#A ✓

37 Cards ✓

LECTURE NOTE On Communication Security

My subject -- The historical background of COMSEC in the Armed Forces -- is a very broad one because it should include the background of the development of each of the components of COMSEC: cryptosecurity, transmission security, and physical security. But since time is limited and I think you would be more interested in the phases pertaining to cryptosecurity, I will omit references to the history of the other two components. And even in limiting the talk to cryptosecurity, I will have opportunity only to give some of the highlights of the development of the items that comprise what we call our cryptomaterials, leaving out comments on the history of the development and improvement of [illegible] procedures and practices -- all of which are extremely important.

Coming now the the history of our cryptomaterials themselves, I suppose there is no need to tell you of the profound effect of the 19th and 20th centuries on electrical communications -- directly upon military communications and indirectly on military cryptography. Hand operated ciphers and codes became almost obsolete with the need for greater and greater speed of crypto-operations. That meant that cryptomachines would have to be developed.

CRYPTOGRAPHY

Begin 2nd part with brief history of development of cipher machines - with growth of radio and communications - effect on military communications profound - necessity for speed

YAMAMOTO

Accident -- literally, a befalling.

a. An event that takes place without one's foresight or expectation; an undesigned, sudden, and unexpected event.
b. Hence, often, an undesigned and 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 an accident.
c. Chance; contingency.

"Thou cam'st not to that place by accident;
It is the very place God meant for thee."

~~LECTURE NOTE -- COMSEC~~ REF ID:A62873

~~One more contrasting example of poor and good COMSEC. Volume of communications necessary in preparing for large-scale operations on hostile shores is tremendous. The figures staggering, both as to number and length of messages. Take the case of Jap~~ "No. 10 Maneuvers" in early 1944, a large expedition involving redeployment of troops for the Dutch East Indies. Their ship~~e~~ment met with many "accidents" because inadequate Japanese COMSEC disclosed all their plans. the Entire move was delayed 3 months and ~~enemy~~ suffered heavy losses in material and personnel. ~~But take case of TORCH -- not only made in great secrecy (took Germans entirely by surprise) but also their troops (100-200,000) "just happened" to be in the wrong place at the right time.~~

But this did not "just happen" and was no accident -- it was brought about.

LECTURE REF ID:A628073 SLIDE 45

The earliest picture of a cipher disk, from Alberti Trattati in cifra, Rome, c. 1470.

"Oldest tract on cryptography the world now possesses"

LECTURE REF ID:A628 FOR SLIDE 45.1

One of the cipher disks in Porta, 1563

[And apparently nobody thought up anything much better for a long, long time. In fact, not only could they not think up anything better, but those who did any thinking at all on the subject merely "invented" or reinvented Alberti's disk -- and that happened time and again.]

[Have Porta Book with me]

LECTURE NOTE FOR SLIDE 45.2

The Myer cipher disk, patented 14 Nov 1865

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

LECTURE NOTE FOR SLIDE 45.4

The Alberti Disk reincarnated in the U.S. Army Cipher Disk of 1914-18.

LECTURE FOR SLIDE 47

The cipher disk as again patented in 1924 -- Huntington Patent

/Shows that the Patent Office does not have general information on cryptography because of the secrecy involved./

LECTURE

FOR SLIDE 49.1

The Decius Wadsworth cipher device (invented and built in 1817 when Colonel Decius Wadsworth was Chief of Ordnance.)

LECTURE SLIDE 49.4

The Bazeries cryptographe cylindrique (1901) as shown in his book "Les chiffres secrets devoiles"

/But he may have described this in his article "Cryptographe a 20 rondelles-alphabets" Comptes rendus, Marselles, 1891./

LECTURE NOTE FOR SLIDE 160.1

Hitt's earliest model of strip cipher device (15)

LECTURE NOTE REF ID:A62873 FOR SLIDE 50.2

Show M-94

If time tell of failure to solve and why

LECTURE NOTE FOR SLIDE 50

Second page of Jefferson's description of "The Wheel Cipher"

LECTURE **FOR SLIDE 50.5**

U.S. Army cipher device M-136

/Begins experimentation with changeable alphabets7

LECTURE NOTE SLIDE 50.8

U. S. Army Strip Cipher Device M-138.

LECTURE

FOR SLIDE 50.12

U. S. Army cipher device, Type M-138-A (with Russian legends)

[Story of Russian legends and how they came.to be there.]

The Kryha cipher machine

Swedish machine connected to electric typewriter.

LECTURE REF ID:A62873 FOR SLIDE 65

The keyboard electrically-operated B-211 Swedish machine.

/Self-contained, instead of separate typewriter./

LECTURE FOR SLIDE 71.1

The first Hebern machine.

[Manufactured for use by the Ku Klux Klan.]

LECTURE **FOR SLIDE 72**

The 5-rotor Hebern machine

[Story of solution]

W.F.F.'s "work-sheet" solution of Navy challenge messages.

LECTURE NOTE FOR SLIDE 172.10

One of Hebern's developments for the Navy, after his release.

/This is the one that wouldn't work - but Hebern said the contract didn't specifically state that it had to work. He insisted on being paid -- and was/

(One Navy file insisted that Navy had an admiral in Navy District HQ in S.F. just to keep Hebern out of jail so he could finish Navy contract!)

170

LECTURE NOTE REF ID:A62878 FOR SLIDE 50.7?

My theory re external key and development of M134 TI (1932)

U. S. Army Converter M-134-B1

Basic principle - external keying element

U.S. Army Converter M-134-T2 (1936)

The SIGABA/ECM
(Converter M-134-C)

A & N get together. Benefits thereof withheld from all Allies.

LECTURE NOTE FOR SLIDE 56

With growth of teletype communications the need for and practicability of automatic encipherment became obvious.

--- The first attempt -- the machine developed by the AT&T Co. (1918) in collaboration with the Signal Corps.

LECTURE REF ID:A62873 FOR SLIDE 61

The IT&T Co. teletype cipher attachment

/Autumn 1931. With the growth of teletype communications, cipher teletype attachments were invented./

The IT&T Co. Teletype cipher attachment

(Internal mechanism exposed)

Solution story

Effects of lack of contact with work

Lesson re flying pay

LECTURE NOTE FOR SLIDE 178

In 1942 the need for automatic teletype encipherment was met on the basis of expediency: The old AT&T Co. double-tape system was adopted and installed on a "crash" program at the few signal centers, while a large program for the production and procurement of Converter M-228 (SIGCUM) was being executed.

LECTURE FOR SLIDE 171

M-161: Signal Corps model made at Fort Monmouth

(Efforts to develop field machine)

Converter M-209

70.2

Converter M-209 with keying mechanism exposed.

LECTURE NOTE

SLIDE 70.3

Example of American resourcefulness and skill under difficulties. Two GI's in Italy mechanize the M-209.

(The cartoon, showing a couple of GI's with a home-made "still," and the legend: "Yes, but will it work?")