REF ID: A38382

SCAMP 1958

LECTURE I - Section 2 - 1525 - 1615

Total No. of Slides -16

Approved for Release by NSA on 10-09-2013 pursuant to E.O. 13526
British Cipher Message using
"The true page of the Army List"
Message dated 13 Sept 1781
The New Spelling Dictionary by
Rev. John Entick, London, 1782
The syllabary used by Thomas Jefferson (Extract from decoding section)

[That all 'round genius also may be regarded as being the first American inventor of cryptographic devices -- as will be discussed later.]
Jefferson Syllabary

(encoding) (enveloping)

Typical of the small code systems used at the time.
In addition, code or conventional words to rep. names British used code names in Clinton plus papers following are found:

American Generals = Apostles
    - Washington = James
    - Sullivan = Matthew

Philadelphia = Jerusalem
Detroit = Alexandria
Delaware = Red Sea
Susquehanna = Jordan
Indians = Pharisees
Congress = Synagogue
REVOLUTIONARY WAR PERIOD - Systems used by Americans and by British

Americans -

a. Simple monoalphabetic sub
b. Monoalphabetic with variants by use of long key
   sentence à la Franklin
c. Vigenère with repeating key

d. Dictionaries
   codes
   c. Syllabaries
   )
   Secret inks
   Grilles

British -

a. Monoalphabetic sub
b. Vigenère with repeating key
c. Grilles

(Entick's)

a. Dictionaries
   b. Small alphabetic 1-part codes of 600-700 items
      and code names
   c. Old book such as Black stone - page, line, no. of words in line
Lecture I

[Begin summary of Section 2]

1) 6.31
2) 6.3 [Total: 16 slides]
3) 257
4) 231
5) 2321
6) 243
7) 244
8) 6.4
9) 6.5
10) 6.6
11) 6.7
12) 6.8
13) 69 [A] bar 231 m here (Fowell, Letter)
15) 240
16) 6.10 and Sect 2.5 Lecture I
Revolutionary War Period - Systems used by Americans and by British:

**Americans:**

- **a.** Simple monoalphabetic substitution.
- **b.** Monoalphabetic with variants by use of long key sentence a la Franklin.
- **c.** Vigenere with repeating key

**British:**

- **a.** Monoalphabetic substitution.
- **b.** Vigenere with repeating key.
- **c.** Grilles
Americans:

a. Dictionaries
b. Keybook using words
c. Syllabaries

Codes

Secret inks
Grilles

British:

a. Dictionaries.
   1. Entick’s
   2. Bailey’s
b. Small alphabetic 1-part codes of 600-700 items and code names.
c. Ord. book such as Blackstone - page, line, no of words in line.
LECTURE I

Section 2 - 1525-1615

50 min

Total no. of slides - 16
In addition, code or conventional words to represent names of persons and places. British used code names in Clinton Papers following are found:

American Generals - Apostles (Washington = James (Sullivan = Matthew

Philadelphia - Jerusalem
Detroit - Alexandria
Delaware - Red Sea
Susquehanna - Jordan
Indians - Pharisees
Congress - Synagogue

-3-
Jefferson Syllabary

(Encoding) (enciphering)

encrypting

Typical of the small codes and syllabaries used at the time.

The syllabary used by Thomas Jefferson (Extract from decoding section)

(That all 'round genius also may be regarded as being the first American inventor of cryptographic devices -- as will be discussed later.)

-4-

Line 22
THE GOVERNORS LIEUTENANT GOVERNORS & C OF HIS MAJESTY'S

Line 23
GARRISONS AT HOME AND ABROAD WITH THEIR ALLOWANCES

"No 6"
VERMONT ASSEMBLY IS TO MEET

-2-
The key for the preceding message.

(Finding the key after solution.)

---

WAIT!

Before showing the next slides explain about British cryptanalysts working on American ciphers.
Franklin (Dumas) Cipher-Key Text.
1706-1790.

Franklin (Dumas) Cipher-Encipher Table.

Beale Papers
Benedict Arnold - "James Moore, Edward Fox, Gustavus"
Major Andre - "Joseph Andrews, John Anderson"

(See next card for text.)

Arnold, disgruntled with injustices of Congress, starts off anonymous correspondence, giving information showing he is well-placed. Arnold gets command of West Point. They used secret inks; Bailey's dictionary, word cipher with words out of Blackstone and songbooks, grilles, slips of paper enclosed in specially constructed hollow bullets. Andre captured Sept 1780, writes out full confession and was hanged. Arnold barely escaped to Br. lines (peculiar part of Arnold's treason).

-9-
One of the cipher letters sent by Benedict Arnold to Sir Henry Clinton: 15 July 1780.

"If I point out a plan of cooperation by which Sir Henry (Clinton) shall possess himself of West Point, the garrison, etc. etc., twenty thousand pounds Sterling I think will be a cheap purchase for an object of so much importance."

(Full text - see typewritten sheet accompanying plate 6.5)
Plain text of the preceding message.

Treason against Washington.
Arnold lays a trap for Washington.

Another example of Benedict Arnold's ciphers

Arnold's Treasonable Cow Letter

-ll-
Example of a grille used by British.

LOVELL, James

Congress' cipher expert who managed to decipher nearly all, if not all, of British code messages intercepted by the Americans

** *** *** ***

(To Gen. Greene, cy to Wash.)

Philad  Sept. 21, 1780

Sir:

You once sent some papers to Congress which no one about you could decipher. Should such be the case with some you have lately forwarded I presume that the result -12-
of my pains, herewith sent, will be useful to you. I took the papers out of Congress, and I do not think it necessary to let it be known here what my success has been in the attempt. For it appears to me that the Enemy make only such changes in their Cypher when they meet with misfortune, (as makes a difference in position only to the same alphabet) and therefore if no talk of Discovery is made by me here or by your Family you may be in chance to draw Benefit this campaign from my last Night's watching.

I am Sir with much respect.

Your Friend

James Lovell

'Stop - Don't click Tell about next great landmark--Egyptian Hieroglyphics and Poe.)
But British cryptanalysts also were at work on American ciphers

Tell about collection of Clinton Papers at Clements Library, U. of Michigan. Tell about how an operation went awry because of incorrect solution by British Army Cryptanalysts (amateur) with British Army in America.

Tell about the British Agency who was illiterate.

And about Ellis history. "The Secret Post Office and Office of Decipherer."

Enciphered resolution of the Revolutionary Congress of the U.S., 8 February 1782. -14-
Interest in cryptology in Europe.

Frontispiece of Dlandol Contre - Espion 1793.

Breadboard model of WAC or WAVE Cryptographic Officer
Lecture V
History of the invention and development of Greek devices and machines.

Section 1 - 1 July 1958
2:15 - 3:05  50 min

Section 2  3:15 - 4:05  50 min

100 min
<table>
<thead>
<tr>
<th>Section 1 (35 pages)</th>
<th>Section 2 (40 pages)</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>58.1</td>
</tr>
<tr>
<td>45.2</td>
<td>59</td>
</tr>
<tr>
<td>45.4</td>
<td>68.5</td>
</tr>
<tr>
<td>47</td>
<td>57</td>
</tr>
<tr>
<td>47.1</td>
<td>71</td>
</tr>
<tr>
<td>48</td>
<td>172</td>
</tr>
<tr>
<td>49</td>
<td>71.1</td>
</tr>
<tr>
<td>49.1</td>
<td>71.2</td>
</tr>
<tr>
<td>49.2</td>
<td>71.3</td>
</tr>
<tr>
<td>49.5</td>
<td>172.1</td>
</tr>
<tr>
<td>50</td>
<td>72</td>
</tr>
<tr>
<td>50.1</td>
<td>166</td>
</tr>
<tr>
<td>160.1</td>
<td>172.2</td>
</tr>
<tr>
<td>50.4</td>
<td>172.3</td>
</tr>
<tr>
<td>159.1</td>
<td>172.10</td>
</tr>
<tr>
<td>50.2</td>
<td>170.1</td>
</tr>
<tr>
<td>50.5</td>
<td>170.2</td>
</tr>
<tr>
<td>50.6</td>
<td>170.7</td>
</tr>
<tr>
<td>50.7</td>
<td>170.9</td>
</tr>
<tr>
<td>50.8</td>
<td>172.4</td>
</tr>
<tr>
<td>50.11</td>
<td>172.5</td>
</tr>
<tr>
<td>50.12</td>
<td>173</td>
</tr>
<tr>
<td>51</td>
<td>174</td>
</tr>
<tr>
<td>52</td>
<td>174</td>
</tr>
<tr>
<td>54</td>
<td>174.1</td>
</tr>
<tr>
<td>55</td>
<td>174.2</td>
</tr>
<tr>
<td>17.1</td>
<td>58</td>
</tr>
<tr>
<td>164</td>
<td>57</td>
</tr>
<tr>
<td>70.1</td>
<td>258</td>
</tr>
<tr>
<td>70.3</td>
<td>60</td>
</tr>
<tr>
<td>260.1</td>
<td>178</td>
</tr>
<tr>
<td>260</td>
<td>179</td>
</tr>
<tr>
<td>261-A</td>
<td>180</td>
</tr>
<tr>
<td>261-B</td>
<td>182</td>
</tr>
<tr>
<td>262</td>
<td>183</td>
</tr>
<tr>
<td>262A</td>
<td>183</td>
</tr>
<tr>
<td>186.1</td>
<td>186</td>
</tr>
<tr>
<td>186</td>
<td>186.1</td>
</tr>
<tr>
<td>236</td>
<td>183</td>
</tr>
<tr>
<td>239</td>
<td>182</td>
</tr>
<tr>
<td>129</td>
<td>181</td>
</tr>
<tr>
<td>130</td>
<td>180</td>
</tr>
</tbody>
</table>
Three or four years ago I was asked to give a lecture 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 a slogan concerned with automobile traffic safety rules. The slogan was "Don't learn traffic laws by accident!"

I thought the slogan useful as the title of my talk, but I modified it a little. I began my talk by reading Webster's def...
I know, of course, that this group here today is not concerned particularly with COMSEC duties of any sort. 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'll read Webster's definition if you'll bear with me.
Webster: "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 effective or unfortunate character; by a mishap resulting in injury to a person or damaged to a thing; a casualty; as to die by an accident.
Having defined the word, let's now proceed by relating an interesting, minor, but nevertheless quite important episode of the war in the Pacific Theatre during WWII, and I will introduce the account of that episode by saying that.
3 During the war, the President of the United States, Commander-in-Chief of the Army and the Navy, the Chief of Staff of the Army, the Commander-in-Chief of the U.S. Fleets, and certain other high officers of 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 across or over enemy or enemy-occupied territory—they met with no "accident". On the other hand, the Japanese Commander-in-Chief of the Combined Fleet, Admiral Isoroku Yamamoto, the man who was maligned by erroneously attributing to him a 1941 statement to the effect that he was "looking forward to dictating peace terms in the White House", (he actually said something of quite different import, viz, that in embarking on a war with the U.S. the Japanese would have to visualize
that its end could come only if they could dictate peace terms in the White House), went on an inspection trip in April 1943, the sequel to which may be summarised by an official Japanese Navy Department communiqué 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."

4. As is often the case, the communiqué didn't 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 remember who first used the vivid description, but it's decidedly applicable in this case "accidents don't happen—they're brought about!" Our Navy communication intelligence people were reading the Japanese Navy's high command messages in Yamamoto's schedule to the day,
Webster:

"Accident — literally, a befalling.

a. An event that takes place without one's foresight or expectation; an unintended, sudden, and unexpected event.

b. Hence, often, an undesigned and unforeseen occurrence of an unfortunate or unfortunate character; a mishap resulting in injury to a person or damage to anything; a casualty or to die by an accident."

__________
The key for the preceding message
[Finding the key after rotation]

Wait!
Before showing next two slides,
I would like to explain about British cryptanalysis
working on American ciphers.
Franklin (Dumas) Cipher - Key Text
1706-1790
1706-1790
Franklin (Dumas) Cipher-Encipher Table

Beale Papers?
Benedict Arnold - "James Moore, Edward Fox, Gustavus"

Major Andre - "Joseph Andrews, John Anderson"

Arnold, disgruntled with injustices of Congress, start off anonymous correspondence, giving information showing he is well-placed. Arnold gets command of West Point. They used secret inks; Bailey's dictionary; word ciphered with words out of Blackstone and songbooks, grilles; slips of paper enclosed in specially constructed hollow bullets. Andre captured Sep 1780, writes out full confession and was hanged. Arnold barely escaped to Br. lines (peculiar part of Arnold's treason)
One of the cipher letters sent by Benedict Arnold to Sir Henry Clinton:— 15 July 1780

"If I point out a plan of cooperation by which S(ir) H(enry) (Clinton) shall possess himself of West Point, the garrison, etc. etc., twenty thousand pounds Sterling I think will be a cheap purchase for an object of so much importance."

(For full text see typewritten sheet accompanying plate 6.5.)
Plain text of the preceding message

...
Treason against Washington.
Arnold lays a trap for Washington.
1) Another example of Benedict Arnold's cipher
2) Arnold's Treasonable Correspondence
3) Example of a grille used by British
The Benedict Arnold Indecipherable Cow Letter
Example of grille message (British)
LOVELL, James

Congress' cipher expert who managed to decipher nearly all, if not all, of British code messages intercepted by the Americans."

Sir:

Philad. Sep. 21, 1780

You once sent some papers to Congress which no one about you could decypher. Should such be the case with some you have lately forwarded I presume that the result of my pains, herewith sent, will be useful to you. I took the papers out of Congress, and I do not think it necessary to let it be known here what my success has (OVER)
been in the attempt. For it appears to me that the Enemy make only such changes in their Cypher when they meet with misfortune, as makes a difference in position only to the same alphabet and therefore if no talk of Discovery is made by me here or by your Family you may be in chance to draw Benefit this campaign from my last Night's watching.

I am Sir with much respect

Your Friend

James Lovell

[Signature]

Stop - Don't click.
Tell about next great bandana.
But British cryptanalysts also were at work on American ciphers -

(Extract from Ellis history here.)

Tell about collection of Clinton papers at Clements Library, U of Mich.
Tell about how an operation went away because of incorrect solution by British Army cryptanalysts (amateur) with American
Wait!

1) And tell about the British agent who was illiterate.

2) And about Ellis's history, "The Secret Post Office and Office of Decipherer."
Enciphered Resolution of the Revolutionary Congress of the US 8 Feb 1982
Interest in cryptography in Europe

1) Frontispiece of D'Landol
   Contre-Espion 1793

2) Breadboard model of WAC or WAVE
   Cryptographic Officer

3)
Dlandol frontispiece (a cryptographer at work)

His assistant -- early model WAF
FRONT

Lectures 1, 5, 7
SCAMP 1958

LECTURE I - 24 June 1958

28 slides Section 1 - 1415 - 1510 55 minutes

16 " 1 2 - 1525 - 1615 50 "

\[ \frac{16}{44} \] (Total no. of slides 28)

\[ \frac{16}{44} \]
LECTURE I - Section 1 - 24 June
1. Appreciate opportunity to participate in SCAMP '58 and to talk a bit about some of the interesting episodes and important landmarks that stand out in the historical background of the science and art of cryptology.

2. On inviting me to speak on that subject I assume that the objective is to deal with that area of the background of cryptology which has primarily to do with the development and manner of employment as a vital military weapon.
3. Now cryptology has certainly not always been considered a vital military weapon, or even as a weapon. For instance, even as recently as in 1955, when the U.S. was trying to help our most important ally in the cultivation of the cryptologic garden by providing her with the money for the purpose I mentioned just a few moments ago, we sought to use funds allocated to MADAP—the Mutual Defense Assistance Pact. But those funds are specifically earmarked for research and development.
of physical instruments, machines, 2
glue, electronic devices, etc., and it
seemed hopeless even to try to justify
the use of NDAP money for cryptanalytic
research and development. It was
only after we had been pointed out the
ways in which military cryptology had
been used in World War I and II that
the funds sought were granted
4. This point about cryptology being
useful only for such relatively unim-
portant things as personal diaries, love
musings, and attempts to prove that Bacon or somebody else wrote the Shakespeare play. It reminds me of a story which may be a bit apocryphal but is somewhat amusing.

5. The Story of the Old Persian Queen Semiramis.
Stay, weary traveller!
If thou art footsore, hungry, or in need of money -
Unlock the riddle of the cipher graven below -
And you will be led to riches beyond all dreams of avarice!

O, thou vile and insatiable monster! To disturb these poor bones!
If thou had'st learned something more useful than the art of deciphering,
Thou would'st not be footsore, hungry, or in need of money!

Many times during course of last 30 years I've had occasion to wish I knew the old gal's present address so that I could put as a 1st Ind. to her basic communication the single word "Concur!"
1. Appreciate opportunity to talk to students and faculty of Electronics Division of Air Command and Staff School of USAF Air University.

2. In inviting me to speak on subject "Communications Intelligence" it was indicated that "the objective is to create an awareness of the background, development and manner of employment of this vital military weapon.

3. COMINT not always regarded as "vital" or even as a "weapon". Story of Semiramis (over) (Well, anyhow it's been an interesting life!)

---

Read extract from THE of 17-Dec-45.

Extract from R.H. report (next card)
It is planned that I give a series of talks on the highlights of cryptologic history. This may be useful at least to some of the members of DISCAMP '58, for I may tell you right away that there doesn't exist a straightforward, adequate, or even a fairly good history of the invention and development of cryptography and its counterpart, cryptanalysis. There is no real history, definitive and detailed.
bits and pieces one finds here and there in popular accounts are generally full of misunderstandings, mis-statements and downright lies.

Of course there is a good reason why no history of cryptology worthy of that name has been produced for public use. It is that as a rule governments don't publish them or permit its cryptologic workers to publish histories, brochures or articles. This is an understandable and sensible rule if not carried to absurd
and illegal limits by insisting that all COMINT must be kept secret for all time. Later on I may tell you about an anni-

if not enlightening conference I was summoned to attend at the Pentagon a week ago today.

Of course, now and then some crypt-

logic information does leak out, as for ex-

ample, when congressional and other official investigations either require or accidentally discover a-

suggestions about the disclosure
of such information; or when some formal trust worker commits underscrption, or
conscious, and deliberately breaks the trust that had been imposed. Of both
these types of security breaches—official or personal—I shall have more to say
later on. At the moment I will merely comment that the history which comes
from such leakages and breaches of trust are apt to contain errors,
ununderstanding, distortion, and lea,
Some if you may have wondered what the title of my talk or series of talks is. Dean Swift-Jackson asked me yesterday to tell him so that it could be indicated on the announcement sheet. I told him I preferred to state the title myself and let him disclose my secret by telling you that the title is, "The Influence of C-Power on History."

Best there be some here who think it laboring under the delusion that their CAMP are US Navy property or that their C's suddenly went psychotic and
Imagine Sir Admiral Mahan, I hasten to explain that the "C" in the title of my talk is not the word "SEA" but the letter "C" and it stands for the word CRYPTOLOGIC. The title of the talk is therefore "The Influence of Cryptologic Power on History." As a subtitle I offer this: "Or how to win battles and wars and go down in history as a great tactician, strategist and Censor of Men; or, on the other hand, how to lose battles and wars and go down in history..."
as an incompetent commander, a 'j
heel, a 'no-good-nike.'

At this point let me hasten to deny that I'm stating any reflections upon certain successful—spectacularly suc-
cessful commanders—such as Field
Lieutenant and MacArthur. But names
will occur to you without my calling
them to your attention—and there will be names of men in each of the
two categories of 'how to win' and 'how
to lose battles and wars.
At this point, Jim remembered of a story about General Montgomery—“Monty” and I have the story on pretty good authority.

Story re Monty at N. Africa, 1942

Before a group such as this, I think it hardly necessary to make this general statement but I'll make it: That not all historians know that the history of diplomacy and warfare seems with justification, where the term fobents was greatly...
affected by the relative cryptologic power of the opposing forces. Most of the history in the history books, when first written, does not tell the complete story or the whole truth -- for the cryptologic facts are usually very carefully hidden from historians and are not brought to light for decades -- sometimes for centuries, or maybe never. Tell about (i) Mission (Sword) Elst, (ii) Navy Op Research on Battle of Atlantic, (iii) Navy Lecture at Naval War College.

Sometimes the course of history is materially or drastically changed by the existence of COMINT, or it could have been changed by its proper use -- as some say about the COMINT available to us before Pearl Harbor; but sometimes, also, the course of history is materially changed by the non-existence of COMINT where it had previously existed and was used. We will discuss an incident of the latter type, too, in due course. But first, an incident of the former type -- Pearl Harbor time.
My talk will be divided into three sections, and the title of the 1st is: "The influence of C - power on history."

Lest there be some in my audience who may fear that I have forgotten I am speaking at the Air University and not at the Naval War College, I hasten to say that I am not laboring under the hallucination that I am Admiral Mahan, or Mahan's ghost; in the "C" in the title of this section of my talk stands for "Cryptologic" — "The influence of Cryptologic Power on history."

It hardly necessary to say more than this. That it has been

(OVER)
I will begin by reading from the 17 December 1945 issue of Time. The war was over—or at least VE and V-J days had been celebrated—and the clamor on the part of vociferous Republicans, who insisted upon learning and disclosing to the world the reasons why we had been caught by surprise, had been met. It could no longer be brushed by the need for military secrecy. So there were investigations—half dozen or more—winding up in a grand finale of the joint congressional investigation into the attack on Pearl Harbor. It was this investigation which not
Some of you may have wondered what the title of my talk or series of talks is and. Get now disclosed this secret by saying, telling you, that it is "The influence of C's power on history.

First there be some here who think I'm talking under the delusion that I'm talking of some U.S. Navy installation and the Naval Academy or the Naval War College, that after Admiral Mahan re-encarnated in the city in which there are many people who believe in reincarnation. Well, let's say that the "C" in the title of my series, it talks is not the word "SEA" but the letter "C," and it stands for the word "CRYPTOLOGIC." The title of my talks is, in short, "The influence of cryptologic power on history."

As a subtitle I might say: Before a group such as this one I think it is
only itself brought into the open every detail and exhibit in its own lengthy investigation and hearings but also disclosed everything that was said and shown at all the previous Army and Navy investigations—about a half dozen years ago.

There came a day in the Congress when General George C. Marshall, Chief of Staff, U S. Army at the time it was called the "West Point" attack was called to the witness stand. He testified for several days, long ones. Toward the end of the ordeal of
he was questioned about a letter it had been worked out to Governor Dewey in the autumn of 1944, during the Presidential Campaign. General C. D. Marshall balked. He pleaded not to correlate with the Committee not to force him to disclose the letter or its contents, but to no avail. He had to bow to the will of the Committee.

Read TIME to "Uneasy Secret"
A few moments ago I commented that the sort of cryptography history which gets published as a result of official investigation is apt to contain errors, misunderstandings, distortions, and downright lies. And this account in TIME contains its share of them. But the curious part of this story is that TIME didn't commit these Offences; they were in the original letter Marshall-Berry letter, which had been prepared by somebody in Marshall's staff who got the results of CONEX but was no technician in cryptography.

I explained that part of the story in the Marshall-Berry letter and in the account of it in TIME magazine.
(to remarks about undoubtedly, we saw the disclosures from the front of thePearl Harbor and then again in a couple days, which gave us a chance to see the Americans on the ground. He asked, do you want to know about the Pearl Harbor attack, we were really surprised by the amount of casualties we had. We wonder if the Japanese had good intelligence, and we try to find out more information about the Japanese intentions."

Ref ID: A388382
Page 4 Majority Report (30 July 1946):

"Intelligence available in Washington (MAGIC)

"With the exercise... etc.

The Committee has been interrogated..."
See return letter to the Marshall - Dewey corres-

pionence. But now

What was meant by the name "MAGS"?

How did the term come to be used?

It was introduced into our usage by the Bri-

It was the cover name during the WWII year

for the product of CEMINT operations and activities:

1) Special intelligence
2) Traffic intelligence
3) Sp weather intelligence

I suppose it hardly necessary for me to tell

you how carefully guarded were the fruits of the

MAGC - even the fact of its existence was known to

only a very few persons. Success rather than continuity

Midway, for instance - Marshall, Dewey, th

went "C Red machine" OSS in Lebanon.

There are many persons who still argue about the future of books. Even so often the story comes up and the fires of controversy are fanned again to the blazing point. (A research at RAND is still working on a rather lengthy treatise on the subject.) The right-wingers are, of course, still convinced and are trying to convince other Americans that President Roosevelt brought the attacks about and deliberately some of them make shocking charges and allegations of conspiracy among Roosevelt-Marshall and Stark. Which of course is nonsense-despicable by rather easy logic. Maybe I'll go into this later if you wish. But now let's get back to the Marshall-Drewry.
The reason that the disclosure of this letter caused so much concern with respect to national security is unacknowledged. The hearings were open and the documents (40 volumes) are public documents.

Should we be greatly astonished that certain governments have greatly improved their communications security devices and arrangements since the close of the Congressional investigation?
I read now from p. 232 of the Majority Report of the
Congressional Committee.

1) "... all witnesses familiar with Magic material,
throughout the war have testified that it contributed
enormously to the defeat of the enemy, greatly short-
eved the war, and saved many thousands of lives."

2) General Chamberlain (473 of Gen. MacArthur's staff thought
the war in the Pacific) told me (the part of an existing for me on
request): “The information of V-2 gave 63 in the Pacific
Theater alone saved as many thousands of lives and
shortened the war by no less than two years.”

3) I hardly need say what the latter saving alone was
worth in billions of dollars. I made a calculation
and found that $1 is spent for COMPUTER = $1,000 spent for other
war material. A war
When we had and didn't have COMINT on our side in our struggle against two very desperate enemies, the Germans and the Japanese, it was definite. COMINT, the so-called magic which meant the difference between help and success when we had magic we could put what little we had at the right time in the right place and when we didn't have it - as in the famous and almost totally disastrous Battle of the Bismarck Sea - we took a bad beating.

- REPLY from Letter -

When we didn't have it - well, as I said, things went badly because our principal J-25 had come to rely too heavily on it.

The Battle of the Bismarck Sea, article.

Read
1. Show 1st page of Baldwin article
2. Read from next card - Morgan
3. Then read extracts from p 40
"According to Eisenhower's personnel officer, American losses in the Battle of the Bulge totalled 76,890 men, of whom 8,607 were killed, 47,139 wounded, and 21,144 missing. Over 8,000 of these casualties were in the 106th Division. Because of heavy German attacks, 733 tanks and tank destroyers were lost. Two divisions, the 28th and 106th, were nearly completely annihilated, although the 28th Division did subsequently enter combat after being rebuilt."
Perhaps I've not tired you out by such a lengthy preface to the real substance of my talks, so as to ask:

Which came first — secret writing?

Or plain-text writing?

The art of writing probably grew out of pictographs and its growth can be traced back to the dawn of civilized man.
marshalls - dewey photo
Example of rebus (p. 2)
Cryptanalysis - and psychoanalysis - in the Bible.

Nebuchadnezzar and his dream
Daniel Chapter 2, 3, 4, 5, 6, 7, 8, 9, 11
Belshazzar - 11:5; 1-5, 25-30
Cypher
Reed from Bible - Daniel
Mene, Mene, Tekel, Upharsin
Belshazzar & "The Handwriting on the wall"
Daniel - The First Cryptanalyst (BC 570-569)
"Second Psychoanalyst or Interpreter"
Instances of actual cipher in the Bible:
Jeremiah 25.26
57.41
Instances of cipher in the Bible

Jeremiah 25:26
51:41

Scytale
Scytale

Wait - see next card
Some history from B.

Manual of Cryptography

Scytale - Spartan Phians send messages to enemies in field.

Example from Spartan history. Satak court of Persian King Darius - message to colleague Aristogoras in Greece. Conveying info in wartime by bundles of ribbons of different colors, notches on
stroke, knots tied in various ways. Fires or beacons—all nations. Of antiquity Polybius describes system used by Greeks. Coordinate system—pro divided into groups of 5 and the number of fires let in two separate places denoted the group of letters at the position of the letter in that group. Fires as late as 1746 in Italy to signal code given to General the Marquis de Mirepoix and worn corps. Fr. Sp. & Germans troops in existence in Africa—vectors in drums—only chiefs of tribes
Caesar's cipher - invented many centuries earlier in various countries - by Carthaginians and Phoenicians. Used by Germans in 1870-71 and by Boers during S. African War.
The only systems known to have been employed between the time of Julius Caesar and the beginning of the 16th Century were two:

1) System in which consonants remain unaltered but the vowels are replaced by the immediately following consonant.

2) System in which consonants remain unaltered but the vowels are replaced by the immediately following consonant.
For many centuries after Roman invasion
by cryptos almost entirely neglected, one
reason being that the art of secret writing
was long regarded as an invention of the
Evils. And there are many instances of
students of it being accused of sorcery,
among whom may be mentioned Trithemius
the Abbe of Spanheim. P 6 - Br. Manuel
of Cryptography. Read
Great between Count of Spain
Henry IV (1553-1610) and chief anti-Royalists in France

REF ID: A38382
RUNES on a stone in front of Gripsholm Castle near Stockholm

As "Rune" - "a secret, a mystery", "Magic".

Any of the characters of the alphabet formerly in general use by the Teutonic, or Germanic, peoples from about the 3rd Century A.D.

Blocked out portion - another type of "Runes"
Beginnings of modern cryptology can be traced back to the days of the early years of the 15th Century, when it was extensively employed by the princes and chancellors of the Papal States. For example, see this alphabet of 1401!
Cipher alphabet of 1401

But recently there came into my hands a book devoted to setting forth in detail the cipher used by Philip II of Spain, who reigned from 1180-1223 long before 1401.
Scytales
Trithemius 1518
Abbe' of Spanheim
Trithemian Oath

Present oath

Back up by P. L. 513 - now
18 USC 798
We administer a special oath to everybody who comes into the field -

Back it up with

PUBLIC LAW 513 now 18 USC 798

1st Slide
Examples of cipher alphabets and small syllabaries used centuries ago.

1) Charlemagne's cipher (768-814) [871-901]
2) Cipher used in England during reign of Alfred
3) Ogam writing of ancient Eire
4) Ogam-like alphabet of Charles I (1646) to Marquis
5) Marquis of Worcesters "Clock Cipher"
6) Cardinal Wolsey, 1524, Vienna
7) Sir Thomas Smith, 1563
8) Sir Thomas Chaloner, Madrid, 1561
9) Sir Edward Stafford, Madrid, 1586
Cipher alphabet in Sir Thomas More's *Utopia*, 1518
Facsimiles of a cipher found among the papers of Mary, Queen of Scots (1542-1587)
Ciphers alpha Keeper Queen Mary & Bishop of Glasgow
then her ambassador or solicitor in France. 1571 3.7

3.7 Sliding card ciphers Jassamblé (one used in the later years of Elizabeth's reign (about 1600) 3.8

3.8 The two-word square cipher. State cipher used in Charles I's time (1625) for communicating
with France and Flanders. (A co-ordinate system.) 3.9

3.9 Part of Duke of Buckingham's cipher used in 1627 3.10

3.10 Part of Charles II between France Rupert and the
Earl of Arlington for communicating with France (1630-1655) 3.11

3.11 Numerical ciphers used in reign of Charles II. Between
France Rupert and the Earl of Arlington. See State
Foreign Office Cipher during reign of George III 1779
Frontispiece of "The Babington Plot" by Alan Gordon Smith, London 1936. The Cipher used by Mary, Queen of Scots with Babington, [1542-1587]

Frontispiece of "The Babington Plot" by Smith. The Forged Postscript, with Phillip's Engraving.
Ciphers involved in the Burlington Plot
The forged postscript
But monoalphabetic ciphers still used today!

Gustav Reinach spy case
Porta's Table (1563)
Porta's table as it appears in an early Elizabethan State paper.
Vigenère Square as pictured in the ordinary literature
Vigenère Square as V. describes it in his book 1586
Ciphers used by

Galileo (1564-1642)
Italian astronomer & physicist

Huygens (1629-1695)
Dutch mathematician, physicist, & astronomer
One of earliest instances of the advantage gained in the course of military operations by the capture and subsequent solution of a message sent by the enemy took place in 1626.

George II, Realmont, seized by the enemy, then in possession of the Augustine, but besieged by the King's troops under command of the Prince de Conde.

The latter about to pass Rossignol reads, Out of which I would have to surrender if not immediately resurr.
End of 1st section Lecture I

2.15 to 3.10 = 55 minutes
Navy's highest command messages; they knew the day and time that Yamamoto would leave Truk, the time he would arrive at Buka and leave Buka for Kahili or Ballale, what his escort would be and so on. It was relatively easy to bring about the "accident". Our Commander-in-Chief journeyed with safety because the communications connected with the various trips were secure; the Japanese Commander-in-Chief journeyed in peril because the communications were insecure. His death was no accident in the dictionary sense of that word; it was brought about.

I will close this introductory comment by noting that the Yamamoto "accident" is an excellent example of highly effective teamwork between the Navy and the Army Air Force in World War II. In this particular case the Navy obtained the intelligence and set the trap; the Army Air Force sprang it.
5. The Yamamoto precedent 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, Chapter III, pp 56-57.

The formal surrender took place on the deck of the U.S.S. Missouri in Tokyo Bay on September 2. 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 Isoroku Yamamoto, the Japanese naval commander-in-chief and architect of 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 (OVER)
of the work of the cryptanalytic divisions, and it brought an anguished cable from the intelligence unit already engaged at Yokohama in the interrogation of Japanese naval officers: "Yamamoto story in this morning's paper has placed our activities in very difficult position. Having 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 face of this disclosure he would have to commit suicide. The cable continued: "This officer is giving us valuable information on Japanese crypto systems 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. . . ."

(CONTINUED ON CARD 2)
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 five thousand six hundred ninety two. All of 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."

The formal surrender took place on the deck of the U.S.S. Missouri in Tokyo Bay on September 2. 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 Isoroku Yamamoto, the Japanese naval commander-in-chief and architect of 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 divisions, and it brought an anguished cable from the intelligence unit already engaged at Yokohama in the interrogation of Japanese naval officers:

"Yamamoto story in this morning's paper has placed our activities in very difficult position. Having meticulously concealed our special knowledge we now become ridiculous." They were even then questioning the Japanese officer who had been responsible for those codes, and he was hinting that in face of this disclosure he would have to commit suicide. The cable continued: "This officer is giving us valuable information on Japanese crypto systems 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: "Your lineal position on the list of those who are embarrassed by the Yamamoto story is five thousand six hundred ninety two. All of 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:

[Next two cards]
"Rear Admiral Tomekichi Nomura, the last CNC in the Japanese Navy, said:

'...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 the loss of the war. We failed in communications.'"
"... Our Navy was being defeated in the battle of radio waves. Our cards were bad, and the enemy could read our hand. No wonder we could not win in this poker game!"

YOKOI, Toshuyuki - The Story of the Japanese Naval Black Chamber.
Books recently published in Japan by former Japanese military and naval officers come out quite openly with statements attributing their defeat to poor COMSEC on their part and excellent COMINT on our part. Read from Midway book
Let you infer that our side didn't meet with any COMSEC "accidents," let me say that we had plenty—but these were most attributable to certain weaknesses in our COMSEC devices, machines, and rules but to human failure to follow the rules implicitly. Or—and this hurts in saying it—to weaknesses in the COMSEC devices, machines, and rules of some of our allies.

Take, for instance, the heavy losses the U.S. 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 doing work, and people at that, they knew exactly when and where our bombers were loaded! 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 leads to the 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 overpowering desire to continue to read friendly traffic by cryptanalytic operators when one knows that that traffic should be made secure against one's enemies! —over—
Thus far, no real psychodynamic cure has been found for the illness. The powers that be have decided that COMINT interests will always supersede 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 may add that U.S. and U.K. physicians collaborate very closely in treating their own patients for the cryptologic schizophrenia and in applying remedies where possible.
Today we are going to see some slides which will illustrate important milestones in the history of the invention and development of cipher devices, cipher machines, cipher apparatus, and of course, rules for establishing and maintaining COMSEC.

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 subsequent to the discoveries over.
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 mechanical, mechanical-electrical, and now, to electronic machines. As mechanization and automation progresses in civilization, similar progress has to follow in communications, especially in military, naval, air, and diplomatic communications.
The earliest picture of a cipher disk, from Alberti
Trattati in cifra, Rome, c. 1470

"Oldest tract on cryptography the world now possesses"
The Myer desk, patented 14 Nov 1865
He is a patent on the US Patent Office, granted in 1991, and is prepared along with the present document. The patent is available upon request, and the person receiving it must be aware of its legal implications.

Somebody once asked if the very rare bluebird found in a particular area was included in the patent. The patent is written to include all rare birds, but the person receiving it must be aware of its legal implications.

A recent acquisition by a company in the area has led to a patent request. The patent is written to include all rare birds, but the person receiving it must be aware of its legal implications.
were alive to contest this patent, issued in 1924, for a cipher disk practically identical with Alberti's disk of 1470.
The cipher disk was again patented in 1924 -- Hunting-тон Patent.

Shows that the Patent Office does not have general information on cryptography because of the secrecy involved.
Cypher desk used by Nazis in 1936
Original Wheatstone cipher device (invented and described in 1879)

First improvement on the Alberti disk

I have one here. [Show it.]
The Modified Wheatstone cipher device

Produced by the British Army 1917-18 but never used because of solution by Wm. F. Friedman -- story of solution.
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 "Cryptograph a 20 rondelles-alphabets" Comptes rendus, Marselles, 1891/
Bozere, Étienne
First page of Jefferson's description of "The Wheel Cipher"
Second page of Jefferson's description showing his calculation of the number of permutations afforded
Original model of Hitt's step cipher ("The Star Cipher").
Parker Hitt's model of strip cipher (1916)

Story of solution at Riverbank Laboratories of test messages prepared by Mrs. Hitt.
The first six messages of their
Plain texts of Mauve’s set of
25 challenge messages
U.S. Army Cipher Device M-94.
Early attempts to use cylindrical cipher device principle but with variable alphabets (M-136)
(M-137) 50.0
(M-138-T1) 50.7
(M-138) 50.8
(Folding M-138) 50.11
(Roman capitals) 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.
1) European model 1 step cipher
2) "disassembled"

Law: step cipher

Court awards £35,000 to "inventor"
The Kryha cipher machine
A German mathematical dissertation on the Kryha

Merely number of permutations and combinations a
given machine affords like - has nothing to do with
the case or at least not much. Depends on nature
of permutations and combinations, what they are
cryptographically. For instance, the principle
of monoglphabetic substitution as in Gold Bug -26!
cipher alphabets or the large number:
\[
\frac{403,291,461,126,605,635,584,000,000}{\text{quad/trillions/billions/millions}}
\]
Estimated would take 1000 million men working a
thousand million years to do the major part of wri-
ting these alphabets out --scroll would reach from
earth beyond the planet Mercury!
261 =
Four hundred and three quadrillions;
two hundred ninety-one thousand four
hundred and fifty-one billions;
One hundred twenty-six thousand six
hundred and five billions;
Six hundred thirty-five thousand five
hundred and eighty-four millions —
"and a few!"

Stop! Don’t quote History if votes.
All the preceding examples of cryptographic cards are in the category of what may be termed "pencil and paper" or "hand-operated" aids. These, of course, had to give way to more rapid and more secure means for crypto-communications, and this meant machines of one sort or another.
There was pressing need in the military and naval services for two machines.

1) A small machine for low echelon or field use.
2) A larger machine for rear echelon and high-command use.

Let's take up the first of these two types.
M-161: Signal Corps model made at Fort Monmouth

(Efforts to develop field machine) tell story re obsolescence of S. C. Labs.
Note power source
Boris C.W. Hagelin

Does a "hysteron-proteron" in inventing C-367
LECTURE NOTE

Converter M-209
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?")
Hagelin CX-52
Double tape-printing
Key-wheels removable
Irregular stepping
Non-guaranteed cycle
Hagelin CX-52
[and its fundamental weakness]

Next card
The big problem in the use of devices and machines which are of the key-generator or additive (or subtractor) type is the fact that when the alphabets involved are known alphabets, solution of a depth of two is generally possible.
Example of solution of polyalphabete encipherment with book-key and known alphabets, in this case reversed standard.

Continuation
Hagelin (M-209) Solution.

"A depth of two"

Stop! Don't check! Next card

We come then to the so-called rotor machines, which are not based upon key-generator principles but are permutation machines.
We come now therefore to (Hebern) History of rotor machines
The Swedish electrical machine B-21

Original Aktiebolaget Cryptographe B-21. Mention Boris C.W. Hagelin/
Swedish machine connected to electric typewriter.
The keyboard electrically-operated B-211 Swedish machine

(Self-contained, instead of separate typewriter.)
The original (commercial) Enigma cipher machine

Later used with one improvement by Germans in World War II
Come now to American developments

Edward H. Hebern

He became interested in cryptography and invented a cipher machine.
The first Hebern machine

Manufactured for use by the Ku Klux Klan
The first Hebern printing model
still a one-rotor machine!
Where did he get the idea of
cascading rotors?
Helium rotors - variable wiring possibilities!
13 to one pole & 13 to other
3-rotor Hebern
Hebern, Edward H.

[How he came to invent machine]
LECTURE

The 5-rotor Hebern machine

Story of solution? with next slide 165—
First Hebrew machine built in accordance with Navy specifications.
Hebern model 51.5
solved on challenge by Navy
One of Hebern's developments for the Navy, after his release. Solenoid operated design built according to Navy specs.

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!

It was last job he did for Navy.

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

No! Don't click on 2nd card 1st!
Navy has enough of Hebern and goes in for its own development.

15 years later Hebern Co. & heirs institute suit in U.S. Court of Claims for $50,000,000! Probable settlement by now for five thousand dollars.
Collaboration and cooperation between the Army and Navy on cryptographic research and development notable for its absence in those days. Each service had its secrets!
U.S. Army Converter M-134-T1

Basic principles - external keying element
Converter M 134

Rear view
Comceptor H 134 -
with printing
U.S. Army Converter M-134-A
Original Navy Mark I ECM

With Bonded wires!
And only 15 starting points!
First production model of Navy Mark I
Army & Navy finally collaborate

SIGABA - ECM

Withheld from British until 1953

Battles to give to
SIGIVI on BASKET
SIGABA - ECM withheld from British.
Battle to give to British.
Finally given in 1953.
But during WWII had to communicate.
Therefore the CCM.
SIGIVI – Explain principle.

Stop! Don't click! See next card.
The German Armed Forces cipher machine of WW II

Effects of solution

German lack of imagination! High speed machinery could do it but they lacked the imagination!

Say, don't check. Say dent word about America. Developman aut.
German 8-wheel printing
Enigma
Captured in 1945 at Maffels
A failure!
German Naval Enigma —
differences between the Army & Air Force
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 AT&T Co. printing telegraph cipher machine (1918) (The original SIGTOT!) 

[Story of solution]
Ex Order 26 Aug 45
Put in sequence in preface to Pearl Harbor account - introduction.
1. Appreciate opportunity be participant of SCAMP '58 and to talk a bit about some of the interesting episodes and important landmarks that stand out in the historical background of the science and/or art of cryptology.

2. In inviting me to speak on the subject I assume that the objective is to deal with that area of the background of cryptology which has primarily to do with its development and manner of employment as a vital military weapon.

3. Now cryptology has certainly not always been considered a vital military weapon, or even as a weapon. For instance, even as recently as in 1955,
when the U.S. was trying to help our most important ally in the cultivation of the cryptologic gardens by providing her with the money for the purpose I mentioned just a few moments ago, we sought to use funds allocated to MDAP—the Mutual Defense Assistance Pact. But those funds are specifically earmarked for research and development of physical instruments, machines, guns, electronic devices, etc., and it seemed hopeless even to try to justify the use of MDAP money for cryptanalytic research and development. It was only after we had pointed out the ways in which military cryptology had been used in World War I and II that the funds sought were granted.

4. This point about cryptology being useful only for such relatively unimportant things as personal
diaries, love missives, and attempts to prove that Bacon or somebody else wrote the Shakespeare Plays reminds me of a story which may be a bit apochraphyl but is somewhat amusing.

5. The story of the old Persian Queen Semiramis.

Stay, weary traveller!
If thou art footsore, hungry, or in need of money-
Unlock the riddle of the cipher graven below-
And you will be led to riches beyond all dreams of avarice!

-3-
0, thou vile and insatiable monster! To disturb these poor bones!
If thou had'st learned something more useful than the art of deciphering,
Thou would'st not be footsore, hungry, or in need of money!

Many times during the course of the last 40 years I've had occasion to wish I knew the old gal's present address so that I could put as a 1st Ind. to her basic communication the single word "Concur".

It is planned that I give a series of talks on the highlights of cryptologic history. This may be useful at least to some of the members of SCAMP '58, for I may tell you right away that there doesn't exist in English
or in any other language, for that matter, an adequate or even a fairly good history of the invention and development of cryptography and of its counterpart, cryptanalysis. There is no real history, definitive and detailed. What bits and pieces one finds here and there in popular accounts are generally full of misunderstandings, mis-statements, and downright lies.

Of course, there is a good reason why no history of cryptology worthy of the name has been produced for public use. It is that as a rule governments don't publish them or permit its cryptologic workers to publish histories, brochures, or articles. This is an understandable and sensible rule if not carried to absurd and illogical limits by insisting that all COMINT must be kept secret for all time. Later on I may tell you
about an amusing if not enlightening conference I was summoned to attend at the Pentagon a week ago today.

Of course, now and then some cryptologic information does leak out, as for example, when congressional and other official investigations either require or accidently bring about the disclosure of such information, or when some formerly trusted worker commits indiscretions, or consciously and deliberately breaks the trust that had been imposed. Of both these types of security breaches--official or personal--I shall have more to say later on. At the moment I will merely comment that the history which comes from such leakages and breaches of trust are apt to contain errors, misunderstandings, distortions, and lies.
Some of you may have wondered what the title of my talk or series of talks is. Dean Swift asked me yesterday to tell him so that it could be indicated on the announcement sheet. I told him I preferred to state the title myself and I'll now disclose my secret by telling you that the title is:

"The Influence of C-power on History."

Lest there be some here who think I'm laboring under the delusion that this building and SCAMP are U.S. Navy property or that I've suddenly gone psychotic and imagine I'm Admiral Mahan, I hasten to explain that the "C" in the title of my talk is not the word "SEA" but the letter "C" and it stands for the word CRYPTOLOGIC. The title of the talk is therefore "The influence of
cryptologic power on history." As a subtitle I offer this: "Or how to win battles and wars and go down in history as a great tactician, strategist and leader of men; or, on the other hand, how to lose battles and wars and go down in history as an incompetent commander, a heel a 'no-good-nik' 

At this point let me hasten to deny that I'm casting any reflections upon certain successful--spectacularly successful commanders--such as Generals Eisenhower and MacArthur. But names will occur to you without my calling them to your attention--and there will be names of men in each of the two categories--"how to win" and "how to lose" battles and wars.

-8-
At this point I'm reminded of a story about General Montgomery-- "Monty" and I have the story on pretty good authority.

Story re Monty in N. Africa, 1942.

Before a group such as this I think it hardly necessary to make this general statement but I'll make it. That not all historians know that the history of diplomacy and warfare teems with instances where the turn of events was greatly affected by the relative cryptologic power of the opposing forces. Most of the story in the history books, especially when first written, does not tell the complete story or the whole truth -- for the cryptologic facts are usually very carefully hidden from historians, even from official
historians, and are not brought to light for years, decades, centuries, and maybe never. (Tell about (1) Morison (Samuel Eliot), (2) Navy Op. Research on Battle of Atlantic, (3) Wenger lecture at Naval War College.

Sometimes the course of history is materially or drastically changed by the existence of COMINT, or it could have been changed by its proper use—as some say about the COMINT available to us before Pearl Harbor, but sometimes, also, the course of history is materially hanged by the non-existence of COMINT where it had previously existed and was used. We will discuss an incident of the latter type, too, in due course. But first, an incident of the former type—Pearl Harbor. The story of P.H., which I begin by reading from the 17 Dec 945 issue of TIME. I should preface the reading by
reminding you that the war was over--or at least V-E and V-J days had been celebrated--and the clamor on the part of vociferous Republicans, who had for years been insisting upon learning and disclosing to the world the reasons why we had been caught by surprise in such a disastrous defeat and calamity as the Japanese had inflicted upon us at Pearl, this clamor had to be met. It could no longer be hushed by the need for military secrecy. So there were investigations--a half dozen or more, winding up in a grand finale of the Joint Congressional Investigation into the Attack on Pearl Harbor. It was this investigation which not only itself brought into the open every detail and exhibit in its own lengthy investigation and hearings but also disclosed everything that was said and shown at all the previous Army and Navy investigations--about a half
There came a day in the Congressional Hearings when General George C. Marshall, Chief of Staff, U.S. Army at the time of the Pearl Harbor Attack, was called to the witness stand. He testified for several days, long, long ones. Toward the end of the ordeal he was questioned about a letter it had been rumored he'd written to Governor Dewey in the Autumn of 1944, during the Presidential Campaign. General Marshall balked. He pleaded most earnestly with the Committee not to force him to disclose the letter or its contents, but to no avail. He had to bow to the will of the Committee.
A few moments ago I commented that the sort of cryptologic history which gets published as a result of official investigations is apt to contain errors, misunderstandings, distortions, and downright lies. And this account in TIME contains its share of them. But the curious part of this story is that TIME didn't commit these offenses; they were in the original Marshall-Dewey letter, which had been prepared by somebody on Marshall's staff who got the results of COMINT but was no technician or cryptologist. I will interrupt the reading of the letter to remark that undoubtedly those of you who followed at all closely the disclosures—the remarkable and shocking disclosures from the point of view of national security—of the Joint Congressional Investigation of the Attack on Pearl Harbor must have wondered about or been mystified by this question: If
we were really reading the Japanese code long before Pearl Harbor, why were we caught by surprise when the attack came? Why did we lose over 3,000 men in a couple of hours, all those big battleships in harbor, and all those planes on the ground?

You weren't alone in thinking about this mystery. Listen to these extracts from the Report of the Majority of that Joint Congressional Committee, p. 170 & 253.

I'll return later to the Marshall-Dewey correspondence. But now:

What was meant by the name "MAGIC"?
How did the term come to be used?
It was introduced into our usage by the British. It was the cover name during the WW II years for
for the product of COMINT operations and activities.

(1) Special intelligence, (2) Traffic intelligence, (3) Weather intelligence.

I suppose it's hardly necessary for me to tell you how carefully guarded were the fruits of the MAGIC—even the fact of its existence was known to only a very few persons. Hearings p. 261. Success—rather its continuance—rested upon a very slender thread.

Midway, for instance, Marshall Dewey letter.

(J. Red machine. OSS in Lisbon. Marshall Dewey ltr.)

There are many persons who still argue about certain questions about Pearl Harbor Every so often the story
comes up and the fires of controversy are fanned once again to the blazing point. (A researcher at RAND is still working on a rather lengthy treatise on the subject.) The right-wingers are, of course, still convinced and are trying to convince other Americans that President Roosevelt brought the attack about and deliberately. Some of them make shocking charges and allegations of conspiracy among Roosevelt, Marshall and Stark. Which of course is nonsense--disprovable by rather easy logic. Maybe I'll go into this later if you wish.

But let's get back to the Marshall-Dewey letter.

The harm that the disclosure of this letter caused is calculable. The hearings were open and the documents are available. The harm that the disclosure of the letter caused is clearly calculable.
(40 volumes) are public documents.

Should we be greatly astonished that certain governments have greatly improved their communications security devices and arrangements since the close of the Congressional Investigation???

I read now from p. 232 of the Majority Report of the Joint Congressional Committee.

1. "... all witnesses familiar with MAGIC material throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

2. General Chamberlin (G-3 of Gen. MacArthur's staff throughout the war in the Pacific (told me (and he -17-
put it in writing for me on request): "The information G-2 gave G-3 in the Pacific theater alone saved us many thousands of lives and shortened the war by no less than two years."

3. I hardly need say what the latter saving alone was worth in billions of dollars. I made a calculation and found that $1.00 spent for COMINT equals $1,000 spent for other war materials and activities.

Now let's see what happened during WW II when we had not have COMINT on our side.

In our struggle against two very desperate enemies, the Germans and the Japanese, it was often the possession of COMINT, the so-called "MAGIC" which meant the...
difference between defeat and success. When we had magic
could put what little we had at the right time in the
right place. And when we didn't have it--as in the
famous and almost terribly disastrous Battle of the Bulge
we took a bad beating.

- READ from letter -

When we didn't have it--well, as I said, things went
badly because our principal G-2's had come to rely too
heavily on it.

The Battle of the Bulge.
Baldwin Article - Read.

1. Show 1st page of Baldwin article. (p. 30) and
read title of.
2. Read from next card — Merriam.
3. Then read extracts from p. 40.
According to Eisenhower's personnel officer, American losses in the Battle of the Bulge totalled 75,890 men, of whom 8,607 were killed, 47,139 wounded, and 21,144 missing. Over 8,000 of these casualties were in the 106th Division. Because of heavy German attacks, 733 tanks and tank destroyers were lost. Two divisions, the 28th and 106th, were nearly completely annihilated, although the 28th Division did subsequently enter combat after being rebuilt.
I hope I've not tired you out by such a lengthy preface to the real substance of my talks. So we'll begin by asking:

How old is the science of cryptology?

Which came first -- secret writing?

Or plain-text writing?

The art of writing probably grew out of pictographs and its growth can be traced back to the dawn of civilized man. Rebus.

Example of rebus. (p 2)
Cryptanalysis - and psychoanalysis -- in the Bible.

Nebuchadnezzar and his dream. Daniel, Chapter 2: 3, 4, 5, 6, 7, 8, 9, 10, 11.


Read from Bible - Daniel.

MENE, MENE, TEKEL (UPHARS IN (PERES Belshazzar and "The Handwriting on the Wall".

Daniel - The first cryptanalyst (B.C 570-569) The Second Psychoanalyst or interpreter of dreams. Joseph was 1st.

Instances of actual cipher in the Bible:
Jeremiah 25: 26  
51: 41

Some history from Br  Manual of Cryptography.

Scytale - Spartan Ephors send messages to commanders in field. Example from Grecian history. Greek at Court of Persian King Darius--message to colleague Aristagoras in Greece.

Conveying info in wartime by bundles of ribands of different colors, notches on stick, knots tied in various ways. Fires or beacons--all nations of antiquity.

Polybure describes system used by Greeks--co-ordinate
system -- Letters divided into groups of five and the number of fires lit in two separate places denoted the group of letters and the position of the letter in that group. Fires as late as 1746 in Italy to signal, code given to General the Marquis de Mirepoix in command mixed corps French, Spanish and Genoese troops, still in existence.

In Africa--beating of drums--only chiefs of tribes and headman initiated.

Caesar's cipher - invented and used many centuries earlier in various countries--by Carthageniains and Phoenicians. Used by Germans in 1870-71 and by British forces during S. African war.
The only systems known to have been employed between time of Julius Caesar and the beginning of the 16th Century are two:

1. i = . a = : e = :: o = :: u = :::
   Th:: t::wn c::p::t::l::t::d

2. System in which consonants remain unaltered but the vowels are replaced by the immediately following consonant.

For many centuries after Roman invasion Br crypt almost entirely neglected, one reason being that the art of secret writing was long regarded as an invention of the Evil One. There are many instances of students of it being accused of sorcery, among whom may be mentioned Tritemius the Abbe of Spanheim . . .
Viete - Then about him. P. 6 Br Man.

Correspondence between Court of Spain Henri IV (1553-1610) and Chiefs Anti-Royalists in France.

RUNES on a stone in front of Gripsholm Castle near Stockholm.

A.S. "Rune" - "a secret, a mystery." "Magic".

Any of the characters of the alphabet formerly in general use by the Teutonic, or Germanic, peoples from about the 3d Century A.D.

Blocked out portion -- another type of "Ruin"
Beginnings of modern cryptology can be traced back to the days of the early years of the 15th Century, when it was extensively employed by the princes and chancerrie of the Papal States.

For example, see this alphabet of 1401! (Next slide)

(Cipher alphabet of 1401)

Trithemuis - 1518

Abbe of Spanheim

Trithemian Oath

Present oath. Back up by P.L. 513 - now 18 USC 798-28
We administer a special oath to everybody who comes into the field.

1st slide. (242)

Examples of cipher alphabets and small syllabaries used centuries ago. (246 or 3)

1. Charlemagne's cipher (768-814)
2. Cipher used in England during reign of Alfred the Great 871-901.
3. Ogam writing of ancient Eire.
5. Marquis of Worcester's "Clock Cipher".

Cipher alphabet in Sir Thomas More's *Utopia*, 1518

3.3

3.5 Facsimile of a cipher found among the papers of Mary Stuart, Queen of Scots (1542-1587).

3.6 Cipher alphabet - Queen Mary Stuart and Bishop of Glasgow, then her Ambassador or solicitor in France, 1571.

3.7 Sliding-card cipher. Facsimile of one used in the later years of Elizabeth's reign (about 1600).
The two-word square cipher. State cipher used in Charles' I's time (1627) for communicating with France and Flanders. (A co-ordinate system)

Part of Duke of Buckingham's cipher used in 1627 for communicating with France.

Numerical cipher used in reign of Charles II (1630-1685) between Prince Rupert and the Earl of Arlington, Sec. State.

Foreign Office Cipher during reign of George III. (1779)
Frontispiece of "The Babington Plot" by Alan Gordon Smith, London 1936. The cipher used by Mary Stuart Queen of Scots with Babington. (1542-1587)

Frontispiece of "The Babington Plot" by Smith. The Forged Postscript, with Phillips' endorsement. (Ciphers involved in the Babington Plot. The forged postscript.)

Ciphers used by Philip II of Spain (1527-1598) reigned 1556-98. (pp. 102, 103)

-32-
But monoalphabetic ciphers still used today.

Gustav Rumrich spy case.

Porta's table (1563)

Porta's table as it appears in an early Elizabethan State paper.

Vigenere Square as pictured in the ordinary literature.
Vigenere Square as V. describes it in his book (1586)

Ciphers used by Galileo (1564-1642)
   Italian astronomer and physicist
Huyghens (1629-1695)
   Dutch mathematicians, physicist and astronomer.
One of the earliest instances of the advantage gained in the course of military operations by the capture and subsequent solution of a message sent by the enemy took place in 1626, Siege of Realmond, a town of Languedoc, then in possession of the Huguenots but besieged by the King's troops under command of the Prince de Conde. 

Latter about to raise siege. Message intercepted. Rossignol reads. Out of powder and would have to surrender if not immediately received new supply.
SCAMP 1958

LECTURE I – SECTION 1 – 24 June 1958
24 June 1958

1) 22q (Marshall-Dewey plate - for testing)
2) 412
3) 0
4) 1
5) 2
6) 31
7) 410
8) 2
9) 151
10) 242
11) 33
12) 243
13) 35
14) 36
15) 37
16) 38
17) 39
18) 3.10
19) 3.11
20) 217
21) 218
22) 52
23) 37
24) 6
25) 61
26) 5
27) 51
28) 4

June

Sunday 19

Total No. days

Cost fees
Cryptanalysis is a game, in which one's adversary makes all the rules, and moreover does his utmost to make them as complicated as possible. Consequently, though the cryptanalyst may (and should) use scientific methods in his research he cannot always be carried along by the scientist's simple faith in the fundamental rationality and uniformity of nature. He will seldom, that is, be able to solve a cypher by direct application of real mathematics, though he will often use methods which are very similar to mathematics, but lack the simplicity and elegance of the real thing and are usually much more laborious.

2. A former member of this organisation had a motto which he used to quote to new recruits "indexing is the mother of solution." When you are confronted with a pile of messages in an unknown cypher the first step, then, is to index them and see what you have got. Then you proceed to theorise about a possible solution that would account for all the phenomena recorded in your index and test it - if it fails you then think of another.

* * * * *

Extract from "The Modern Problem"
Joshua A Cooper
in remarks
made at the occasion
of the opening of "Effigy"
at C.N.A. 24 Feb 1958
Problems of manufacture and tape production machinery
Tape No. 3

Begins with

ITT Machine
The IT&T Co. teletype cipher attachment

With the growth of teletype communications, cipher teletypewriter attachments were invented.
SIGCUM

Cover removed
LECTURE NOTE

SIGCUM with B-131 set and teletype machine

(SIGHUAD - a form of SIGCUM with one-time key features)
(Dangers of electrical radiation)
(Dangers of depth)

Stop! I can't check! Next case!
SIGNIN

Wartime development

lots of "bugs"
Hebert Co settled for $50,000,000
Instituted about 10 years ago.
Probably will be settled for a few thousand
Cyphory and cifax machines

Glasary

Vocoder types
New developments in cipher machines

\{ AFSAM-7,  
AFSAM-9,  
AFSAM-15,  
AFSAM-36 + AFSAM-D21 \}

"Integrated" equipments

Ciphery + its problems. Slightly
Recognition and Identification
Call sign
Telemetering
Television
The professional cryptologist is always amused by the almost
unwarrantable reference by the "layman to "the German Code"
or "the Japanese Code" or "the
U.S. Code."

To give an idea as to the
multiplicity of systems—
show next 2 lectures.
Number of cryptographic systems in effect 7 Dec 1941 - October 1945

[U.S. Army + Army Air Forces only]
Number of holders of cryptographic materials Dec 1941 - Oct 1945 [U.S. Army & Army Air Forces only]

Stop! Don't check! Next 2 cards
Keeping track of crypto material + accounting.

Japanese incident I certify to destruction by burning.
I will bring this talk to a close now by reiterating the importance of the slogan we try to inculcate:

"Don't learn your COMSEC laws by accident!"
History of the operation

Lecture V - 7

Section 1
THE GOVERNORS, LIEUTENANT GOVERNORS, and
Capt. of His MAJESTY'S

GARRISONS AT HOME AND ABROAD, WITH
THEIR ALLOWANCES

VERMONT ASSEMBLY