"C"

LECTURE I - SECTION 2

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

Ciphers

Americans:

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

British.

a. Monoalphabetic substitution.
b. Vigenere with repeating key.
c. Grilles

Codes

a. Dictionaries.
b. Keybock using words
c. Syllabaries.

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

Misc
a Secret inks
b Grilles
c Various concealment methods.

In addition, code or conventional words were used to represent the names of persons and places. The British used code names: ~~In Clinton Papers following are found:~~

American Generals - Names of the Apostles
- Washington = James.
- Sullivan = Matthew.
- etc

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

```
T H E  G O V E R N O R S  L I E U T E N A N T  G O V E R N O R S  &  C  O F  H I S
1 2 3  4 5 6 7 8 9 1Ø 12 13 15 17 19 21 23 25 27 29 31 32 33 34 36 38
                  11 14 16 18 2Ø 22 24 26 28 3Ø 35 37
M A J E S T Y ' S
  4Ø 42 44 46
39 41 43 45
```

Line 23

```
G A R R I S O N S  A T  H O M E  A N D  A B R O A D,  W I T H  T H E I R  A L L O W -
1 2 3 4 5 6 7 8 9 1Ø 12 14 16 18 2Ø 22 24 25 27 29 31 33 35 37
                  11 13 15 17 19 21 23 26 28 3Ø 32 34 36
A N C E S
38 39Ø 41 42 43
```

"No 6"
22.

```
6 7 8 39 5 8 17  2Ø 12 31 26 39 23 2Ø 35 22 45 14 12 22 1Ø 39 26 15 17.
V E [illegible] M O N T  A S  S E M  B L  Y I S T O M E E T
                          Line      Line
```

232.1
The key for the preceding message. (Finding the key after solution)

- - - - - - -

Before showing the next slides explain about British cryptanalysts working 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".

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 September 1780, writes out full confession and was hanged Arnold barely escaped to British 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."

(Full text - see typewritten sheet accompanying plate 6.5)

6 5
Plain text of the preceding message.

6 6
Treason against 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, of not all, of British code messages intercepted by the Americans.

* * * * * * * * *

To Gen. Greene, cy to Washington)

Philadelphia Sept. 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 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.

-4- [cont'd next page]

I am Sir with much respect.

Your Friend,

JAMES LOVELL

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 Agent who was illiterate.

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

24ø
Enciphered resolution of the Revolutionary Congress of the U.S , 8 February 1782

6.1ø
Interest in cryptology in Europe

Frontispiece of Dlandol. Contre - Espion 1793

Breadboard model of WAC or WAVE Cryptographic Officer