SCAMP 1958

LECTURE I - Section 2 - 1525 - 1615

Total No. of Slides -16

British Cipher Message using title page of the Army List

Message dated 13 Sept 1781

The New Spelling Dictionary by 257
Rev John Entick, London, 1782

LECTURE

SLIDE 6.3

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)(enciphering)

encrypting

■ Typical of the small codes + syllabaries used at the time.

In addition, Code or conventional words to rep names "of persons"
British used code names In Clinton places
Papers following are found

American Generals – Apostles { Washington = James
Sullivan = Matthew

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

LECTURE NOTE

~~[EAS[illegible] 7 H]~~ noslide

REVOLUTIONARY WAR PERIOD – Systems used by Americans and by British

Americans –

iphers
- a Simple monoalph sub
- b Monoalph with variants by use of long key sentence à la Franklin
- c Vigenère with repeating key

odes
- a Dictionaries
- b Keybook using words
- c Syllabaries

)
- Secret inks
- Grilles

- over -

British –

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

- 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

REF ID:A38382

Lecture I ~~14~~ 4 June total ↓

~~[illegible]~~ ~~[illegible]~~ (~~Beginning of~~ Section 2) Lecture ~~[illegible]~~ — ~~[illegible]~~ slides

[16 slides] Total

1) 631
2) 63
3) 257
4) 232
5) 2321
6) 243
7) 244
8) 6.4
9) 65
10) 6.6
11) 67
12) 6.8
13) 69 (A) Slip 231 in here (Lovell letter)
15) 240
16) 6.10 End Sect 2 of Lecture I

No slide

Revolutionary War Period - Systems used by Americans and by British:

Americans:

Ciphers

a Simple monoalph. sub.

b. Monoalph. with variants by use of long key sentence ala Franklin.

c. Vigenere with repeating key

British·

a monoalphabetic sub.

b Vigenere with repeating key

c. Grilles

Americans:

Codes
- a. Dictionaries
- b. Keybook using words
- c. Syllabaries

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.

Typed

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

———————

6.31

Jefferson Syllabary

(Encoding) (enciphering)
encrypting

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

6.3

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.)

257

The New Spelling Dictionary by Rev. John Entick, London, 1782.

232

British Cipher Message using title page of the Army List. Message dated 13 September 1781.

Applies to 232.1

Line 22

THE GOVERNORS LIEUTENANT GOVERNORS & C OF HIS
1 2 3 4 5 6 7 8 9 10 11 12 13 11 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38

MAJESTY'S
39 40 41 42 43 44 45 46

Line 23

GARRISONS AT HOME AND ABROAD, WITH THEIR ALLOWANCES,
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43

"No 6"

Line Line
22. 6 7 8 39 5 8 17 28 12 31 26 39 23 20 3 23 45 11 12 22 10
VERMONT ASSEMBLY IS TO
39 26 15 17
MEET

The key for the preceding message.

(Finding the key after solution.)

WAIT!

Before showing the next slides explain about British cryptanalysts worxing on American ciphers.

243

Franklin (Dumas) Cipher-Key Text.
1706-1790.

244

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 escapted to Br. lines (peculiar part of Arnold's treason).

64

One of the cipher letters sent by Benedict Arnold to Sir Henry Clinton: 15 July 178Ø.

> "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."

(Full text - see typewritten sheet accompanying plate 6.5)

6.5

Plain text of the preceding message.

6.6

Treason agairst Washington.
Arnold lays a trap for Washington.

6.7

Another example of Benedict Arnold's ciphers

6 8

Arnold's Treasonable Cow Letter

6.9

Example of a grille used by British.

231

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. 21,178ø

Sir:

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 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 Ageny who was illiterate.

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

240

Enciphered resolution of the Revolutionary Congress of the U S., 8 February 1782.

6.1∅

Interest in cryptology in Europe.

Frontispiece of Dlandol
Contre - Espion 1793.

Breadboard model of WAC or WAVE
Cryptographic Officer

SCAMP 1958

Lecture V

History of the invention and development of cipher devices and machines

Section 1 - 1 July 1958

2:15 - 3:05 50 min

Section 2 3:15 - 4:05 50 "

100 "

SCAMP 1958

1 July

Lecture V – Cryptomachines etc

Section 1 (35 slides)

45
452
454
47
47.1
48.
49
49.1
49.4
495
50
501
160.1
504
159.1
502
505
506
507
508
5011
50.12 ?
51
52
54
55
171.1
164
70.1
703
2601
260
261-A
261-B
262
~~58.1~~
~~59~~

Section 2 (42 slides)

58.1
59
65
57
71
172
71.1
71 2
71.3
172.1
72
165
172.2
172X
172.10
170-A
170 2
1707
170.9
172.4
172.5
173
174
74
74.1
742
58
56
258
60
178
179
180
182
183
185
186
1861
236
237
129
130

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 ~~your~~ traffic laws by accident!"

I thought the slogan useful as the title of my talk but I modified it a little.

Don't learn ~~your~~ COMSEC laws by accide

I began my talk by reading Webster's def of the word accident

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 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.

Having defined the word, I'll 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 say that;

3 During the war, the President of the United States, ~~and 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~~ know who first used the following terse statement ~~vivid~~ ~~description~~, but it's decidedly applicable in this case "accidents don't happen--they ~~are~~ brought about!" Our Navy communication intelligence people were reading the Japanese Navy's high command messages, they had Yamamoto's schedule to the day,

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 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."~~

The key for the preceding message

[Finding the key *after* solution]

Wait!

Before showing next two slides explain about British cryptanalysts working on Am. ciphers.

243

Franklin (Dumas) Cipher-Key Text
1706-1790

244

1706-1790
Franklin (Dumas) Cipher-Encipher Table

Beale Papers ?

no slide

LECTURE NOTE ~~FOR SLIDES 6-7~~

See next card for text

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 showi he is well-placed. Arnold gets command of West Point. They used secret inks; Bailey's dictionary; word ciphe with words out of Blackstone and songbooks, grilles; slips of paper enclosed in specially constructed hollo bullets. Andre captured Sep 1780, writes out full confession and was hanged. Arnold barely escaped to Br. lines (peculiar part of Arnold's treason) 11

LECTURE [redacted] SLIDE 6.4 [illegible]

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. ete, 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

LECTURE NOTE

6.6

Treason against Washington.

Arnold lays a trap for Washington.

13

6.7

1) Another example of Benedict Arnold's ciphers

2) Arnold's Treasonable Cow letter 6.8

3) Example of a grille used by British 6.9

6.8

The Benedict Arnold Indecipherable cow letter

REF ID:A38382

69

Example of grille message (British)

LECTURE NOTE

LOVELL, James

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

* * * * * * * *

[illegible] Philad^{a}. Sep. 21, 1780

Sir:

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

[STOP - Don't click.
Tell about next great landmark [illegible]
[illegible] roof + [illegible]

(THE END)

no slide

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 awry because of incorrect solution by British Army Cryptanalysts (amateur) with " " in America

Wait!

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

2) And about Ellis history "The Secret Post office and Office of Decipherers"

Enciphered resolution of the Revolutionary Congress of the US 8 Feb 1982

Interest in cryptology in Europe 6 10

1) Frontispiece of Dlandol
Contre-Espion 1793

2) Breadboard model of WAC or WAVE
Cryptographic Officer

3)

LECTURE NOTE

6.10

Dlandol frontispiece (a cryptographer at work)

His assistant -- early model WAF

103

Typed

FRONT

Lectures I, ~~II, III~~

SCAMP 1958

LECTURE I - 24 June 1958

28 slides Section 1 - 1415 - 1510 55 minutes

16 " " 2 - 1525 - 1615 50 "

44 105.

(Total no of slides 28)
16
44

SCAMP 1958

LECTURE I - Section 1 - 24 June

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 that 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

COPY

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, gims, 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 ~~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 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!

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

Many times during course of last ~~30~~ 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!"

A-1

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 ~~x~~even as a "weapon". Story of Semiramis (over) (Well, anyhow it's been an interesting life!)

? ~~4. Read extracts from TIME of 17 Dec 45.~~

~~Extracts from P.H. report (next card)~~

1)

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 USCAMP '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 accidentally 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 this talk or series of talks is. Dean Swift asked me yesterday to tell him so that it could be indicated on the pre-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 <u>CRYPTOLOGIC</u> 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 of "how to win" and "how to lose" battles and wars

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 history in the history books, especially when first written, does not tell the complete story or the whole truth -- for the cryptologic facts [redacted] are usually very carefully hidden from historians, even from official historians, and are not brought to light for years, decades, ~~-- sometimes for~~ centuries, or maybe never (Tell about (1) Morison (Samuel Eliot), (2) Navy Op Research on Battle of Atlantic, (3) Wenger lecture at Naval W 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 -- the story of P.H. ~~(NEXT CARD)~~

51

My talk will be divided into three sections, and its overall ~~the~~ title ~~of the 1st Section~~ 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; ~~and that~~ the "C" in the title of this section of my talk stands for ~~"Cryptologic" -- "The influence of Cryptologic Power on history."~~
hardly necessary to say more than this That not all historians know ~~But~~ that the history of mankind and particularly of warfare teems with instances where the turn of events was much

(OVER)

(81) ~~[illegible]~~ ~~when I are~~ began by reading from the 17 December 1945 issue of TIME. ~~I propose~~ preface the reading by reminding you 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 ~~bad pummeling~~ 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

Some of you may have wondered what the title of my talk or series of talks is about. I'll now disclose this secret by ~~saying~~ telling you that it is "The influence of C power in history."

Lest there be some here who think I'm laboring under the delusion that I'm talking at some U.S. Navy installation, such as the Naval Academy or the Naval War College, or that I think I am Admiral Mahan re-incarnated in this city in which there are many people who believe in re-incarnation, I'll hasten to say that the "C" in the title of my series of 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 of them

There came a day in the Congressional Hearings when General George C Marshall Chief of Staff, U S. Army at the time of 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

Read TIME to "Uneasy Secret"

A few moments ago I ~~co~~ commented that (83) 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 ~~[illegible]~~ 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 ~~[illegible]~~

~~I will try to explain and to point out the errors in the Marshall-Dewey letter and in the account of it in TIME magazine~~

~~I now Read TIME MAG.~~

~~And now, after so many preliminaries,~~
~~let me read from TIME~~

~~For a few moments I shall return to the Marshall-Dewey~~ (8-2)

~~Etc.~~ 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 3000 men in a couple of hours, ~~and~~ 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:

(LF) [illegible] remarks that undoubtedly [illegible] VR, 8/3?

REF ID:A38382

~~63~~

P 79 of Majority Report (20 July 1946):

"INTELLIGENCE AVAILABLE IN WASHINGTON ("MAGIC")

"With the exercise . . . etc.

P. . .

"The Committee has been intrigued . . .

8 Ill return later to the Marshall - Dewey correspondence But now

(5) What was meant by the name "MAGIC"?

How did the term come to be used?

It was introduced into our usage by the Br -

It was the cover name during the WW II years

for the product of COMINT operations and activities.

→ 1) Special intelligence (2) Traffic intelligence (3) Sp Weather intelligence

I suppose its 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

Hearings P261 ← rested upon a very slender thread

only a very few persons. Success - rather its continuance,

Midway, for instance - Marshall Dewey lttr

mention (J Red machine OSS in Lisbon " " .

only ~~itself~~ brought into the open the details of ~~the~~ ~~the [illegible]~~ its own lengthy hearings but also disclosed every bit of what was said and disclosed at all the previous investigations.

There came a day in the Congressional Investigation when General George C. Marshall was called to testify and testify he did for several long days. Toward the end of that ordeal he was questioned about a letter he'd written in the autumn of 1944 to Governor Dewey. Marshall balked. He pleaded earnestly with the Committee not to force him to disclose the contents of that letter but finally he had to give in. He had to bow to the will of the majority of the Committee ~~And not to see what the letter [illegible] Marshall to [illegible]~~

about Pearl Harbor.

~~[illegible] About to~~
[illegible] There are many persons who still argue about ~~certain~~ questions, ~~and~~ 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 now let's get back to the Marshall-Dewey ltr ~~what happened during~~

The harm that the disclosure of this letter caused to our National Security is incalculable 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 ??

~~Summary~~ to (7) (88)

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 Chamberlain (G-3 of Gen MacArthur's staff throughout the war in the Pacific) told me (& he 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 & found that $1^{00} spent for COMINT = $1000 spent for other war materials & action

Now lets Are we not R Paraphrase paraphrase

2 WW II when we had and didn't have COMINT on our side (8:30)

In our struggle against two very desperate enemies, the Germans and the Japanese, it was different. possession of ~~magic~~ COMINT the so-called which meant the difference between defeat 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 terribly disastrous Battle of the Bulge we took a bad beating

~~Insert~~ ~~[illegible] to what Marshall told~~ Dewey

- READ from letter —

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

The Battle of the Bulge

Baldwin article - Read

8.10

1 Show 1st page of Baldwin article [p 30] and read title: "

2. Read from next card – Mourdan...

3. Then read extracts from p 40

9) [illegible] 1947 -Ziss [illegible]

Extract from: Merriam, Robert E., *Dark December*; The full account of the Battle of the Bulge, p. 211:

"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."

I hope I've not tired you out by such a lengthy preface to the real substance of ~~any~~ 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

Rebuses

229

Marshall - Dewey photo

4.12

Example of rebus
(p 20)

Cryptanalysis — and psychoanalysis — in the Bible,

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

Belshazzar - " 5: 1-5, 25-30

Cipherdor

Read from Bible - Daniel ∅

MENE, MENE, TEKEL, {UPHARSIN
{PERES

BELSHAZZAR & "The Handwriting on the wall"

DANIEL - The First Cryptanalyst (BC 570-569)
" _Second Psychoanalyst or interpreter of dreams, Joseph was 1st

Instances of actual cipher in the Bible:

Jeremiah 25, 26
51, 41

~~No slide but mention~~

Instances of cipher in the Bible

Jeremiah 25:26
51:41

<u>Scytale</u>

2

Scytale

Wait - see next card

Some history from Br
Manual of Cryptography

Scytale - Spartan Ephors send msgs to cmdrs 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
Polybius describes system used by Greeks - Coordinate system - ltrs divided into groups of 5 and the number of fires lit in two separate places denoted the group of letters & 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 cmd mixed corps Fr, Sp + Genoese troops - st in existence.
In Africa - beating of drums - only chiefs of tribes or [illegible] initiated

<u>Caesar's</u> cipher – invented & used many centuries earlier in various countries – by Carthagenians + Phoenicians

Used by Germans in 1870-71 + by Br forces during S. African war

The only systems known to have been employed between time of Julius Caesar + the beginning of the 16th Century are two:

1) ~~[illegible]~~ 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 Trithemius the Abbé of Spanheim. P 6 - Br Manual of Cryptography Read

Viète — Then about him P6 Br Man.

Corresp between Court of Spain
Henri IV (1553-1610) + 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 & chanceries of the Papal States

For example, see this alphabet of 1401!

[next slide]

4.10

Cipher alphabet of 1401

~~But recently there came into my hands a book devoted to setting forth in detail the ciphers used by Philip II of Spain who reigned from 1180-1223 long before 1401~~

SCYTALE

245.2

Trithemius 1518

Abbé 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

246 or 3

Examples of cipher alphabets and small syllabaries used centuries ago.

1) Charlemagne's cipher (768-814)
2) ~~Alfred~~ Cipher used in England during reign of Alfred the Great 871-901
(246) 3) Ogam writing of ancient Eire
4) Ogam-like alphabet of Charles I (1646) to Marquis of Worcester
(3) 5) Marquis of Worcester's "Clock Cipher"
6) Cardinal Wolsey, 1524, Vienna
7) Sir Thomas Smith, Paris, 1563
8) Sir Thomas Chaloner, Madrid, 1561
9) Sir Edward Stafford, Madrid, 1586

3.3

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

35

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

Cipher alph Queen Mary Stuart + Bishop of Glasgow 3 6
then her ambassador or solicitor in France. 1571

3.7 Sliding-card cipher Facsimile of one used in 37
the later years of Elizabeth's reign (about 1600) 3.8
3 8 The Two-word Square Cipher State cipher used 3.9
in Charles I's time (1627) for communicating
with France and Flanders (A co-ordinate system) 3.10
3.9 Part of Duke of Buckingham's cipher used in 1627 3.11
~~reign of Charles II between France Rupert and the~~
~~Earl of Arlington~~ for communicating with France. (1630-1655)
3 10 Numerical cipher used in reign of Charles II between
Prince Rupert and the Earl of Arlington, Sec State
3 11 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] 217

See next card [Frontispiece of "The Babington Plot" 218 by Smith, The Forged Postscript, with Phillip's Endorsement]

Cyphers involved in the Babington Plot

The forged postscript

5.2

Ciphers used by Philip II of Spain

1527-1598 ~~1165-1223~~; reigned 1556-98 ~~1180-1223~~]

(P102, 103)

~~Long before 1407!~~

3.4

But monoalphabetic ciphers still used today!

Gustav Rumrich Spy case

Porta's table (1563)

6.1

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

Vigenère Square as pictured in the ordinary literature

5.1

Vigenère Square as V. describes it in his book 1586

Ciphers used by

Galileo (1564-1642)

Italian astronomer + physicist

Huyghens (1629-1695)

Dutch Math, physicist, + astronomer

REF ID:A38382

P9 - Br manual

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 Siege of Réalmont (a town of Languedoc, then in possession of the Huguenots but besieged by the King's troops under command of the Prince de Condé.

Later about to raise siege. Msge intercepted Rossignol reads. Out of ~~supplies~~ powder & would have to surrender if not immediately receive new supply.

End of 1st section Lecture II
2.15 to 3.10 = 55 minutes

Navy's ~~highest~~ command ~~code messages; they knew the day and~~ exact ~~time~~ [illegible] that Yamamoto would leave Truk, the time he would arrive at Buka and leave Buka for Kahilli or Ballale, they also knew what his escort would be and so on. It was relatively easy to bring about the "accident". Our 1st Commander-in-Chief journeyed with safety because the communications connected with ~~the~~ his various trips were secure; the Japanese Commander-in-Chief journeyed in peril because ~~the~~ his 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 Yamomoto "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 [illegible]

5. The Yamamoto incident later gave rise to a somewhat amusing exchange of top secret telegrams between Tokyo and Washington, and after the war was all over these telegrams turned up in *The Forrestal Diaries*, Chapter III, pp 86-87

CARD 1

Extract from the "Forrestal Diaries," Chapter III, "Foretaste of the Cold War," pp. 86 and 87.

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)

Extract from the "Forrestal Diaries" continued. 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 localiz 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. . . ."

Extract from the "Forrestal Diaries," Chapter III, "Foretaste of the Cold War," pp. 86 and 87.

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 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, Toshiyuki - 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.

<u>Read</u> from Midway book

Lest you infer that our side didn't meet with any COMSEC "accidents," let me say that we had plenty — but these were not attributable to serious weaknesses in our COMSEC devices, machines, and rules but to human failure to follow the rules implicitly, or — and this hurts in saying it — to ~~COMSEC~~ 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

-over-

air strikes on the Ploesti oil fields in southeastern Europe We lost several hundred big bombers because of weakness we didn't realize existed in Russian communications. Those big raids constituted field days for the German fighter commands — because merely by T/A work, and simple at that, they knew exactly when and where our bombers were headed! When we found out, it was too late!

This incident leads me to say

that the COMSEC weaknesses of our allies and friends even today) 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 overweening desire to continue to read friendly traffic by cryptanalytic operations when one knows that that traffic should be made secure against one's enemies!

-over-

Thus far, no real pragmatic or psychoanalytic cure has been found for the illness. The powers that be have decided that ~~we keep~~ the illness will be avoided by the simple ruling ~~[illegible] as~~ that COMSEC interests will always override ~~COMINT, depressed~~ 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 & in applying remedies where possible in bolstering COMSEC weaknesses in NATO

Today we are going to see some slides which will mark and illustrate important milestones in the history of the invention and development of cipher devices, cipher machines, cipher apparatus, and, if there is time, 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, mechanico-electrical, and now, to electronic machines As mechanization and automation progresses in our civilization, similar progress has to follow in communications, especially in military, naval, air, and diplomatic communications.

LECTURE FOR 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"

57

The Myer disk, patented 14 Nov 1865

LECTURE NOTE FOR SLIDE 45.4

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

56

Somebody once said that the very nice looking document with seal and red ribbon the is issued when the U.S. Patent Office grants a patent is nothing but a fine looking invitation to participate in a lawsuit for infringement But the person being hurt by infringement upon his patent must be alive to file the suit - or at least his heirs and/or assignees should be alive I doubt however that Alberti or his heirs and/or assignees

- over -

were alive to contest this patent, issued in 1924, for a cipher disk practically identic with Alberti's disk of 1470'

LECTURE FOR SLIDE 47

The cipher disk finally [as again] patented in 1924 -- Huntington Patent

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

471

Cipher disk used by Nazis in
1936

LECTURE   FOR SLIDE 48

Original Wheatstone cipher device (invented and describc in 1879)

[First important improvement on the Alberti disk]

I have one here [Show it.]

LECTURE

FOR SLIDE 49

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./

[Story [illegible] — of three [illegible] [illegible]]

61

LECTURE FOR SLIDE 49.1

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

LECTURE FOR 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 "Cryptograph a 20 rondelles-alphabets" Comptes rendus, Marselles, 1891]

63

19.5

Bazeries, Etienne

LECTURE NOTE FOR SLIDE 50

First ~~Second~~ page of Jefferson's descnptıon of "The Wheel Cipher"

5c 1

Second page of Jefferson's description showing his calculation of the number of permutations afforded

160 1

Original model of Hitt's strip cipher ("The Star Cipher").

LECTURE FOR SLIDE 50.4

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 Mauborgne's set of 25 challenge messages

159.1

LECTURE NOTE FOR SLIDE 50.2

U.S. Army Cipher Device M-94.

– – –

50.5

Early attempts to use cylindrical cipher device principle but with variable alphabets (M-136)

(M-137) 50.6

(M 138-T1) 507

(M-138) 50.8

(Folding M-138) 50.11

~~(Russian Figures) 50.12~~

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.]

Stop! Don't click! Contents of next card 1st

(70)

1) European model A strip cipher 51
2) " " disassembled 52

Syko strip cipher

Court awards £35,000 to "inventor"

LECTURE NOTE

The Kryha cipher machine

72

LECTURE **FOR SLIDE 55**

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 subsitution as in Gold Bug -26! cipher alphabets or the large number:-
403,291,461,126,605,635,584,000,000 see over for 26!
quad/trillions/billions/millions
Estimated would take 1000 million men working a thousand million years to do the major part of wri-
13 ting these alphabets out --scroll would reach from earth beyond the planet Mercury!

26! =

Four hundred and three quadrillions;
two hundred ninety-one thousand, four
hundred and sixty-one trillions,
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 smile History of rotor
mac [illegible]

All the preceding examples of cryptographic aids are in the category of what may be termed "pencil and paper" or "hand-operated" aids. These, ~~but~~ of course, had to give way to more rapid and more secure means for crypto-communications, and thus meant <u>machines</u> of one sort or another.

-over-

There was pressing need in the military and naval services for <u>two</u> 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 those two types.

94)

171 1

LECTURE

FOR SLIDE 171

M-161: Signal Corps model made at Fort Monmouth

(Efforts to develop field machine) tell story re obtuse director of S.C Labs.

Note power source

LECTURE FOR SLIDE 164

Boris C.W. Hagelin

[Does a "hysteron-proteron" in inventing C-36]

LECTURE NOTE

70.1

Converter M-209

97

LECTURE NOTE FOR 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~~s~~, but will it work?")

99

260.1

Hagelin CX-52

Double tape-printing

Key-wheels removable

Irregular stepping

Non guaranteed cycle

260

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.

261-A

Example of solution of polyalphabetic encipherment with book-key and known alphabets, in this case reversed standard

261-B

Continuation

—— —— —— –

Hagelin (M-209) Solution.
"A depth of two"

Stop! Don't click! Next card

We come then to the so-called rotor machines, which are not based upon key-generator principles but are permutation machines

— -

71 FF

We come now therefore to (Hebern)

History of rotor machines

LECTURE

FOR SLIDE 58.1

The Swedish electrical machine B-21

/Original Aktiebolaget Cryptographe B-21. Mention Boris C.W. Hagelin/

75

LECTURE NOTE

Swedish machine connected to electric typewriter.

LECTURE FOR SLIDE 65

The keyboard electrically-operated B-211 Swedish machine

/Self-contained, instead of separate typewriter./

77

REF ID:A38382

LECTURE

FOR SLIDE 57

The original (commercial) Enigma cipher machine

/Later used with one improvement by Germans in World War II/

79

LECTURE NOTE

Come now to American developments

Edward H. Hebern

How he became interested in cryptography and invented a cipher machine,

18

LECTURE FOR SLIDE [redacted] 172

The first Hebern machine

[Manufactured for use by the Ku Klux Klan]

79

71.1

The first Hebern printing model

Still a one-rotor machine!

Where did he get the idea of cascading rotors?

712
713

Hebern rotors — <u>variable wiring</u> possibilities!

13 to one side & 13 to other

172.1

3-rotor Hebern

71

Hebern, Edward H.

[How he came to invent machine]

LECTURE FOR SLIDE 72
165

The 5-rotor Hebern machine

[Story of solution] with next slide 165

Tell this

80

1722

First Hebern machine built in accordance with Navy specifications

172.X

Hebern model S.I.S

Solved on challange by Navy

R

LECTURE NOTE FOR SLIDE 172.10

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

82

Stop! Don't click. Next 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 few thousand dollars

LECTURE NOTE

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!

LECTURE NOTE

170 A

U.S. Army Converter M-134-T1

Basic principle - external keying element

84

170.2

Converter M 134

Rear view

170.9

Converter M 134 -
with printing !

170.9

U.S. Army Converter M-134-A

86

1724

Original Navy Mark I ECM
With Bowdin wires!

And only 15 starting points!

172.5

First production model
of Navy Mark I

—

Army & Navy finally collaborate

SIGABA - ECM

~~Withheld from British until 1953~~

~~Battle to give to~~ ------

SIGIVI or BASKET

SIGABA - ECM withheld
from British.
Battle to give to British
Finally given in 1953
But during WWII had to
intercommunicate
Therefore — the CCM

174

~~SIGIVI -~~

~~explain principle~~

~~Stop! Don't click! See next card~~

{74
74.1
74.2}

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!

Stop! Don't click. Say [illegible] word about [illegible]. developm [illegible] [illegible]

(100)

German 8-wheel printing Enigma

Captured in 1945 at Mittelfels

A failure!

#17

COM

German Naval Enigma — differences between it & Army & Air Force E

LECTURE NOTE [redacted]

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.

88

LECTURE SLIDE 56

The AT&T Co. printing telegraph cipher machine (1918) (The original SIGTOT!)

[Story of solution]

247

Ex Order 28 Aug 45

Put in sequence in preface to Pearl H 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!

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 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 <u>all</u> 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 comits 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 imcompetent 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.

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 history in the history books, especially when first written, does not tell the complete story or the whole ruth -- for the cryptologic facts are usually very arefully 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 ometimes, also, the course of history is materially hanged by the non-existence of COMINT where it had eviously existed and was used. We will discuss an ncident of the latter type, too, in due course. But irst, an incident of the former type--Pearl Harbor. The tory 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 dozen of them.

There came a day ın 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.

Read TIME to "Uneasy Secret"

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 Attach 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 its 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 s halculable. The hearings were open and the documents

(4ø 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

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 nd didn't have COMINT on our side.

In our struggle against two very desperate enemies, he Germans and the Japanese, it was often the possession f COMINT, the so-called "MAGIC" which meant the difference between defeat 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 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. 3Ø) and ead title of.

2. Read from next card -- Merriam.
3. Then read extracts from p. 4Ø.

Extract from: Merriam, Robert E., Dark December: The full account of the Battle of the Bulge, 1947-Ziff-Davis Publishing Co., p. 211:

"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. Rebuses.

Example of rebus. (p 2) 4.12

Cryptanalysis - and psychoanalysis -- in the Bible.

Nebuchadnezzar and his dream. Daniel, Chapter 2: 3, 4, 5, 6, 7, 8, 9, 1Ø, 11.

Belshazzar - Daniel, Chapter 5: 1-5, 25-3Ø.

Read from Bible - Daniel.

MENE, MENE, TEKEL (UPHARS IN
(PERES

Belshazzar and "The Handwriting on the Wall".

Daniel - The first cryptanalyst (B.C 57Ø-569)
The Second Psychoanalyst or interpreter of dreams. Joseph was 1st.

Instances of actual cipher in the Bible:

1

Jeremiah 25: 26
51: 41

2

Scytale

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.

Polybuis 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 Carthagenians 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 Tritaemius the Abbe of Spanheim . . .

p. 6 - Br Manual of Cryptography. Read.

Viete - Then about him. P. 6 Br Man.

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

3.1

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 14Ø1! (Next slide)

4.1Ø

(Cipher alphabet of 14Ø1)

245.2

Trithemuis - 1518

Abbe of Spanheim

151

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.

<u>1st slide.</u> <u>(242)</u>

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

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.
4. Ogam-like alphabet of Charles I (1646) to Marquis of Worcester.
5. Marquis of Worcester's "Clock Cipher".
6. Cardinal Wolsey, 1524, Vienna.

(246
3)

7. Sir Thomas Smith, Paris, 1563.
8. Sir Thomas Chaloner, Madrid, 1561.
9 Sir Edward Stafford, Madrid, 1586.

3.3

Cipher alphabet in Sir Thomas More's Utopia, 1518

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).

3.8

The two-word square cipher. State cipher used in Charles'I's time (1627) for communicating with France and Flanders. (A co-ordinate system)

3.9

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

3.10

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

3.11

oreign Office Cipher during reign of George III. (1779)

217

Frontispiece of "The Babington Plot" by Alan Gordon Smith, London 1936. The cipher used by Mary Stuart Queen of Scots with Babington. (1542-1587)

218

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

5.2

Ciphers used by Philip II of Spain (1527-1598) reigned 1556-98. (pp. 1Ø2, 1Ø3)

But monoalphabetic ciphers still used today'

3.4

Gustav Rumrich spy case.

6

Porta's table (1563)

6.1

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

5

Vigenere Square as pictured in the ordinary literature.

5.1

Vigenere Square as V. describes it in his book (1586)

104

Ciphers used by Galileo (1564-1642)
Italian astronomer and physicist
Huyghens (1629-1695)
Dutch mathematicians, physicist and astronomer.

P 9 - Br Manual

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 Realmont, a town of Languedoc, then in possession of the Huguenots but besieged by the King's troops under command of the Princ 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

Lecture ~~Part~~ I - ~~[illegible]~~ — 28 slides

24 June 1958

1) 229 (Marshall + Dewey photo - for testing ~~[illegible]~~ slide projector
2) 4.12
3) ∅
4) 1
5) 2
6) 31
7) 410
8) 2
9) 151 — 245 2
10) 242
11) 3.3
12) 246
13) 35
14) 36
15) 3.7
16) 38
17) 3.9
18) 3.10
19) 3.11
20) 217
21) 218
22) 52
23) 3.4
24) 6
25) 61
26) 5
27) 51
28) 64

June

S	M	T	W	T	F	S
				19	20	21
22	23	I 24	II 25	26	III 27	28
29	IV 30					

travel 12 [illegible]
17 0
LA time

July

S	M	T	W	T	F	S
		V 1 8	9 2	VI 3 10	4	5
6	7 11	8 12	9 13	10 14	11 15	12
13	14 16	15 17	16 18	17 19	18 20	

Total No days
Cons 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 on the occasion
of the opening of "Effegy"
at GCHQ 24 Feb 1958

Problems of
Manufacture of tape

Our electronic tape
production machine
Solve problem

REF ID:A38382

Tape No 3

Begins with

ITAT Machine

LECTURE

FOR SLIDE 60

The IT&T Co. teletype cipher attachment

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

90

SIGCUM 178

" cover removed 179

LECTURE NOTE FOR SLIDE 180

SIGCUM with B-131 set and teletype machine

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

Stop! I can't check! Next ca..!

182

SIGNIN

Wartime development
lots of "bugs"

SIGMEW

CIFAX

185

CIPHONY

SIGJIP — Bell Tel 1st dev

Hebern Co suit for $50,000,000
instituted about 10 years ago.
Probably will be settled for few thousand

1864

Ciphony and cifax machines 186.1

SIGSALY

Vocoder types

New developments in cipher machines

- AFSAM-7
- AFSAM-9
- AFSAM-15
- AFSAM-36 + AFSAM-D21

"Integrated" equipments

Ciphony — + its problems. Sigsaly

Recognition & Identification

Call sign

Telemetering

Television

The professional cryptologist is always amused by the almost invariable 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 slides

Number of cryptographic systems in effect 7 Dec 1941 – October 1945

[U.S. Army & Army Air Forces **only**]

237

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

Stop! Don't click! Next 2 cards

129
130

Keeping track of crypto-material & accounting.

Japanese incident of certifying to destruction by burning

I will bring this talk to a close now by repeating the importance of ~~this~~ slogan we try to inculcate: "Don't learn your COMSEC laws by accident!"

History of the invention SCAMP 1958

Lecture V.

Section 1

Applies to 2321

Line 22

THE GOVERNORS LIEUTENANT GOVERNORS
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

&C OF HIS MAJESTY'S
32 33 34 35 36 37 38 39 40 41 42 43 44 45 46

Line 23

'GARRISONS AT HOME AND ABROAD, WITH
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

THEIR ALLOWANCES
29 30 31 32 33 34 35 36 37 38 39 40 41 42 43

'No 6"

22 6 7 8 39 5 8 17 20 12 31 26 39 Line 23 20 35 Line 22 45 14 12 22 10
V E R M O N T A S S E M B L Y. I S T O

39 26 15 17
M E E T