SECRET

Skird Reread

as modified and delivered on 26 April 1960

SLIDES FOR THIRD PERIOD

36 plides mead

	PAGE	SLIDE NO.	TIPLE
	7	 45 45.1 45.4 47 48 	Alberti disk Porta U.S. Army disk Cipher disk finally patented Wheatstone
	8	4949.4	Wheatstone - modified Bazeries Cylindrique
	9	√ 16ø.1 √ 5ø.4 ✓ 159 ✓ 5ø.3	Colonel Hitt Hitt's original strip Hitt's wooden strip model Mauborgne M-94
	1ø	√ 50 √ 50.1 √ 50.11 √ 54	Jefferson's Wheel Cipher Page 2 of same M-138 Kryha
	11	/ 55	Dissertation on Kryha
	12	√ 171	M-161 (Sig. C. Labs machine)
•	12A	√ 164.1	Hagelin
	13	√ 68	c-36
×	14	√ 70.3 ★ 260.1	G.I. model of M-209 CX-52
	15	✓ 59	B-21
	16	65✓ 57✓ 71	B-211 integrated Enigma Hebern
X T	17	√172 ✓ 71.1 × 71.2) × 71.3) ✓ 172.1	First Hebern model First Hebern printing model Connectable wirings 3-cascade Hebern
	į.	√72 ⊀ 73	5-rotor Hebern 5-rotor with rotors removed
	2ø	165	Solution of Navy test messages
ر -		×170.7	Hebern's last machine for the Navy Converter M-134-T2, and electrical typewriter
	22	172.4 173	Original model of the Mark I, ECM.
er e	23	√ 173	SIGABA
	25	×177	CCM
	26	× 74.1	The German Steckered Enigma, with box of rotors
	27	√ 56	The AT&T Co. Printing Telegraph Cipher Machine

PAGE	SLIDE NO.	TITLE
* 28 *	258 178 ×179	One-time tape production equipment SIGCUM Unit (external view) SIGCUM Unit (internal view)
29	¥ 183 ≭ 185	SIGMEW - Cifax SIGJIP
. 31	* 236	Number of cryptologic systems in effect - 7 December 1951- October 1945
34	×	KL-7 KW-9 KW-26 KL-36 KL-17
34-A	Y X-27	KW-3
35	x x-28	KW-37
	× X-29 × X-30 × X-31 × X-33 × X-32	KY-3 KY-8 KY-9 SIGSALY terminal of World War II days. KY-11



COMMUNICATIONS SECURITY

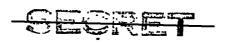
Gentlemen, this period will be devoted to the subject of communications security, how it can be established and maintained.

Three or four years ago there was being hammered into our ears over the radio in Washington a slogan concerned with automobile traffic safety. The slogan was: "Don't learn your traffic laws by accident." I think the slogan useful as a sub-title for my talk but I'll modify it a little--"Don't learn your COMSEC laws by accident." I begin my talk by reading the Webster

Dietionary definition of the word "accident". I know, of course, that payable only a few of you will ever be directly concerned with COMSEC duties, but as potential future commanders of fighting units the definition of the word "accident" should be of seal interest in connection with the law of 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."

I will now make the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by reminding you of a minor Example and the definition relevant by the definit



CENED-A63360

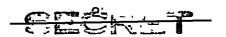
important episode of the war of the Pacific during World War II, and I will preface reminding you that during over participation in introduce the account of that episode by coving that during over barthe preface World War II the accompanied by a good many VIP's, President of the United States, Commencial with Charles and Commencial Commen Christian Company of the Company of journeyed several times half-way around the world to attend special markings want conferences. They apparently could go with safety almost anywhere. <u> misophyddingyddau mae comerciae serenengai croenengo o compted coesistatury</u>. They met with no accidents. On the other hand, the Japanese Commander-in-Chief of the Combined Fleet, Admiral Isoroku Yamamoto went on an inspection trip in April 1943, the sequel to which may be summarized by an official Japanese Navy communique reading in part as follows: "The Commander-in-Chief of the Combined Fleet, Admiral Isoroku Yamamoto, died an heroic death in April of this year in air combat with the enemy while directing operations from a forward position." Uuquota As is often the ease, the communique did not tell the whole truth. In sure that everybody in this audience brown that 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 maybe it was Jimmy Walker, then Mayor of New York City, statement/but it is decidedly applicable in this case: "Accidents don't happen,

they are brought about". U.S. Navy communications intelligence experts were quite

regularly reeding practically all because its cryptosystems the Japanese Navy's high secured messages/anisting were not secure.

In the case of Yamamoto's inspection trip our Navy had his, schedule down paty

AND THE TRANSPORT AND THE TRANSPORT OF THE TRANSPORT AND THE TRANSPORT OF THE TRANSPORT OF



They also knew what his air escort would be, and secon. It was relatively easy to bring about the "accident" Yamamoto was to suffer: and it is abrices that his death was no accident in the dictionary sense of that word--it was brought about, hereing Change om vikinerosekinemorinamakose jeruxmasyasida karistnix vasastasdagosinastasa air inecazonum maakosa istomas vasastastas d Wikity Aries x verte konnex kuri konex kermen kermen karang x kalang kermen ker imperior because his communications were insecure. 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 certain of them 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.



said aute

"Yamamoto story in this morning's paper has placed our activities in

very difficult position. Have meticulously concealed our special.

At this point Forestal interpolated that 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 continued: "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 suicide until after next week when we expect to have milked them dry...."

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered with an operational priority TOP SECRET dispatch.

Washington answered who are embarrassed by the

Washington answered with an operation of the story washington and priority TOP SECRET dispatch.

Washington answered who are embarrassed by the

Washington and Secret dispatch and priority Top Secret dispatch and priority Top Secret dispatch.

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

But not many years passed before the Japanese began to realize many hour was that had happened to them had come work, and recently published books by

Harradinius kalignuss patiteras ta Commandon aim Glick and the adequace allowy amid as



REF. ID: A63360...

Japanese

Navy officers come out quite openly with statements attributing their defeat to poor COMSEC on their part, and excellent American COMINT and COMSEC. For example, Silved you a paragraph from there is Captain Fuchida's book entitled Midway: The Battle that Doomed Japan,

Chapter VIII, p. 131:

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."

So much for tan introduction to this period on COMSEC, and now (Here as an acide what Wenger told as to disbelief in decrypts.)

lets get down to the matter itself.

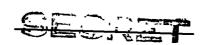
It is hardly necessary to tell you that with the advances made in the

CECRET

various

consider the ever-increasing speed of electrical communications. However, to approach the ever-increasing speed of electrical communications. However, the state of the ever-increasing speed of electrical communications. However, the state of the electrical communications and let me remind you that the impetus for devising and developing better untilization means for crypto-communication came not only from the need for speedier crypto-apparatus but also—and perhaps more importantly—from the need for much greater security in those communications, which were now largely by radio and were therefore susceptible of interception and study by the enemy. However, the state of the electrical communications are electrical communications. The state of the electrical communications would at least begin to approach to approach the electrical communications. However, the state of the electrical communications would at least begin to approach the electrical communications. However, the state of the electrical communications would at least begin to approach the electrical communications. However, the state of the electrical communications would at least begin to approach the electrical communications. However, the state of the electrical communications would be electrical communications and the electrical communications would be electrical communications.

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 some slides.



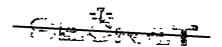
Aside from the much earlier Scytale used by the ancient Greeks, the earliest cipher device known to history is the cipher disk, first described by an Italian cryptographer named Alberti, who wrote a treatise on ciphers in Rome about 1470.

His xis the soldes between expression of yether baths arough a parameter

- later in a book by another Italian cryptographer, Porta, who recommends the use of the cipher disk with keywords. I have the Porta with me.
 - The next slide pictures the U.S. Army Cipher Disk, which was used in the period 1914-1918, and which follows exactly the same principles that Alberti recommended. It seems to have taken a long time 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 it is.
- Next is a picture of the Wheatstone Cryptograph, the first real improvement on Alberti's device. I have the only expr in the United States, maybe in the world, and I've brought it with me. Sir Charles Wheatstone interested himself in cryptography and invented his device in the latter part of the decade 1870.

 It is not just a simple cipher disk. It consists of the ordinary alphabet on mixed the outside and an alphabet on the inside; the latter being a mixed sequence; and 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

the plain text, the small or "hour" hand advances one step for each complete

Thus the capter agricultation of the "minute" hand, just as in a clock. At the close of this period change as you go 'round and 'round.

those of you who would like to examine the device may do so.

Western front, our British allies resuscitated 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 can

now be made variable mixed sequences, whereas before, in the original Wheatstone,

only the inner alphabet could be varied.

How of these drives

to be issued to field units, not only British but also French and American. All the top cryptographers of the Arlied Foreas were have of the tryptotecounty of he doing forces were to use it. But even before they could be put into use it was shown by a young updat that the pecunity mashturat those cryptographers thought it was that the security of the device was inadequate and they were withdrawn. I had I was still at Riverbank when I proved its insecurity by solving five short message something to do with demonstrating the insecurity of the device and when I pent to Riverbank as a challenge. The first challenge message said in Whan I reached American GHQ in France about three months later I found I wasn't a bit popular second those thousands of Wheatstone dericas which had been solved had popular with certain British, French and American cryptologister. Reliance therefore continued to be placed in codes.

Sometime in the 1890's

Mert 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

-82 "This cipher is absolutely underplaceble

49.4

sequence, and the mixed alphabets are all different, each bearing an identifying letter or number for assembling them upon the shaft in some key order, so that the correspondents have the same sequence of disks on their cylinders.

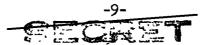
You not your message interesphere 20 letters at a time (because there are 20 rings), by rotating the rings to align the letters of your plain text horizontally, whereupon for the cipher text you can choose any plain text horizontally, whereupon for the cipher text you can choose any plain one of the other 24-rows of cipher text. (Bazeries used a 25-letter alphabet.)

This principle seemed to be a very good one and messages in it appeared to be quite safe, but Bazeries never got anywhere in his attempts to get the Army to adopt any of his ciphers, uncluding his cylindrical cupher.

The adopt any of his ciphers, uncluding his cylindrical cupher.

- In 1915, an American Army officer, Captain Parker Hitt, about whom I have wentioned before, told you, conceived the crypto-principle of the cipher cylinder independently.
- you see. This was Hitt's very crude first shot at it, and, as a gift
- the interesting items in way.

 50.4 from him, it is among a collection. Here is a better model, one he made in 1915, with the paper strips mounted on wood--wooden sliders. That
- device was brought to the attention of the then Signal Corps Major Manborgne, imagined in Washington, who thought he'd thought up something new when he made a cylindrical form of the thing, going back/unknowingly to Bazeries' model.
- Here is Mauborgne's model; it is made of brass and is very heavy. -And here's
- 50.3 the final form of the device, as adopted in 1922 by the U.S. Army. It became



what we call Cipher Device type M-94, used by the Army, the Navy, the Coast

Guard, and the Treasury. A couple of years after the M-94 was put into service

a friend showed me a write-up of something he'd come across more or less accidentally

in the Library of Congress, among the papers of Thomas Jefferson. Jefferson was

the first to invent the cipher cylinder principle, and he anticipated the Frenchman,

Bazeries, by a century. Here is the first page of his description of his device,

which he called "The Wheel Cypher." 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 both Army and Navy cryptologists soon came to the conclusion that security would be much increased Muriable.

by the use of changeable instead of fixed alphabets. Among other versions, I had one made which used metal rings on which we could mount slips of paper and fasten them; thus we could change the alphabets as often as was felt necessary. Navy

Between Army and Navy

tried other versions. That was the beginning of the various forms of strip

were developed and come to be
cipher devices used by the Armed Forces, and later by the State Department and

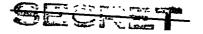
U.S.

50.11 the Treasury Department. Here is a picture of the final Army strip cipher device.

The strip ciphers carried an enormous amount of traffic before and during World War II.

But the were to-called "hand-operated" or penell and paper ciphers, whereas what we have to a machine called the Kryha, invented by a German, in about the year 1925. According to its inventor the Kryha was the last word in the way of mechanical cryptographs, and he tried to interest various governments in his machine. There isn't time to explain the machine, but

readed were marking or better devices.





xtededigioscrepatives differentiado de la contrata del contrata de la contrata de la contrata del contrata de la contrata del contrata de la contrata de la contrata del contrata de la contrata del contrata del contrata de la contrata del contrata dela xisconoundedconoscodiskxisioischxisconoteisedcengubenkycaeccondingotockbeotootbaedc wick consumption of the constraints and constraints are constraints and constraints and constraints are constraints and constraints and constraints are constraints are constraints and constraints are constraints and constraints are constr xecunosistic xxxxx a local contrator de la con Address control of the control of th and colored and the colored and control an XXXIII SOCIAL CONTROL here is a dissertation on the number of permutations and combinations the Kryha machine affords, written by a German mathematician. All I have to say about it is that in this case, as in many others, merely the number of permutations and combinations which a given machine affords, like the birds nothing or that sing in the Spring, often have/little to do with the case. Much depends upon just what kinds of alphabets are employed and exactly how they are employed. Large numbers of permutations and combinations don't frighten the cryptanalyst at all. For example, to give you a simple illustration, 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 ciphers by an exhaustion method. There are very much simpler ways of deing it. Take another example: Suppose you have a machine that provides hundreds of millions

have a machine that provide

55

presented successively in a fixed sequence. Such a machine would give poor security because in heavy traffic many messages would be enciphered by the same sequence of alphabets, producing a condition which the cryptologist calls "depth". When this is the case he proceeds to solve the set of messages vertically, column by column, and when he's finished he can read the messages horizontally and cureka! the business is successfully terminated. When

To return now to our general survey of crypto-machines, it became clear that there was a pressing need in the military and naval services for two types of automatic machines, that is, machines which would get out of the reals of hand-operated gadgets. First, we needed a small machine for low echelon or field use and all machiness; second, we needed a larger, address high-security, electrically-operated machine for name achieves, high-command use. Let us take up the first of these two types and see what happened.

171

I show you next a development model of a machine constructed by the

about 1934
Signal Corps Laboratories, developed without guidance from Washington. The

Director of the Laboratories at that time was a great believer in autonomy

and he wasn't going to have Washington tell him anything about how things were

in Laboratories

to be done. When it came to developing a cipher machine, he decided that he

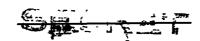
and his staff could produce a really good machine without the help of the Washington

cryptanalysts. So he proceeded on this basis to use up the tiny bit of money

then

not permitted

that was available—\$2,000. We in Washington were to know what



was being built until the final model was completed and ready to be delivered to us. 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. There's the machine, take it The Colonel never was given the opportunity to improve his model, with you." Alberteconserves and the construction of the constructi because the crypto-principle was very faulty and the laboratories development motorine, xboth hexperexxensive white xpportant by the very contact that xplan x because x came to a sudden and ignominious end. The whole development represented a loss the cryptoeprinciple was were faulty sold with the beauty and the contract of t That fiacco A STATE OF THE PROPERTY OF THE PROPERTY AND A STATE OF THE PROPERTY OF THE PRO xing venitors according a comparation of the compar Ay and a contraction of the cont these value came via terror exemple more via circulation in the content of the co xygototogyx y wild a single of the contraction of t

Now we come to a development which is of considerable 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

American field forces

that all the services 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 the forces one that will present become clear. It wasn't a case

of NIH--"not invented here" but the decision to have them made for and used

164.1

by the United States Army-was a decision on a level higher than my own, and standard about 1939 at a level higher than my own, and standard accomplished that it turned out. The thank that my superiors were right, for our troops at least had something for low-echelon crypto-communications, whereas if I'd had my way they'd have had nothing but pencil-and-paper ciphers, or the strip cipher device-all too slow.

Now just a bit about Mr. Hagelin. He did what A best described as a hysteron-proteron. That'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 meanly two several million U.S. dollars from his invention. That's not at all a poor sort of hysteron-proteron if you're going to do one.

wol. ?

Here's a picture of Hagelin's very first machine. I've brought one of his

very first models, in fact, number one, fer your inspections. It was a present

from Mr. Hagelin, for my museum. Interested the Signal Corps in them. As

a consequence we built in America, for World War II, this six-wheel Hagelin

machine, which many of you no doubt know as Converter M-259. Prove the translation with

machine, which many of you no doubt know as Converter M-259. Prove the translation with

George continuous times you who six sales to the many hadron and the machine the machine the machine and specifications, and with American tools, rapher

ECRET

then European metric measurements and tools, and we built an astonishing number

of them--over one hundred and ten thousand, w fact. They were used by the Army, the Navy, and the Marine Corps.

Many-of-you key know that the M-289 had a serious; a very serious security

weekness, about which I'll say a few words later. This is a picture of one our M.209
of the Hagerin machines as modified by some of our GI's in Italy. The M-209

70.3 has no printing mechanism and you know how resourceful GI's can be. A couple

of them serounged parts here and there end improved their machine to make it

a printing model. See, here's the keyboard, and here's the printing mechanism.

they pasted Inside the cover 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 damned thing work?"

continued has broduced so wrat has broduced so wrat machine and this is a side view

models which 260,1 of one of his latest models the CX-52: It prints not only the plain text but also the cipher text, and its incorporated a much improved ciphering mechanism, with associated driving mechanisms. However, all of these models have a because the wheels, instead of being permanently fixed upon the shart, are demountable and ear be rearranged in 720 different ways. The stepping motion for these wheels is complicated. We've studied this improved model for some time and as of this moment we do not know how to solve ciphers produced by this machine. But it still has the very serious weakness, that when two messages are in depth, that is, as I've explained earlier, when they are enciphered by the same keying sequence, they are pendily solvable. If time permitted I could show you how easily this is done; but you'll just have to take my word

for it. When there are several messages in depth the solution becomes even And the bad part about this from the standpoint of COMSEC is that with easier. a solution by depth the recovery of the key -- the whole setting of the machine -often is not at all difficult. Then, of course, the solution of all other messages arrangement of keying elements is an easy matter. enciphered by the same That is the fatal weakness of machines of the type of the M-209 and is the big problem in connection with the use of what we call key-generator problem in connection with the use of what we call key-generator cipher machine which has been built and proposed possession types of devices. amakundissaniki kupika inara aranggan ministrang kanaga kanaga Till show you a produce of it later. use 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 I think we will have easy solution when two or more messages are in depth. With xim was xx kpk n hex xx something better very soon, and I've brought a model to show you. It doesn't have the weakness of the M-209, and has a much higher degree of security. Moreover, it requires no source of electrical power -- not even a dry cell- and it produces the last proposed and the surface of the last printed record.

Now for a quick review of the development of what we call electricalrotor machines. The first one I show--also a product of the Hagelin Company
in Stockholm--was not a real rotor device of the type we use today but I

don't want to go into details. I merely want to show the device, which is

connected to a Remington electric typewriter, so that instead of writing

down letters one by one you can make much more speed by having a printed record.

Up to that time devices of this sort were only of the lamp-indicator-type of

You'd aircota would move but you'd

machine. You'd aircota would move but you'd

machine. You'd aircota would move to write down

have a Rey for the next encepherment,
the letter flashed on the light bank and then the cipher wheels would step.

59

The next forward step was taken when Hagelin made the printing mechanism an integral part of the machine itself. Here is the keyboard, the printing mechanism is in here, and now the whole assembly is very much smaller and more compact.

57

Now I show a German machine known as the Enigma, a commercial model, which was available until Iteler came into power. invented and put on the market in about 1923 24. It comprised a keyboard, a light bank, a set of plactric wheels called rotors, and a small dry cell for power. In this case the enciphering-deciphering circuitry is more complicated. The current The current to to the keyboard, then through a contact on a fixed entry and then through plate or stator, into these stepping rotors, and by means to a reflector or plate which sends the current but over a different path reversing when, back through the cipher rotors to one of a bank of lights. The current goes through the rotors twice, which complicates things a good deal. Each time a key is depressed at least one rotor steps forward and changes the circuits between the keys and the lamps. In World War II the Germans such things go, tese than 263; it was a little less than 233 because of certain used a modification of the Enigma, but they lost the war nevertheless. factors into which it isn't necessary to go.

war II. At the moment, and in period of time to anticipate German developments

'hear'

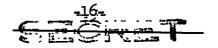
in this field, I want to go directly to the American developments in rotor

machines. First, I show a picture of the late Mr. Edward H. Hebern, a

Californian, who seems independently to have thought of rotor machines. I

asked Mr. Hebern one day how he happened to get started on such things 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: 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. It is possible 172 that he built it as an item of occupational therapy while in jail. but I think it more likely that he built it after he got out of jail. It has a keyboard, a left-hand stator, that is, a ring of 26 stationery contacts arranged in a circular fashion to one of which the current goes when a keyboard key is depressed; a rotor of 26-points, and an exit stator of 26 contacts on this side. It is important to note that there was no reflector rotor; the type here is what we call a "straight through" rotor machine. You press a key and a There was just one rotor in his first model, which he built in 1922 At/1923 for the Klux Klan. Here is the first printing model made by 71.1 Mr. Hebern--still a one-rotor machine--with a keyboard and, now, an electric typewriter connected thereto. \One interesting thing about Mr. Hebern's rotors is worth noting. He didn't have apsolutely fixed wiring, as in the German Enigma rotors, for these are detachable wires, showing that at an early date he conceived the idea of variable connections in rotors. This is an extremely in any kind of a high-security rotor machine.

development description of a high-security 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

72. show his next development--a 5-rotor machine. Here are the rotors removed.

23. from the machine to show you what they look like. They were still variable

connection-changers -- you could take wires and rearrange them as and when you pleased. There is an interesting story connected with that model. The Navy Department was very much interested in cipher machines, much more so than the Army in those days, because they absolutely had to have secure means for speedier communications from Washington to the Fleet Commanders and, of course, for intra-fleet communications. The Navy thought this Hebern model a suitable machine and they got an appropriation for the purpose, a large sum of money for those days, \$75,000. They proceeded then to negotiate with Mr. Hebern. I was asked by the President of the Naval Board that had been appointed to study the Hebern machine to give him my personal opinion of its security., I had no machine and the Navy had only two, both undergoing service tests. But I persuaded the War Department to purchase a machine from Mr. Hebern., I set and studied it for some weeks -- three or four weeks. (The whole of my outfit them consisted of myself and a World War I veteran, an ex-prize fighter, with crossed-eyes, pug-nose and cauliflower ears; the only thing he could do was type; and I may say that he could copy from draft letters or cipher text with absolute accuracy, but that sall he could do The rest of the was up to me. for three or four weaks without even a glinemer of the I say, I studied the Hebern machine until an idea for a solution. come to Suddenly one come to me. I tried it out and found it pretty good, whereupon I went over to the Navy Section, which was then in charge of a Lt. Struble, was now in 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?" I said: "How about ten messages put up on your machine?" He gave me the ten messages and with some typing bely from that exprize fighter I worked on them until I got to a place one day, at the close of business, when I had reduced the first line of the text of one of the messages to simplest terms: I knew that in the first line of the text of that message the letters which were the same but I didn't

know what the letters actually were. Let us say, for

-22-

-19-

action was accommondated by the start start action from the start action in the start account action and the st

19th +25th

instance, that the first, the seventh, the ninth letters were the same, what-18th 22th 24th

ever they were; the second, the seventeenth and the twenty-third were the same,

\65 and so on. That's all I had when I left for home that evening. We were going

but these identities were apparently deeply ! I to some sort of a party, and I had these letters in my mind, at least the ones

inhedded in my subconscious mind.

that were identical and their positions. As I was tiging 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 repetitions in the proper

place: "President of the United States." I could hardly wait to get to the

next when, office in the morning, and to my intense gratification, I found that my sub-

conscious guess was correct. I reconstructed the ten messages, turned them

over to Lt. Struble, and there was a considerable amount of excitement after I

showed him how I'd reasoned out a solution. The Navy Department cancelled the

order that they had placed; the Hebern Company, which had been selling stock at \$200 of Delling many machines to the Wavy Autorial a financial disaster to on the basis of great prospects, went to pieces.

wiencjoimedatheringrerriemelestarkenriodrendenkesselt tomber telegrapheck. Mr.

Hebern, trying to recusitate what he could from his unfortunate encounter with

Hebern Company
an unknown cryptanalyst, bought stock in the Southern part of California at

40¢ and sold it in the northern part of the state at about \$2.00. The

California Blue Sky Laws didn't like that sort of conduct and Mr. Hebern spent another

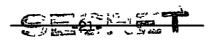
giving him lots of time and opportunity to think up improveyear in prison,/ Imperiment addresspace and a single process and the prison,/ Imperiment address and a single prison,/

ments on his machine. AMORTOLIMOMENTANIA NATIONALISE XIL SENIONE SEN

Despite my solution we thought that the Hebern principle was still a because the money was available, good one, and Navy went ahead with Mr. Hebern after he got out of prison. He built another model and poon after to delivery Mr. Hebern naturally wanted 172.10 Here's a picture of the last machine he built for the Navy. Hebern wanted · - - - ite. to get paid for it; there was just one hitch--the machine wouldn't work. when this was pointed out to him 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 establishing in Washington, went into research and development themselves, a laboratory being established . . in what was then called the Navy Yard. Years later the Hebern heirs brought suit in the United 100 States Court of Claims against the United States for \$50,000,000, which was settled plast summer at a considerable discount, \$30,000, just to get him of their necks. Now for a few words about

I'm going to show you now a few slides of the Army developments in rotortype crypto-machines. This After the debacle I've told you about, was the first shet that we in the Signal Intelligence Service in the Office of the Chief had the cooperation of the Signal Corps La broatories in Signal Officer, in Washington, had at developing a machine for the Army. Https: picture of it. had a keyboard, a light-bank, 5 rotors, and now an interesting feature -- an external keying mechanism. I had come to the conclusion that internal control mechanisms for stepping rotors had a fundamental weakness; that is, I felt that you must not make the rotors depend upon themselves for the stepping, and I conceived the idea of having an external key, for example, a teletype tape, which would step along and control the stepping of the rotors in random

the rotor stepping was quite erratic, and that was our first shot at it...



I-think the principle is still quite safe, especially if the tapes aren't : overburdened in usage. This is another view of the same machine -- here is the tape-transmitter, the rotors, the keyboard, an electromatic typewriter, etc. I think this was one of the very early models. We had boxes of about 100 key tapes from which you could make the selection for the day according to the keying document. A serious practical weakness, of course, was the necessity These. These machines functioned all right but before even ten of them had been produced we had hit upon a new principle for the control of the rotor stepping. I tried my very best to get the Signal Chief 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 on my third true division with the remark, "Go back to your den--you inventors are all alike. A new and better idea every day. If we listened to you inventors we'd never get anything out." So we had to put the idea on ice, that is, in secrecy for a while. About Hat time the Wary had its Mark I ECM, an I will switch Now to the New MARK I ECM, the electric cipher machine, designed, developed and built by the Nevy without any help from Mr. Hebern. It had a new type of control mechanism for rotor stepping, based upon the use of Bowden wires or flexible cables . They were tricky and gave rise to a lot of difficulty

172.4

but over and beyond that the machine had a fatal security weakness. It had not

Reguence decorate of tremendous length but with only 15 different starting points.

Yeu'il remember what I said about such a situation a few minutes ago.

/ New this case I do not know for there wasn't any coordination

Between Navy and collaboration in those days with Army cryptologists -- we didn't even know that

such a machine had been the machine built by Navy. Each service went its own way. When

there came a change in command in the Navy code and signal section, the new head Re security of the Mark I ECM wasn't good

decided that that development had gone far enough and 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 new ideas. if we have any? I said: "Well, we

or I have a good idea but it's secret." He asked: "Well, what do you/have to do to get

it released so that you can /tell me?" I told him: "I'll have to get permission from the Chief Signal

Officer", which I proceeded to do. I mention this specifically and ask that

you believe that this was the situation in those days--there were Army secrets

and Navy secrets, and never the twain did meet. When I told the Chief Signal

Officer what Navy wanted, he promptly said: "Of course, let them have it".

So A told the Navy about the Army idea for rotor control; we showed them the

involved. They liked it and by joint action at large number of their circuitry, and after some delay the thing was adopted. The delay was caused by

Navy doubts that sufficient current

Navy doubts that sufficient currents could be obtained through sets of 16 or more rotors,

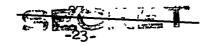
they were having contact troubles with their rotors of But the machines were built

Imachines for the Navy and the Army were built the machines mad the by the Teletype Corporation, a very competent organization, and were highly.

Anny cryptoprinciples and they were highly
173 successful. Here is a picture of the MARK II ECM, Navy terminology, or the

SIGABA, Army terminology. If it hadn't been for the fact that we got together

before we became belligerents in World War II, it would have been extremely



difficult for the Army and the Navy to have had any inter-communication at all

in World Were II - A River and Architecture abiestican xinetic floridation and approximate and a second and a

proprietient vogeka trect xa i plaenvoor ing xpara kirvendorpegeavo; malaka kirat kirea xalampiaedocvany

The ECM-SIGABA came into use just in good time, and it was used

with great satisfaction on both sides. I might add, in closing that incident,

that, to the best of my knowledge, this is the only gadget that was withheld throughout World War II.

from our British Allies, Although They knew that we had a machine of this character and although we knew all about their type of machine, in fact, the Navy was using it for communication with the British, Reduced the second communication with the British and the second communication with the second communicat

it was U.S. policy on the highest level in both the Army and the Navy to

Them.
withhold our machine 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 current 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 for this adamant policy was

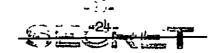
that they were daily getting the decrypts that were being produced from German,

Italian and Japanese messages and they just didn't feel like taking any chance.

"How can 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 for the salver

in establishing means for inter-communication with the British. By this I mean



that we had to develop, produce, and use an adaptor for our machine so that it Inter-communicate with the British TYPEX, and the British had to do the same for their machine to inter-communicate with the ECM-SIGARA. 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 it would be nice if there were time to explain the crypto-principles of the ECM-SIGABA but suffice it to say that we know of no case of solution of this machine and system throughout the war, and it is still in service as a high-grade off-line machine. During its use in World War II there was one possible compromise which raised quite a storm when it was discovered that some Frenchman had liberated a U.S. Army truck and trailer -- the latter carrying all the 28th Division's HQ cipher machines and materiel. But the stuff was soon found where it had been dumped in a nearby river who wanted only the vehicles that not their contents. The episode was one which caused the by the Frenchmen in a nearby river Signal Officer and other officers to be tried by court martial. We had and still have 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. I can hardly refrain from telling you one of the funny and wanted things about our not giving the machine to the British when they needed it so desperately. I mentioned the strict rules about safeguarding it -- who could see

Carrie 1

Ú.T

SECRET

the thing, who could service it, and so on, and we saw to it that these rules were strictly enforced. But there came a time in North Africa when all our maintenance men were knocked off and there was nobody to service the machines. However, a very skillful British RAF Officer, an electrical engineer, was pressed into service and he maintained our SIGABAs there for a while. I'm sure you won't be astonished to learn that when he got back to London he built for the RAF a machine based upon the ECM-SIGABA principle!

I want to show you next the cipher machine which was used very extensively 74.1 by all the German Armed Forces in World War II. This was a modification of their commercial Enigma machine but an important modification, introduced when Hitler came into power, at which time the commercial model was withdrawn from the market.

ANDRESSE XXXIII SERVICE REPORT OF THE PROPERTY you can see it better on the next slide. Here are the rotors -- they are exactly the same physically as they were on the commercial model, but with different wirings of course. Now let's see what the modification was -- the addition of a plug board by means of which one could change the connections between the keys of the keyboard and the lamps on the lightbank. There were 13 plugs and jacks and this number was not chosen by accident; they apparently had mathematicians figure out absolutely the best number of plugging arrangements for this particular machine. There were certain weaknesses in the German Military Enigma but the absolutely fatal weakness was that they couldn't, or at least they didn't, change their rotor wirings at all throughout the war. Without the rotor wirings we couldn't have done anything with their traffic; but with them we were able to read practically all of it. The form the control of winder with a military of the control of the contro manuskanok xkon xkin miligite manuski manuski manuski manuski The Naval Enigma was much like the Army and Air Force machine except/is had one more wheel and the rotor wirings were different. Jil come back to the Enigme in the west period. Now we come to the development of cipher machines for teleprinter communithe need for which cations, With the ever increasing speed of tommunications, it was necessary to

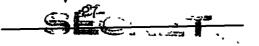
speed up this business of protecting the contents of messages by pryptography.

Lad been recognized even during World Was I.

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 machine to make it a printing-telegraph

56



cipher machine, using circular key tapes of random characters. Great faith
was placed in this machine but it was not put into use until the war was over.

By that time I had come back from France, rejoined the Riverbank Laboratories
and accepted a challenge to solve this kind of cipher system. It's 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 when we had a need for
teleprinter ciphering in the early days of 1942 we actually had nothing except
this thing. The big trouble, of course, was the production and distribution of
these key tapes, and it is a problem which is still with us. Here's an early
model of a machine for making key tapes. We improved such machines very greatly
in the next year or two, so that we could produce hundreds of thousands of good
tapes in a hurry. Our modern key tape manufacturing apparatus uses a key generator.

For producing electronically the random impulses for punching the tapes.

178

.258

This is a rotor machine, the SIGCUM, which the Army developed in 1942-43

which was
and used very successfully to encipher teletype communications. It uses not

perforated tapes but rotors which step in an erratic fashion, but not as erratic

as in the ECM GIGADA. But even while in service, it had weaknesses, every once

in a while, when we discovered new cryptanalytic techniques, we found that SIGCUM

had weaknesses which could be exploited; whereupon we would proceed to tighten up

things by changes in the method of usage or the method of stepping the rotors,

and so on. The machines are still in use, doing valiant service because we were

able to incorporate more and more improved features in it. Its new designation

APPRILEZ.

-28-

Superior and the superior of the superior and the superior of the superior of

Now we have to say a few words about certain other types of ciphering apparatus. For example, it is necessary to send, with security, weather and situation maps, and so it was desirable to have a machine which can encipher and decipher facsimile. The generic name we gave to machines for ciphering facsimile was cifax. Here is one such machine that was developed by Army for the purpose, telephone We also had need for machines for enciphering/conversations, called SIGMEW. machines with the generic name ciphony equipments, here's the first shot at ita development by the Bell Telephone Laboratories, called SIGJIP .- It was a gyp it gave you much more feeling of security then was warranted by the Conversations enciphered by means of that thing could be read. my readily and we all knew this but it was only an interim piece of equipment. The Telephone Company proceeded with its work, in collaboration with engineers from the Signal Intelligence Service and the Signal Corps, and a very high-grade ciphony system which became known as SIGSALY was finally developed and was of which there were seven, extremely successful, Each terminal, cost over a million dollars, and there were

2837

seven of them.

The professional cryptologist is always amused by the almost invariable reference by the layman to "the German code", "the Japanese code", "the U.S. Navy code", etc. To give an idea as to how fallacious such a notion is, I will say that there are hundreds of systems in simultaneous use in the communication services and all large governments. You not only have to have different kinds to meet specific types of communications but you have to divide up the traffic for two reasons?

first, so as not to overload one system beyond the safety limit, and second, so

even if they all have the same machine or crustosystem. that not everybody can read everybody else's messages, even in the same family. There was a look in connection with the Navy's success in the Battle of Midway and the Midway took happened primarily because this last principle wasn't in effect

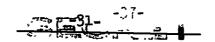
at that time in U.S. Naval communications.

-3ø-

This-slide shows the number of cryptographic systems in effect on 7 December 236 1951 until October 1945 in the U.S. Army alone There were literally hundreds of them. The next slide shows the number of holders of cryptographic materials ' was almost 6,000, during the same period, December 1941-October 1945, and, mind you, this je U.S. the thou U.S. Army and U.S. Army Air Corps alone. It does not consider U.S. Navy, which had nor as great or perhaps greater distributive; the State Department, the Treasury, U.S. government and the many other agencies that use cryptography.

Keeping track of 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 definite and detailed rules for accounting for crypto-material. They were enjoined supposed to burn the codebooks, the cipher keys, the cipher tables, and so on. They were enjoined to scatter the ashes and then make a certificate, witnessed by a fellow officer, as to the complete destruction of the material. -Occasionally these certificates were sent by radio and then we would find a case like this, where two chaps became had certified the destruction by burning and the scattering of one chap the day.

the askes, But was observed by binoculars when he took a spade and dug a hole, dumped the codebooks and the tables in that hole, and poured/some water. mother well, In due time, some of our people sneaked out, dug minime hole, got out the material brought it in metabolisers it is, being dried, out. sort of This recovery of crypto-material helped a great deal because it saved us an and labor and set of tables. enormous amount of time/to reconstruct that particular code/ There were



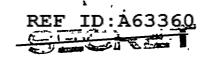
I have already mentioned that

instances of this sort every now and then. By the way, the Japanese were

cryptoworried about this business of their security. They sensed that something very complex and they felt sure of their security. Yet they felt that something about their secrecy systems, was wrong and the only thing the they could imagine We read and were amused by messages was that there were spies all 'round them. There were messages all the time-

requiring the commands to go through their quarters and look under the beds and into all closets, hunting for spies. Of course, that wasn't the case at all; we were solving their codes and ciphers because they were not secure.

You have seen the important World War II developments in crypto-apparatus and now it's time I told you a bit with new ones, conceived, developed and in some cases produced by the now centralized cryptologic agency of the Armed Forces, the National Security Agency. In general the trend has been toward these things:(1) making the machine more manageable as to size and weight, by miniaturization, the use of transistors and other solid state components, and by better packaging; next, by making the machines more secure, by incorporating better or more advanced crypto-principles, and particularly by simplifying the procedures. The aim of this last set of improvements, simplification, is accomplished, wherever practicable, by eliminating as many features and procedures which, because of operators' errors, lead to crypto-security weaknesses. That is, we've been trying to make the machines as nearly and foolproof as possible, as regards their keying and functioning, so as to eliminate weaknesses caused by human error. We must take into account the fact that the machines have to be operated by human beings, and human beings occasionally and inevitably make mistakes, they are prone to errors of omission



and commission. Experience has proved that in the past it has been these errors and not so much technical weaknesses in the cryptosystems and machines themselves that have made solution on a regular basis possible. This sort of practical experience means that the keying procedures should be made simpler, and, if possible, entirely automatic so far as concerns the human operator and user of the machine and system. Complexities can be introduced, incorporated, or applied at NSA, where there are extremely well-trained and experienced cryptoengineers and their helpers.

You understand, I'm sure that we depend for crypto-security not on keeping the construction or design of the machines deep secrets. This means that the machines must be based upon crypto-principles such that even if the machines fall into enemy hands, by capture or otherwise, without possession of the exact key for the day, for the period, or for each individual message itself, the enemy can never learn by cryptanalysis the contents of the messages, or at least he can't for a very large number of years. At the same time there is a real point in keeping the machine appearatus or system itself in a classified status as long as possible, because in the case of well-designed crypto-apparatus if you don't green know what the machine looks like, or its general principles of ciphering, you can't even make a start at cryptanalysis, or, to be more accurate, it will take a considerable length of time and more or less involved study to ascertain what you must know before you can make an attack on the messages with some hope of success. In a nutshell, then, we keep the machines in a classified

some hope of success. In a nutshell, then, we keep the machines in a classified status as long as possible, first, in order to delay the enemy's real attack on the traffic, and second, to prevent a -33- potential enemy from duplicating the machines and turning our own weapons against us.

SPET ID 463360

stabus as long as possible in order to delay the enemy's real attack on the traffic enciphered by the machines. But, of source, there's the other reason, which is already mentioned to prevent a potential enemy from copying our machines and turning our own weapons against us.

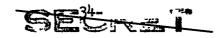
Now let's see pictures of some of the new apparatus, which will soon be seed for issue.

For field use we now have in place of Converter M-209 a small off-line high security machine designated the KW-7. It has a keyboard and prints the cipher text. For electric power it uses any 24-volt source. This machine is now the work-horse for tactical cryptocommunications, and, by the way, several thousands of them have been issued to our NATO allies.

Next we have the KW-9, an on-line or off-line teletype encipherment machine that uses rotors instead of key tapes and is very much safer than the old SIGCUM or KW-2 I showed you. Here we have the new KW-26, which is in fact becoming the work-horse of fixed station teletype long-range communication systems. It is an on-line synchronous teletype cipher system with link-encryption, that is, so far as enemy intercept is concerned it is impossible to tell when the circuit is idle and when it is carrying a message.

This and the next slide are a bit out of order but I didn't have glass slides for them and have to use the small 35 mm. ones. This one showing the [KL-36]KL-36 is the one I mentioned before as having been developed for the Marine Corps.

The next one is the pneumatic rotor machine that we think would serve the needs [KL-17] better than the KL-36 and be far safer.



GECHET

Here's a machine designated the KW-3, now undergoing test. 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. The KW-3 will become the real work-horse of our Armed Forces high-command cryptocommunications.

Next I show the KW-37, designed for Navy Fox or broadcast transmissions, and now undergoing service test. It is a machine which embodies a teletype printer and uses an IBM card for keying purposes. So far as the ship is concerned, the radio operators aboard won't even see the cipher—the messages within the communication center aboard will be in plain language; the ciphering is done elsewhere on the ship. The 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.

Next we have the KY-3, a ciphony or telephone security equipment. It has very high security and excellent quality, and is not a push-to-talk machine.

It's range is 10-15 miles but this can be extended with good repeaters.

Here's the KY-8, a smaller version of the KY-3, occupying less than one cubic foot space and weighing between 10 and 15 pounds. It's for air-to-air and air-to-ground talk with high security.

Next we see the KY-9, a great improvement over its predecessors, one of which was the SIGSALY I mentioned a few minutes ago. It uses the vocoder principle, which yields talk that is intelligible but of poor quality. What it lacks in that respect it makes up by having excellent reliability. Moreover, you can use it on any commercial telephone circuit in the U.S. or circuits of equivalent quality abroad. For comparison as to size I show you again a SIGSALY terminal of World War II days, which cost over \$1,000,000. The KY-9 gives equal security and costs only about \$60,000.

Finally, I show you the KY-11, the crypto-portion of a microwave telephone system. We have this between Fort Meade and our former headquarters at the Navy Security Station in Washington where our COMSEC operations are conducted, and where also is located the Navy Security Group. The telephone micro-link is rented from the telephone company. We also have a similar link between the Navy Security Station and Arlington Hall Station where the headquarters of the Army Security Agency are located.

I'm porry that I can't show you pictures of some of our new machines and amplow it wouldn't do much good unless I explain specifically what they are for they work, and there you is it the formall that I I will say, however, that we now have machines for Extral communications, such as the KL-7, which has a Reyboard and prints the ripher text. It uses any 24-volt source. Several thousand of them have been issued to our NATO allies. We have machines for on-line and off-line telaprenter capturing, and we - have one on-line synchronous teleprenter diplor system with link-everyption, that is, so far as every interest is conserved, it is impossible to talk when the circuit is idling and when a massage is being transmitted.

Next, we have only better differing materials. for protecting telephone communications, there are what we calle siphony systems. I told you a let about SIGSALY of World War II days, teach terminal of which over \$1,000,000, But now we have uphony machines of equal security, which are much much smaller and cost a mere \$ 60,000 a priace. Han we also Rowe Cifax machines, for protecting facomile Transmiss [34.34A-35- 36 out] This is new p. 36

In what I've just showed you'll notice the emphasis placed on telephone security devices and systems, and on automatic teleprinting systems. The days of hand-operated devices is over, and those of semi-automatic off-line cryptographic machines are drawing to a close. And, last to be mentioned, NSA cryptoengineers are doing development work in civision systems—enciphered television—which will doubtless come into use within a few years.

But with all these modern improvements I don't think the day has yet dawned when it can be said that human factors that make for crypto-insecurity have been altogether eliminated. Perhaps it's true that at the moment COMSEC technology can be said to be ahead of COMINT technology; but with ever increasing speed of electronic analytic apparatus the gap can and perhaps will be closed, unless the COMSTC engineers keep pace with that apparatus. In short, it is the age-old battle between armor and armor-piercing projectiles. In the meantime, communicators must keep their guard up and enforce the rules supplied them for operating their crypto-equipments. In closing this period let me remind you, of the following: (1) that the establishment and maintenance of communications security is a responsibility of command; (2) that there aren't any short-cuts to achieving communications security; and (3) that the rules of COMSEC must be followed to the letter by everybody connected with COMSEC but most especially by crypto-operating personnel. If these reminders are followed, the chances are good that you won't learn your COMSEC gules by accident:



With the foregoing remarks T bring to a close my talk on COMINF and COMSEC. If there is any last word or impression that I would like to leave with you let it be that, in my opinion, COMSEC, though less spectacular and less interesting facts of the cruptologic coin.
than COMINT, is by the more important of the two. There are two reasons for this opinion. The first is that asservey in the conduct of modern large-scale military operations, ground, sea, air, and para-military, is of the highest importance to their success; without secure communications there can be little on mo secrecy, and without secrecy nearly every such operation is doomed. The second reason is one that is not so obvious. It is that your COMINT successes will soon be eliminated unless the communications over which the traffic and the final results must pass to reach those who can use them are secure. Therefore, COMSEC is doubly important, case and first, to protect our own plans and movements, and once again, or second, to protect our COMINT product and sources. I'd therefore like to present for your consideration and rumination the following statement of what I'll immodestly call Friedman's Law--something patterned after Professor Parkinson's Law: Your cryptologic coin, like any other coin, has two faces. If you're up against equal or even superior forces, and if the COMINT face of the coin is bright and shiny, your chances of winning are good -- maybe and at times excellent; but if you let the COMSEC face of your coin become tarnished and dull, you'll sure as hell lose.

Thanking you for your patience in listening to my rather lengthy discourse and for your courtesy in paying such careful attention to what I

SECRET

have presented for your information, let me invite hose of you who care to examine some of my exhibits to come up to the table here and we can look at them as long as you wish.