

*Transcribed from
tape of SCAMP's
lecture.*

~~TOP SECRET//SI~~

Gentlemen, this talk this afternoon is going to be devoted to the history of the invention and development of cipher devices and cipher machines. Three or four years ago I was asked to give a talk before the Communications-Electronics Division of the Air University, USAF on the subject of communications security, COMSEC. 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 begin my talk by reading from Webster's Dictionary on the word "accident". I know, of course, that this group here today is not concerned particularly with COMSEC duties of any sort except of course when you go on active duty some of you but the definition of the word accident will nevertheless 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 ^{sudden and} undesigned/~~an~~ unexpected event, hence, ^{often} an undesigned or unforeseen occurrence of an afflicted 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 now proceed by relating an interesting, minor but nevertheless quite important episode of the war of the Pacific during World War II and I will introduce the account of that episode by saying that

~~TOP SECRET//SI~~

during the war the President of the United States, Commander-in-Chief of the Army and Navy, the Chief of Staff of the United States Army, the Commander-in-Chief of the United States Fleets and certain other high officers of the Government journeyed several times half-way around the world to attend special meetings and conferences. They apparently could go with safety almost anywhere except directly over or across enemy or enemy occupied territory. They met with no accident. On the other hand, the Japanese Commander-in-Chief of the Combined Fleet, Admiral Yamamoto went on an inspection trip in April 19 43, the sequel to which may be summarized by an official Japanese/communicate Navy Department reading in part as follows

"The Commander in Chief of the Combined Fleet, Admiral Yamamoto, died an heroic death in April of this year in air combat with the enemy while directing operations from a forward position "

As is often the case, the communicate did not tell the whole truth. Yamamoto didn't die in air combat with the enemy while directing operations--he met with an accident. I don't know who first used the following terse statement but it is decidedly applicable in this case: Accidents don't happen, they are brought about. Our Navy communications intelligence people were reading the Japanese Navy high command messages. They had Yamamoto scheduled to the day, hour and minute. They knew when he would leave Truk, the time he would arrive at Bukka and leave Bukka for Trihele or Balalle. They also knew what his escort would be and so on. It was relatively easy to bring about the accident. Our top Commander-in-Chief 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 and after the war was all over these telegrams turned up in the Forrestal Diaries (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. "Yamamoto's story in this morning's paper has placed our activities in very difficult position. Have meticulously concealed our special knowledge, we now become ridiculous " They were even then questioning the Japanese officer who had been responsible for these codes and he was hinting that in the face of this disclosure he would have to commit suicide The cable continues: "This officer is giving us valuable information on Japanese cryptosystems and channels and we

do not want him or any of our other promising prospects to commit hara kari until after next week when we expect to have milked them dry." Washington answered with an operational priority TOP SECRET dispatch. "Your lineal position on the list of those who are embarrassed by the Yamamoto story is 5,692. All the people over whose dead bodies the story was going to be published have been buried. All possible schemes to localize the damage have been considered but none appears workable. Suggest that only course for you is to deny knowledge of the story and say you do not understand how such a fantastic tale could have been invented. This might keep your friend happy until suicide time next week which is about all that can be expected."

But not many years passed before the Japanese began to realize what had happened to them in the cryptologic battles of World War II. For example, Rear Admiral Nomura, the last Commander-in-Chief of the Japanese Navy said (this was on an interrogation), "Not only have we been beaten in the decisive battles of this war, but also we lost the communications war. We felt foolishly secure and failed to take adequate measures to protect our own communications on one hand, while on the other hand, we failed to succeed in breaking into the enemy's traffic. This is undoubtedly one of the major reasons for our losing battles and in turn one of the major contributing factors to our losing the war. We failed in communications." Here is another one from a Japanese Naval Officer. "Our Navy was being defeated in the battle of the radio waves. Our cards were bad and the enemy could read our hand. No wonder we could not win in this poker game."

Books recently published in Japan by former Japanese military naval officers come out quite openly with statements attributing their defeat to poor COMSEC on their part and excellent COMINT on our part. For example, there is a book on Midway, Chapter VIII:

"American Situation and Preparations If Admiral Yamamoto and his staff were vaguely disturbed by persistent bad weather and by lack of information concerning the doings of the enemy, they would have been truly dismayed had they known the actual enemy situation. Post-war American accounts make it clear that the United States Pacific Fleet knew of the Japanese plan to invade Midway even before our forces had started from home waters As a result of some 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, General Summary.

"The distinguished American Naval historian, Professor Samuel E. Morrison, characterizes the victory of the United States forces at Midway as 'a victory of intelligence'. In this judgment, this author/~~fully concurs for~~ 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."

Less^t you infer that our side didn't meet with any COMSEC accidents, let me say that we had plenty but these were not attributable to serious weaknesses in our COMSEC devices, machines and rules, but principally to human failure to follow the rules implicitly or, and this hurts me to say, to weaknesses in the COMSEC devices, machines and rules 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 because of weaknesses we didn't realize existed in Russian communications. 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. When we found out, it was too late. This incident leads me to say that the COMSEC weaknesses of our Allies and friends 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 when one knows that that traffic should be made secure against one's enemies. 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 suppressed COMINT wishes. You will understand that this problem is a rather serious one in connection with our relations with certain of our allies in NATO. I might add that U.S and U.K. physicians collaborate very closely in treating their own for the cryptologic schizophrenia and in applying remedies where possible in bolstering the COMSEC weaknesses they find in their NATO allies

Today we are going to see some slides which will mark and illustrate important milestones in the history of invention and development of cipher devices, cipher machines, cipher apparatus and, if there is time, rules for establishing and maintaining communications security.

The need for these things arose as a consequence of the constantly increasing necessity for more security in military and diplomatic communications, more especially after the advent of telegraph, cable and radio communications subject to the discoveries of the pioneers in the field of electrical invention and development. It soon became obvious that the so-called pencil and paper cipher systems and a little later the so-called hand-operated cipher devices had to give way to machines and to mechanical, mechanical-electrical, and now to electronic machines. As automation and mechanization progress in our civilization, similar progress has to follow in communications especially in military, naval and air and diplomatic communications. Now we will proceed with the slides.

First, I show you the earliest cypher device known to history This one is

the cipher disk taken from Alberti, who wrote a treatise on ciphers in Rome about

1470 It is the oldest on cryptography that the world possesses.

The next slide shows, many many years later, Porta, whose book I showed you the other day, had a similar device, if you call it a device.

November

The Myer disk is next, patented in/1865 by the first Chief Signal Officer of the United States Army

It took a long time but the Signal Corps caught up with Alberti in due course

This is the U S. Army Cipher Disk, 1914-18, exactly the same principle.

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

This is a picture of the cipher disk used by the Nazis in 1936

This is the picture of the Wheatstone device. I have the only copy in the world, I think, now. *Charles* Churchill Wheatstone interested himself in cryptography

and he invented a cipher device Here it is. It is not a simple disk It consists of an alphabet on the outside and an alphabet on the inner which is a mixed sequence but one additional important feature -- the alphabet on the outside contains 27 places, the one on the inside is 26. There is a differential gear ratio therefore in this device so that as you encipher a message and you turn the big hand to the letters to the plain text, the small hand advances one step for each complete revolution of the big hand After the talk is over, those of you who would like can come up and examine that.

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 and embodied it in a little different mechanical form. Here it is and here is a copy of it -- 27 unit alphabet on the outside and the 26 on the inside but one additional feature. You will notice that both alphabets are now disarranged for mixed sequences. 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 and was approved by the British cryptologic agency and by the French and American GHQ (by that time it had been set up and they approved of it) and the device was sent to Washington and Washington approved of it. At that time I was teaching at 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 test and one day Colonel Fabyan came walking into my office and he handed me a piece of paper and he said, "these are in Wheatstone, I think. Solve them". And I took a look and saw there were five messages, just five and they were very short--they had 35 letters each, and I said, "oh, I have other fish to fry--it's silly to try this". And he said, looking down on 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 the piece of paper, you will 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 with a keyword at the top of it or at least the rectangle was based on a keyword and it appeared to me from the distribution of the half dozen letters that I had reconstructed in that sequence of 27 that ~~the word~~ the word might have been cipher and so I set back and thought/^{now}if a chap is idiotic enough to use as a keyword a word connected with the subject for the one alphabet, he would probably use one associated in his line 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 all that sort of thing One after the other, this took a little time. Finally I came to the end of my rope and I said to the then and new Mrs. Friedman, Elizebeth, I want you to stop what you are doing and do something for me. And, I said, make yourself comfortable-- whereupon she took out her lipstick and made a few passes and I said, now I am going to say a word to you and I want you to come back to me with the very first word that comes to your mind. "Are you ready?" She said, "Yes". And I said cipher--she said, machine. Machine was the word. You see the male mind didn't regard this thing as a machine at all Well, the messages were deciphered in a hurry The first message, by the way, read. "This cipher is believed to be absolutely indecipherable " We sent the solution to Washington and there was a to-do there and also in Europe and when I got to GHQ three or four months later, I wasn't very popular with our British friends. They had to withdraw the device. Thousands of them had been manufactured

Now I show you a very poor picture of a similar device, bearing on its face the engraved date 1817. It was invented by 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 but you see Decius Wadsworth anticipated Sir Charles by a good many years.

Next comes the cypher cylinder. A Frenchman by the name of Bazeries, Commandant Bazeries, a French Army officer, Ret., tried to interest the French Army in a device which he called the "Cryptographe Cylindrique", cylindrical cryptograph. Well, it consists of a series of disks or rings rather which we mount upon the shaft --each of the rings bears an alphabet in disarranged sequence and you put your message up by rotating the rings to bring the letters of your plain text -- the first twenty in that case -- on a horizontal line whereupon for cipher text you can choose any other of the, in this case 23 rows of cipher text. This principle seemed to be a very good one and messages in it appeared to be quite safe. Here is a picture of the gentleman--he was quite a battler. He was always having letters exchanged with the French War Department but he never got anywhere and later on, after a good many years after I studied the cipher cylinder, the Bazeries cipher cylinder, I came upon a description of the cipher cylinder in the papers of Thomas Jefferson. Thomas Jefferson was the first to invent the cipher cylinder principle. There is the first page of his description

of the thing, there is the second page, you see the calculations, giving you at the bottom the number of permutations that his particular device affords

In 1915, an Army officer, Parker Hitt about whom I have told you, thought of the principle independently. He knew nothing about Bazeries His form of the device, however, was in strips, you see. This is the very, very crude first shot at it. This he gave me and it is among my treasured collection There is a better model that he made in 1915 with the paper strips mounted on wood -- wooden sliders That device was brought to the attention of the then Major Marbourgne in Washington and Major Marbourgne got up a cylindrical form of the thing Here is the first model ~~of this thing~~ of it--it is made of brass and is very heavy. And this is the final It became what we call Cypher Device, M-94.

Now, when Major Marbourgne decided to go ahead with this device, Mrs. Friedman and I were still at Riverbank and ^{this was} after I had returned from the AAF. I didn't think the device was very secure and said so whereupon he issued a challenge. I accepted the challenge He sent 25 messages. I started in with my crew to try to solve the messages by lining them all up and trying to guess the first word This was no-go. We spent a lot of time that way Ten years later I found the plain text of the messages, the test messages, amongst some old papers in the Signal Office and then I knew why I couldn't read them--

_____ . All of the rest of them were worse than that. Well, when we couldn't come up with a solution and, by the way, I must say that it wasn't Major Marbourgne himself who cooked the messages up He said to an aide, "Put up some messages in this thing" so the aide thought the best thing to do was

to make them like that He went ahead then and got the thing out and this was the M-94. We had thousands of them made They were used by the Army, the Navy, the Coast Guard, the Treasury and that's the picture of the thing I think we can stop with that.

Very soon after I came to Washington, I decided that fixed alphabet--these are engraved, of course, it would be best to have this with variable alphabets so I had a gadget built on which we could mount slips of paper and fasten them and then have the alphabet changed as often as you felt it was necessary And that was the beginning of our variant forms of strip cipher devices used by both the Army and the Navy and the Coast Guard-- an original version of the strip cipher device -- this one here seems to be

it was a difficult thing but it was finally accomplished and our devices in the Army and the Navy were made of aluminium to begin with and then we got actually into the war, they made them out of scrap. Here is one of our Army type devices with 25 channels and the alphabets which were printed up and cut apart and you could of course these strips according to the daily key with which you were provided with There is another type although it is not made we used it and this was then pulled down and we carried

This then is the same sort of thing. This is the European form of the strip cipher device except it is very much poorer. There, not only are the alphabets fixed but all you can do with them is to pick out the whole strip and they are detachable in the middle. See the number of permutations--they are not very

great there, a very insecure machine

Next we come to a machine called the Kryha, invented by a German, in about the year 1925. The Kryha was the last word at the time and Mr Kryha tried to interest various governments in his machine and I think I should explain it for those who have never seen it. Here is an alphabet and an inner alphabet. The alphabet is mounted on a disk which is rotated angularly according to the reel which is in here. The alphabets can be rearranged if you wish by sliding them into a slot. From a given starting point, you start with the first letter and then you and then you push this button and then this will slip or skip a certain number of spaces, one to seven, something like that and then you insert the next letter and give the button a push. Now there is a dissertation on the number of permutations and combinations that the Kryha machine affords. This is written by the German mathematician and all I have to say about it is that, in this case, as in many others, the number of permutations and combinations which a given machine affords, like the birds that sing in the Spring, have little to do with the case. It much depends upon just exactly how the alphabets are composed, not only their numbers. For example, to give you a simple illustration, you take a simple monoalphabetic substitution cipher. The number of alphabets that can be produced is factorial 26--that's a large, large number -- 403 quadrillions, 291,451 trillions, 126,605 billions, 635,584 millions and a few more but you know as well as I that you don't solve the monoalphabetic substitution cipher by an exhaustion method. They are There are very much simpler ways of doing it

Now there was of course a pressing need in the military and naval services for two types of machines. First the small machine for low echelon or field use and second a large machine for rear echelon high-command use. Let us take up the first of these two types and see what happened.

I show you next a device which was development model of a so-called ^{M-161} device or machine constructed by the Signal Corps Laboratories. This machine was developed sans guidance from Washington. The Director of the Laboratories at that time was a great believer in economy and he wasn't going to have Washington tell him anything about how things were to be done and when it came to developing a cipher machine, he knowing at least the alphabet or part of it decided that he was capable of inventing a cipher machine so he proceeded and the result was that we in Washington were unable even to know what was being built until ~~finally~~ the final model was completed. It was delivered to us and I asked the Chief of the Division to put up some messages himself so that there would be no question as to whether myself or some of my assistants had gotten any help. Well, he put up some messages and I brought him back the answer to the first message in 20 minutes and the answer to the rest of them in 35 minutes. The whole development was wasted energy and wasted what little money we had for such business. I almost forgot to tell you. This was very amusing. When we finally went to get the machine, pick it up, I talked to Colonel So and So and he told me that his machine was all mechanical and that there was nothing in the way of an electrical machine or electrical operation that you couldn't do mechanically.

And I said, Colonel, can you light a room and he said, you've said enough--

get out That's the machine You see the power source It's laughable. He

said, of course, that he was planning to put some sort of motor on it _____

but the cryptoprinciple was very faulty--it didn't take kvery much time as I

indicated to read the messages

Now I'm coming to a line of development which is of deep interest to us

This is a picture of Boris C W Hagelin, a Swedish engineer 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 (Mr Hagelin is a Swede) became very good friends I was opposed to taking on the Hagelin device for reasons that will become clear presently but the decision to have them made for and used by the United States Army was a decision made on a level somewhat higher than my own, and I accepted it

Now just a bit about Mr Hagelin He did what I best describe as ^{hysteron-} *protogron* corodorone--now 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" Now 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 That's ^{"hysteron-proteron"} why I say he did a hysteron corodorone

OGA

Now here is a picture of his very first machine and this by the way is a copy

of that, in fact,



Very interesting device

From that device we built in America for World War II (that's another picture of that old one) but this six-wheel Hagelin machine with American specifications and with American rather than converted

We had one hundred and ten thousand of these machines made--made by Smith Corona

Company up in Groton, New York They had a weakness, you know, among other things

they had no printing machine--no printing mechanism This thing we got in Italy after the war was over and you know how resourceful some of our G I's are and here is one which they had manufactured into a printing model--see here

is the keyboard

cartoon of a couple of G I 's

and it says here "Yes, and the God Damn thing works'!"

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

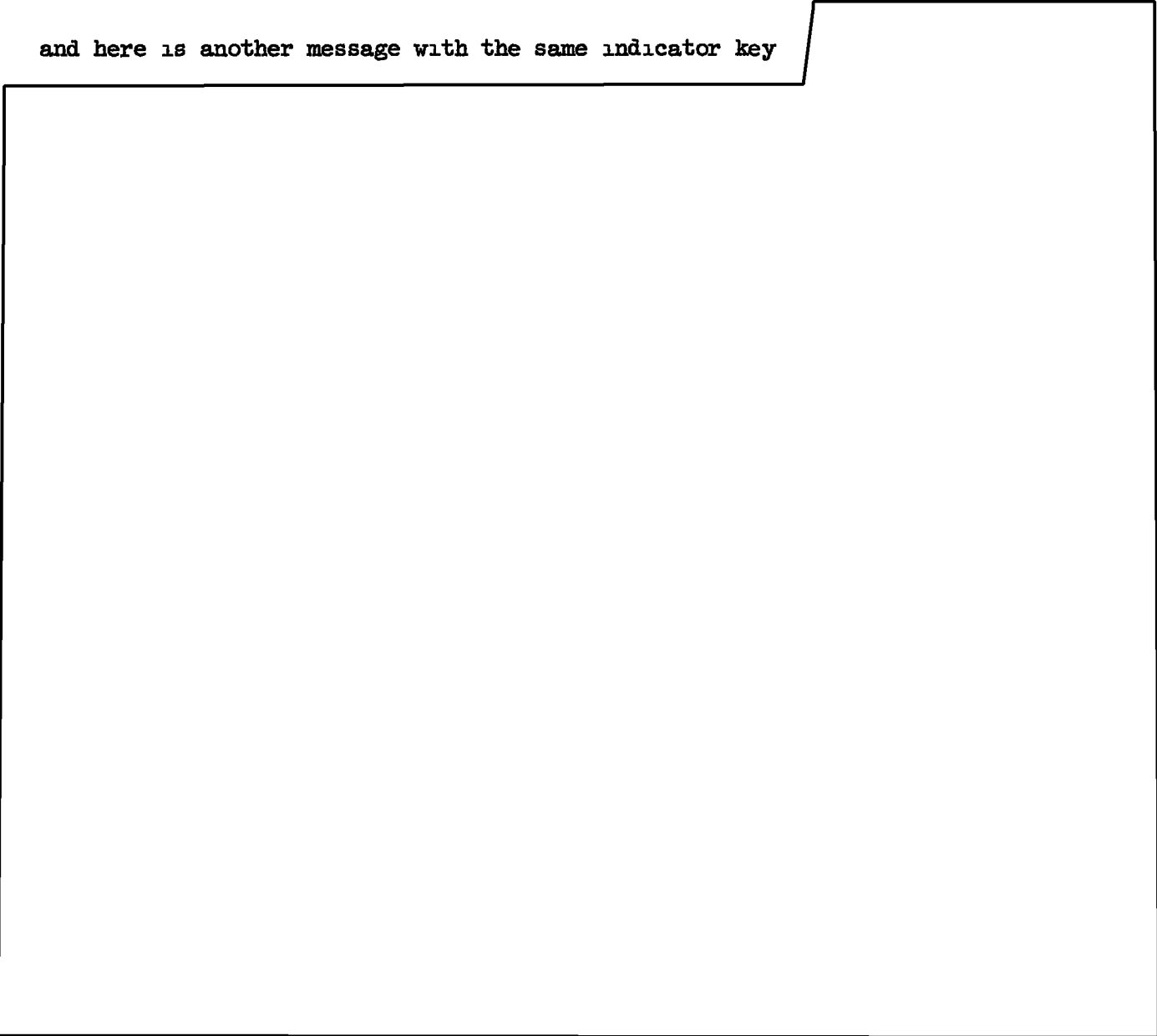
Now, Mr Hagelin proceeded to improve his machine and this is a side view of one of the late models--the CX-52 It prints not only the plain text but also the cipher text. It has a very great change Now the wheels instead of being permanently fixed upon the shaft are demountable The stepping motion for these wheels is complicated and they say as of this moment we do not know how to solve this machine but ~~it~~ it has weaknesses. It has,



on my part--I will go through the steps First of all I will show you how a message which has been enciphered by an intelligible key sequence can be deciphered--here is the message Now we take the cipher message and we are going to assume that the word "possible" is used in the message and we assume further that the alphabets are, in this case, ^{are what we call} reversed standard alphabets So then, here is

we build up plain text because this key has been taken from a book and

so you see, here is plain text and what you have to do from here on is to guess what can follow such as the constitution, the constellation, the construction, anything that comes to mind until you get something clear that will follow logically the word hostile. Now the next step where you have two messages identically keyed in the M-209 device or any similar device Here is the two messages Here is a cipher message A and here is another message with the same indicator key



Now then this brings us to a good stopping place and we will have a break of ten minutes

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

- - - - - used in World War II, it was Of course, we had many many of them out for training and that's all we did have until the M-209 became available but for actual communications this was used in [redacted] and I'm going to tell you also of another place where it was used You will remember that we had a lot of our forces packed to the gills^{7.} in the [redacted] and they were officers, pretty clever young men and we received a message one day in Washington and in this cipher device which was preceded by a few words in the device itself for that message There was no other way of doing it at that time When the message was unbuttoned, it said, "Would like to get into communications. Please suggest key". Well, we scratched our heads and somebody came up with a good idea to wit. We would look in the roster of the names of the enlisted men in that unit and we would pick out one who was married and whose wife's full name was given and also this man should be a non-com, so we sent back word "Key to be used will be first and middle name of wife of so and so " Now this non-com's name was not in any directory so that the Japanese could easily find out who the officer was and that was the beginning of communications with these isolated units

Now we are going to proceed with the development of what we call rotor machines, electrical rotor machines This is the first one that I show--a product of the company which was headed by Mr Hagelin when his father bought out a Swedish cryptograph company in Stockholm This device was not a real rotor device in the sense of rotors as we know them today but I don't want to go into details. I merely want to show the device. The device is now connected with an

typewriter, an electrical typewriter, so that you have a permanent record Up
 to that time the device was only an indicator type of machine You press a
 key and the light would light and wheels would step and that way the type of
 message was stepped

The next slide shows a better picture of this with the Remington typewriter
 and the next step, of course, Mr. Hagelin took and he made the printing
 mechanism an integral part of the machine itself Here is the keyboard, the
 printing mechanism is in here and now very much smaller

Now I show the German Enigma machine, commercial model, which was invented
 and put on the market in about 1923-24 or thereabouts A keyboard, a light
 band, a set of wheels--these are the rotors In this case the circuitry

through a key of the keyboard, then through these rotors,
 I think beginning here, through these rotors and through this reversing wheel
 and back again through a light and everytime you press ~~you press~~ a key one of
 these rotors would step forward and it was in its stepping so that

it had a very short cycle as such things go about 26^3 and a little less than
 that on account of necessary to set the wheels. Now, I'm not

going to take the developments of that machine through World War II until

later. At the moment, I want to go directly to the American development in

rotor machines For this I show the picture of 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" and I said, "in jail, what for" and he said, "horse thievery"

I said, "were you guilty", and he said, "the jury thought so" and it was while he was in jail that he conceived the idea of a machine and here is the very first model, built presumably after he got out of jail, a keyboard, a left hand _____ or a place where you have 26 contacts arranged in a circular fashion, a rotor, a 26-point _____ on this side. You press a key and a lamp would light. Just one _____ --he built this machine for the Klu Klux Klan Here is the first printing model made by Mr. Hebern--still a one wheel or one rotor machine-- keyboard _____ electric typewriter connected thereto. I have among my treasures in the library a brochure which went with this thing and its a very curious document Now, one curious thing about Mr Hebern's rotors is worth noting He didn't have absolutely fixed wiring--these are detachable and this next slide shows 13 leads on one side and 13 on the other--this is a kind of _____ arrangement in order to save space but at any rate he did have 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 was a very important step--the cascading effect was a great advance in connection with rotors. Here I show his next development which was a 5-rotor machine Here are the rotors taken out just to show you what they look like They were still variable--you could take wires and rearrange them, keyboard and light band There is an interesting story connected with that one The Navy Department was very much interested in cipher machines which

was something they absolutely had to have for communications from Washington to the Fleet Commanders and, of course, intra-fleet and they were scurrying here and there 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 of a large sum of money for those days, \$75,000 and they proceeded then to negotiate with Mr Hebern. Now, at that time, in the code and cipher section, the Registered Publication Division they called it, there was a cryptanalyst of parts, it happened to be a lady, and she was quite able. She was the one who got Mr Hebern ready to jump from a three-wheel to a five-wheel machine and when he finished the development of that and he seemed to be on the point of getting a good sized order from the Navy Department, she accepted an attractive offer from Mr Hebern to come and join him out in California which she did. I apologize for introducing the first person singular so much but the fact that I became interested in this machine as a result of an inquiry from the President of the Naval Board that had been assigned to study the thing and I got the War Department to purchase one of these machines from Mr Hebern. I sat and studied that thing for some weeks--three or four weeks. The whole of my outfit consisted of myself and a veteran, an ex-prize fighter with cauliflower ears and the only thing he could do was to type, 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 thing for sometime until an idea came and then I went over to the Navy Section, it was in charge then of a Lt Struble, who now is Vice Admiral Struble, he may be retired. 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?" and he said, "yes" and I said, "I accept" and he said "well, what do you want" and I said "Oh, I'll take ten messages if you will put them up on your machine". He gave me the ten messages and I worked on those messages and I got to a place one day at the close of business when I had reduced the text of one of those messages to monoalphabetic terms--by this I mean I knew in the first line of the text of one of the messages, let us say, the first, the seventh, the ninth letters were the same letters, whatever they were--the second, the seventeenth and the twenty-third were the same and so on. That's all I had when I left for home that evening We were going out to some sort of a party and I had these letters in my mind, at least the identities and their positions, and as I was tying a black tie, it suddenly came to me and I can't tell you to this day just how or from where but the whole line of text fell into place with all the identities in the proper place. "President of the United States." I could hardly wait to get to the office in the morning--it was correct. I reconstructed the ten messages, turned them over to Lt Struble, and there was considerable amount of excitement. The Navy Department cancelled the order that they had placed, the Hebern Company, which had been selling stock on the basis of great prospects, went to pieces, the lady who joined from the Navy lost her job and came back Mr Hebern, trying to recesitate what he could from his fortunes, bought stock in/Southern⁵⁴⁵⁰California the part of at 40¢ and sold it in the northern part of California at about \$2.00 and the

California blue sky laws didn't like that so Mr. Hebern was tried and he spent a year in prison

I hope you won't think I am vain by showing this--I saved the paper which 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. Now then the Navy decided that the Hebern principle was still a good one and they went ahead with Mr. Hebern after he got out of prison and Mr. Hebern built some machines for them. I think this is the last machine -- this ~~xxx~~ is the last machine he built for them. They weren't satisfied with the power drive and the hand drive and this machine--again the Navy challenged the Army and the Army accepted and we solved messages in it. It had a different kind of stepping motion on which the Navy had put a great deal of faith. It was a good motion but nevertheless it had weaknesses that we could exploit. Now, that last machine that Hebern built, didn't work--I think that's it but there may be one more-- that's the last one he built and he wanted to get paid for it and when it was pointed out to him that the machine didn't work, he said, "show me in the contract where it says it has to work" and they couldn't so he was paid off and the Navy decided that they had had enough of Hebern and they went in on its own. They had a laboratory established in the Navy Yard and with a very able young man, named Seiler, now a Captain in the Navy, did some excellent developmental work. Now fifteen years later, the Hebern heirs and the Hebern widow brought suit in the

United States Court of Claims against the United States for \$50,000,000, believe it or not. The case has been pending for a number of years and the last I knew which was about a month or two ago, a settlement was in prospect for about \$30,000--that's quite a discount I might say that, except for these challenges, and acceptances of challenges, there was very little collaboration between the Army and the Navy cryptologic organizations. Each Service had its own secrets-- this was really too bad but it was mended later as we will have occasion to learn

Now, I'm going to show you a few slides of the Army developments This was the first shot that we had at developing a machine under the guidance of the cryptanalytic people in the Chief Signal Office, Signal Intelligence Service. A keyboard, 5-rotors, and now an interesting feature--an external keying mechanism I had come to the conclusion that internal drives for rotors had a fundamental weakness that you must not make the rotors depend upon themselves for the stepping so I conceived the idea of having a teletype tape which would step along and step these rotors in random fashion because these tapes were composed of random characters and that was our first shot at it I think the principle is still quite safe This is another view of the thing--here is the transmitter, tape transmitter, all the connections, etc It was a slow machine because of
 - - - - - Now we had a printing model, there it is connected with a electromatic typewriter, I think this was, one of the early models Still a five-rotor tape transmitter For the tapes we had boxes of I think

there were about 100 to ---- tapes from which you could make the selection for the day according to the keying document and you had various starting places on those tapes. The fatal weakness, of course, was the production and the distribution of the tapes. This was quite a headache and the tapes would break after they had gone through say thirty or forty times. Now, the Army development continued and here is the next one -- ^{keying mechanism with the} side-by-side arrangement with the/type-writer and this was the Converter M-134, which was finally put out. We had about 75 of these manufactured by a concern in New Jersey that was not particularly gifted in the typewriter art and the machines functioned all right but before even ten of them had been produced, we had come across a new principle for the control of the rotor stepping. I tried my very best to get the Signal Corps to change the development right there and then and shift to the new type of control. I was practically thrown out of the office of the Chief of the Division with the remark, "you go back to your den--your inventors are all alike. If we listen to you, we would never get anything out. Everyday you've got a new idea. Get out". So, we put the idea on ice. Now, this, I will switch to the Navy MARK I ECM-- electric cipher machine, developed and patented by the Navy without any help from Mr. Hebern. This now had a control mechanism for the rotors ----- the control mechanism consisted of wires. Now this is tricky and gave rise to a lot of difficulty but over and beyond that the machine had a fatal weakness. It had a key length of tremendous length but with only 15 different starting points. How this came, I do not know, but this was done of course without any coordination or collaboration from the Navy--we didn't ~~xxxx~~ even know there

was such a thing This was very very secret and finally I think the next is
the first production model of the MARK I ECM When there came a change/in the
in command
Navy code and signal section the new head decided that that development had gone
far enough and he wanted some help He wanted some help from the Army if he
could get it He came to see me one day and told me that they were in difficulty
and needed ideas if we had any I said, "well, we have a good idea but it's
secret" And he said, "well, what do you have to do to tell me I said, "I'll
have to get permission from the Chief Signal Officer," which I proceeded to do
Now I mention this specifically and I ask that you believe that this was the
situation--there were secrets from the Navy and secrets from the Army of course
on the other side But the Chief Signal Officer said "of course, let them have
it" And then we went ahead together and I told the Navy, showed them the
circuitry and the thing was adopted--the machines were developed by the Teletype
Corporation, a very competent organization and this is a picture of the MARK II
ECM--Navy terminology, SIGABA, Army terminology If it hadn't been for the fact
that we got together before World War II broke out, I mean when we began to
participate in it, it would have been extremely difficult for the Army and the
Navy to have any inter-communications at all The only thing that we had was
a disreputable hand-operated cipher scheme, pencil and paper which had been
adopted way back in 1930 by direction of the Chief of the Staff of the Army and
the Chief of Naval Operations and that's all there was. Fortunately, the ECM
SIGABA went to a war with great satisfaction to both sides and I am very happy
that we were able to get together 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 and although they knew that we had a machine of this character and although we knew their type of machine with which we were not at all happy, it was the policy of the, on the highest level of the Army and Navy to withhold this from the British and there was a terrible terrible struggle for several years until the recalcitrant people in both services high up began to see the light. The trouble was that when the technicians assured them that we didn't know they didn't know how to read messages in this machine without having the rotors and key list, they just wouldn't believe it. One reason is, of course, they were getting daily the ~~messages~~ ^{decrypts} that were being produced by the British and ourselves from German messages and they just didn't feel like taking any chances. They wouldn't believe the technicians so I don't know how many millions of dollars were spent needlessly in establishing ~~machines~~ ^{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 this one. A wholly unnecessary expense and extravagance, I think, but in the end in 1953, we were able to convince the authorities and powers that be that it would be all right and finally the British were allowed to use the ECM until they could get along with their own developments and be on their own. I think even at the present time, they still have some of these machines. As long as this slide is on here, I can explain the principle of the thing perhaps. This is the essential element for keying in the machine, it consists of a set of rotors here, five of them

and another set, five here, making a set of ten altogether. These are all interchangeable so you see to begin with you have a great number of selections from a primary set of ten rotors. Now a circuit, rather there are four inputs in this row of rotors and the output of these rotors then goes to control the stepping of the cryptographic rotors so that the stepping of these rotors is very erratic according to the output, the sequence of characters that come out of here. Here is another set of rotors, five small ones, which are used to permute the output of the control rotors,

Question from the audience. Will you comment on the relative security of this system and also whether it was ever compromised?

Well, we know of no 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 van containing the cryptomaterial and the SIGABA was stationed in front of the place where the Signal Officer and his entourage were quartered for the night. In the morning, that van was missing. It was a trailer, the whole thing was gone and there were messages sent instantly to Washington and there was a great to-do-- we blocked all the roads, the idea was to make sure that it wasn't being carried off by some German outfit but nothing turned up. We even diverted a river and we found the machine in the river. The vehicle had been stolen by Frenchmen purely for the vehicle. The contents were of no interest to them. The episode was one which caused court martial for the Signal Officer and several others. We had very strict rules about the safeguarding of this gadget. One of the funny things about not giving the machine to the British, I think I can hardly refrain from

telling you. I mentioned the strict rules about who could see the thing and who could service it and the maintenance, and so on and there came a time in North Africa when we had a unit there and maintenance men were knocked off and there was nobody to service the thing but there was a very very skillful British engineer. He serviced and maintained our SIGABA's.

Question:

No, we didn't learn of that until after the war

Question.

No, the strip cipher was but the ECM was never shown to the any of the Allies until 1953, not even to the British.

Now, I want to show you next the German Military Enigma. This was a modification of their commercial enigma but an important modification. I think you can see it better on the next slide. Here are the rotors--they are exactly the same as they are on the commercial model. now let's see what the modification was. There was a plug board, by means of which one could change the connections between the keys of the keyboard and the . There were 13 and this was not by accident, they had mathematicians who figured out absolutely the best arrangement for this particular machine and now the fatal weakness in the German Enigma communications was that they couldn't change their rotor wirings at all throughout the war. Without the rotor wirings we couldn't have done anything. With them we were able to read a very great amount of traffic. The German Command tried to make a printing model with wheels and this is it. We captured this in 1945 at

, Germany. It was not a success. Now about the enigma, I'll come to

that in the next talk The Naval enigma was much like the military except it had one more wheel and there were other things to it.

Now we come to the development of teletype cipher machine With the ever increasing speed of communications, it was necessary to speed up this business of cipher communications This was recognized a long time ago In 1919, for example, the A.T. & T. Company engineers, in collaboration with the Signal Corps, devised this modification of the then standard printing telegraph to make it a cipher printing telegraph This is the way it was done Here is the ordinary tape transmitter which was used to take the and shoot it out through the line but here there were two additional transmitters and they were differential diameters To begin with they started out with 1,000 characters in length and the other 999 so you can see if you start at a initial point, they would not reach that initial point until the long key and the plain text tape here a cipher tape here. This was a and of course know where to put them Now the A T & T Co. had great faith in this machine and they wanted to get the thing in use by the Army. It was put into use in 1919 By that time I had come back from France and we were challenged to solve this kind of system at Riverbank. I accepted the challenge and I think it is too long a story to go into right now but as a result of the solution, the Army dropped the project I think it was in a way too bad because we had a need of it later on in the early part of ~~1921~~ 1942 when we wanted crypto-communications and we actually went back to this thing. The big trouble of course was the production of key tapes.

The problem of manufacturing key tape is one which is still with us and this is an old model of a machine for making key tapes. You see this is an electronic type of key generator, random noise, noise is used to produce the impulses in random manner to make tape for teletype encipherment purposes.

Next I show a development called SIGCUM. This is an I.T.T. venture. They were interested in trying to get up a cipher machine teletype encipherment. This, by the way was designed by

(tape ran out)

after he had retired from the Army and presumably was to incorporate a very secure principle but, I am sorry to tell you that it wasn't a secure principle and again ~~the~~ I had the unpleasant duty of having to tell Colonel Hitt, after some test messages were solved by the Secretary of State by the Army group, that I wasn't at liberty of telling him what the trouble was. This was a fixed policy in the Office of the Chief Signal Officer and I think ~~you know~~ ^{an} understandable one. If we undertook to tell inventors what the trouble is with their inventions we would never get anything else done but try to bring them up-to-date in cryptanalysis and this ~~is~~ was not a politic thing to do.

This is the device which the Army developed to encipher teletype communications. We call this the SIGCUM. It used not perforated tapes but rotors again, rotors which step in an erratic fashion but not as erratic as in the SIGABA and ECM-- it's not a bad machine. It had weaknesses, every once in a while when we discovered new ways of doing things, we found that SIGCUM had weaknesses and then we would proceed to tighten up the thing and change the method of usage or their method of stepping and so on. That was used, well that's a picture of the entire

workings of the thing-- that was used in connection with the big set here--most of that was unnecessary, there is the SIGCUM there teletype and all this is the mixing apparatus for taking signals from here and mixing them with the SIGCUM and then putting them out on the line--a very very dangerous thing from the point of view of electro-magnetic radiation

This is a war-time development of a self-contained or integrated unit, particularly teletype and cipher machine Not successful ~~complexity~~, a little too complex for use by even the large commands in the rear Now we have to say a few words about other types of ciphering apparatus For example, it is necessary to send meteorological data and maps in time of war, weather maps and other types of maps so it was desirable to have a machine which would encipher facsimile and here is one such machine that was developed by Army for the purpose, called SIGMEW We call a machine for enciphering facsimile, cifax We also had need for machines that would encipher telephone conversations and this was the first shot at it--a development by the Bell Telephone Laboratories, called SIGJIP. It was a gip in a way--it gave you much more feeling of security than was warranted by the circumstances means of Conversations enciphered by/that thing could be read very readily but the Telephone Company proceeded with its work in collaboration with engineers from the Signal Intelligence Service and Signal Corps and we developed a very high grade ciphony system which became known as SIGSALY. Each terminal cost over a million dollars and there were a total of 7 of them This is just one piece of apparatus--the two ends of the circuit were kept in synchrony by means of a very very high grade record playing mechanism that controlled the

----- and so on. It was very very useful, the whole thing was very useful

~~XXXXXXXX~~ This is a vocoder type, those of/^{you} who have gone in for ciphony realize that what I mean, or recognize what I mean, by vocoder. You take the speech and signals and you chop them up into discreet units and you encipher those and that is what you transmit. At the other end you take off the cipher and then you have the units and you put them together in the proper way

Now in addition to machines for facsimile, machines for telephony, we have been working along the lines of machines for other purposes, such as, recognition, identification, IFF, callsign machines--this is a war-time callsign machine developed by the U S. Navy and based upon an algebraic principle which was described in a paper in one of the mathematical journals and it appealed to me.

I could never get the Army to go ~~into~~^{in for} callsign changes in a big way, the Navy ^{was} did and this ~~is~~ a principle that appealed to me and I suggested its possibilities to the Navy and they liked it and I think my friend here, Dr. Tompkins, had a lot to say about the actual form of this thing This isn't what he really had wanted and perhaps he would like to say a word or two after I finish in a moment or two

We will have to have enciphering apparatus for telemetering signals and for television, anything in the way of a signal, sooner or later we are going to have to have means and mechanisms for their protection

Now a professional cryptologist is always amused by the almost invariable reference by the layman to "the German code", "the Japanese code", the U.S. code To give an idea as to how fallacious such a notion is, I will say as I said once

before, there are hundreds of systems in simultaneous use in the large governments, at least, of the world and the next slide will tell you--oh, that's a picture of the SIGSALY--just one part of the terminal. We have, by the way, reduced that. It used to take as much space as this whole building here but we have reduced it now so that a machine the size of one of these little chambers or cells is quite adequate and we have got even smaller ones.

This slide shows the number of cryptographic systems in effect on 7 December 1941 until October 1945 in the Army alone. Thousands of them and the next slide shows the number of holders of cryptographic materials from the same dates, December 1941-October 1945 and this is U.S. Army and U.S. Air Forces alone. It does not consider U.S. Navy which had as great or perhaps greater distribution. Now keeping track of the crypto-material and accounting for it is a big headache. There is no way of getting around this that I know of and it is important that the rules for the protection of the material be followed absolutely to the letter. I'm going to show you as my wind-up two slides. The Japanese had very very definite rules too about the accounting for crypto-material and they were supposed to burn the codebooks and the keys and the ciphers tables and so on and to scatter the ashes and then make a certificate witnessed by a fellow officer. Now we very often got these certificates by radio and then we would find a case like this where a chap has made a certificate, certifying to the destruction by burning, the scattering of the ashes but he was observed. He took a spade and he dug a hole and he dumped the codebooks and the tables in that hole and he poured some water in and he went away and that was it. Well, in due time some of our people sneaked out, dug up the hole, got out the material and brought it

in and there it is being dried out This helped a great deal because it saved us an enormous amount of time to reconstruct that particular code There were instances of this sort every now and then By the way, the Japanese were worried about this business of their security They felt that something was wrong and the only thing that they could imagine was that there were spies so there were messages all the time requiring the commands to go through their quarters and look under the beds and seek spies Of course, that wasn't the case at all, we were solving their codes and ciphers because they were not secure

I am going to bring this talk now to a close by repeating the importance of the slogan which we try to inculcate Don't learn your COMSEC laws by accident Gentlemen, thank you