machines.

Now let's see pictures of some of the new apparatus.

Here's a machine designated the KW-3. It is an off-line teleprinter cipher machine but it has all the conveniences of an on-line machine and eliminates some of the weaknesses of the latter. The machine generates the key as well as the indicators for messages. All the operator has to do is to type the address, punch a starting key on the machine, and then proceed to type off the plain text of the messages, whereupon a cipher tape is produced, which can be put on any teleprinter circuit for transmission. At the receiving center the operator puts the cipher tape into a reading head, the start button is pushed, the message sets up its indicator and key, and the tape produced is the plain text of the original message.

Next I show the KW-37 designed for Navy Fox or broadcast transmission. The machine which embodies a teletype printer uses an IBM card for keying purposes. So far as the communication center aboard ship is concerned, the operators don't even see the cipher--the messages arrive there in plain language. The ciphering is done elsewhere on the ship. This system is a synchronous one, meaning that both ends of the circuit are constantly and automatically kept in step; also, and related to this fact is the fact that the system is such that the intercepting enemy can't tell when a message is being transmitted and when the circuit is idling, giving what we call "link security," a very important element in communication security.