#A

37 Cards

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 crypto-
security, 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 REF ID:A62873 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-
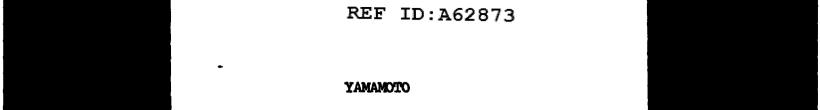operations. That meant that cryptomachines would have
to be developed.

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 befallings

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 occur-
rence 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 <u>accident</u>;
It is the very place God meant for thee."

~~One more contrasting example of poor and good~~
~~COMSEC. Volume of communications necessary in pre-~~
~~paring for large-scale operations on hostile shores is~~
~~tremendous. The figures staggering, both as to number~~
~~and length of messages. Take the case of Japs~~ "No. 10
Maneuvers" in early 1944, a large expedition involving
redeployment of troops for Dutch East Indies. Their
shipment 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.

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

"Oldest tract on cryptography the world now possesses"

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]

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."

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

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./

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

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./

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

Show M-94

If time tell of failure to solve and why

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

U.S. Army cipher device M-136

/Begins experimentation with changeable alphabets/

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

REF ID:A68873   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.7

The Kryha cipher machine

Swedish machine connected to electric typewriter.

REF ID:A62878

The keyboard electrically-operated B-211 Swedish machine.

/Self-contained, instead of separate typewriter./

The first Hebern machine.

/Manufactured for use by the Ku Klux Klan./

REF ID:A62873

The 5-rotor Hebern machine

/Story of solution_7

REF ID:A62873 165

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

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!)

LECTURE NOTE   REF ID:A62878OR 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.

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.

The IT&T Co. teletype cipher attachment

⎣Autumn 1931. With the growth of teletype communi-
cations, cipher teletype attachments were invented⎦

REF ID:A62873

The IT&T Co. Teletype cipher attachment

(Internal mechanism exposed)

Solution story

Effects of lack of contact with work

Lesson re flying pay

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.

REF ID:A62873

M-161: Signal Corps model made at Fort Monmouth

(Efforts to develop field machine)

Converter M-209

Converter M-209 with keying mechanism exposed.

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?")