Rotating Grille for Alexander Hamilton

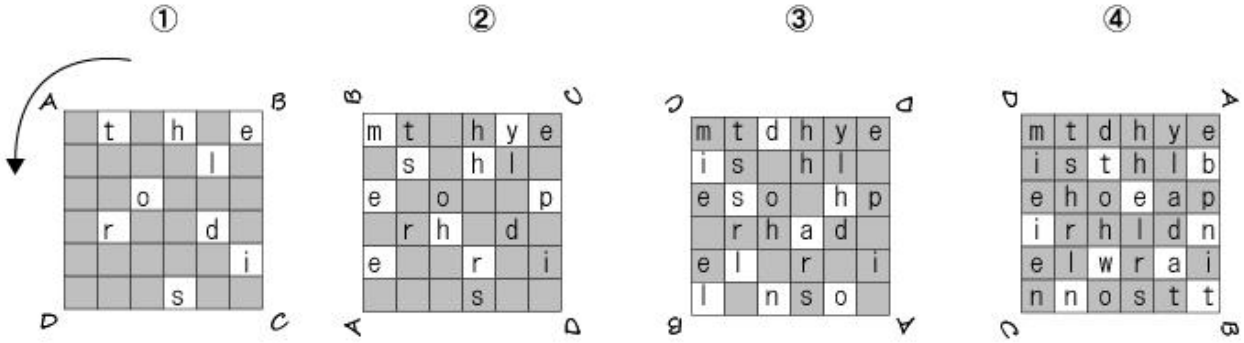
Rotating Grille for Alexander Hamilton

Some years after Alexander Hamilton died (1804) from the wound he received in a duel with Aaron Burr, a packet containing instructions of a cipher was found among his papers. The endorsement states it was forwarded to Hamilton on 23 May 1803. (As to the origin of the document, see the editors' notes in *The Papers of Alexander Hamilton*.)

Rotating Grille

The method described in the document is what is known as a rotating grille or a turning grille. It was popular at the end of the eighteenth century, notably after C. F. Hindenburg first provided a complete description of the scheme in 1796 (Karl de Leeuw, *Cryptology and Statecraft in the Dutch Republic*, p.111).

A grille is a sheet with a grid of squares thereon. Some of the squares are cut out. The figure below shows a procedure to encipher a phrase "The Lord is my shepherd. I shall not be in want." with such a grille.



Enciphering with a rotating grille. © S. Tomokiyo

In this example, the grille has a 6-by-6 grid of squares, of which nine are cut out. To begin with, the first nine letters of the phrase (t, h, e, l, o, r, d, i, s) are one by one written in each square cut out, from left to right, top to bottom. Then, the grille is turned by ninety degrees in a predetermined direction (counterclockwise in this example). Then, the next nine letters (m, y, s, h, e, p, h, e, r) are written similarly. After the steps of turning the grille and writing the subsequent nine letters are repeated two more times, every square is filled by exactly one letter.

Copying the letters written from left to right, top to bottom, the following ciphertext is obtained:
mtdhyeisthlbehoeapirhldnelwrainnostt.

Deciphering with a Rotating Grille

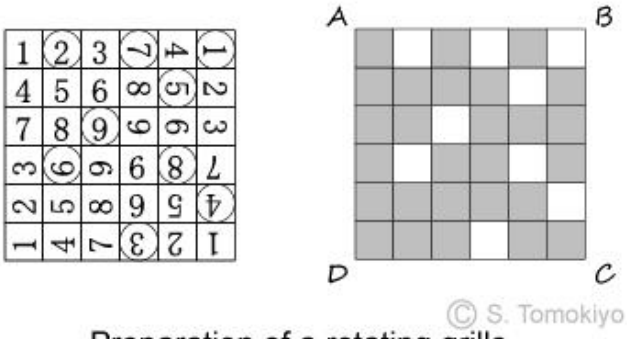
A recipient should have the same grille as the one used in enciphering. Knowing the grille is 6-by-6, the decipherer copies the enciphered message in a 6-by-6 grid of squares of the same size as the grille:

```
m t d h y e
i s t h l b
e h o e a p
i r h l d n
e l w r a i
n n o s t t
```

Applying the grille, the recipient would read the first nine letters (t, h, e, l, o, r, d, i, s) through the cut out squares. After turning the grille by ninety degrees, the next nine letters can be read, and so on.

Preparation of a Rotating Grille

It is noted that, when enciphering, every time the grille is turned, the cut out squares are precisely positioned at squares not yet filled. To achieve such a feat, the squares of the grille to be cut out should be carefully chosen. The figure below shows a procedure for that.



Preparation of a rotating grille.

First, the grid of squares is divided into four 3-by-3 quadrants. The nine squares of each quadrant are numbered 1-9 in a corresponding manner. Then, among the four squares numbered "1", one is selected to be cut out. In the above example, the rightmost square of the top row is cut out. This ensures that each of the four squares numbered "1" is exposed exactly once during enciphering by this particular cut-out square. Similarly, one of the four squares numbered "2" is selected to be cut out. By choosing thus exactly one square to be cut out from among the four squares bearing the same number, it can be ensured that each square can be filled at one of the four rotating positions.

Rotating Grille for Alexander Hamilton

A 6-by-6 grille may be too small to be used for messages in practice. The rotating grille for Hamilton contained 26-by-26 squares.

The instructions (in French) read as follows (the present author's translation).

> To use the checkerboard included here in place of a cipher in order to prevent discovery of your correspondence, employ the following manner. After having written your letter as usual, prepare the paper, on which you intend to put down your secret copy, of the same size as the square of the checkerboard placed on the said paper. Fix the square to the paper at the four corners with pins. It does not matter at which corner you begin, either A, B, C, or D, provided that you take care to turn the checkerboard to the left. Thus, if you begin at the corner A, you write your communication by placing on the paper prepared to this effect only one letter in each square cut out, proceeding from the right to the left, line by line. After having written in this manner to the end of the page, detach the checkerboard, turn it from the right to the left, with A making way for B, and fix it with pins by the same holes on your paper for the letter. Continue to copy your letter as explained herein above. After having filled all the squares cut out of the said page, turn again the checkerboard such that B makes way for C. By following this manner until you have used the four corners of the checkerboard, you will have filled your paper with twenty-six lines, each containing 26 letters. In order to avoid any difficulty and confusion, you may designate at which corner of the checkerboard you began, by placing at the top of your communication the letter indicating the said corner, for herein above the letter A.

Other codes and ciphers

Some other codes and ciphers by and for Hamilton are known, though the repertory was far less extensive than that of Thomas Jefferson or John Jay, who experienced foreign missions.

Roman Nicknames for Gouverneur Morris (WE095)

From 1792 to 1794, Hamilton's friend Gouverneur Morris, staying in Europe since 1789, was US minister residing in France. When Morris learned of his appointment, he wrote to Hamilton and proposed mutual confidential communication. Hamilton had a cipher devised and, for the time, proposed substitution of Roman names for some political figures.

> Will it not be a necessary preliminary to agree upon a cypher? One has been devised for me, which, though simple in execution, is tedious in preparation. I may shortly forward it.
> In the mean time, let us settle some appellations for certain official characters. I will call,
> The President, Scaevola.
> The Vice President, Brutus.
> Secretary of State, Scipio.
> Secretary at War, Sempronius.
> Sec'y of the Treasury, Paulus.
> Attorney General, Lysander.
> Senators.
> Robert Morris, Cato.
> Oliver Ellsworth, Virginius.
> Rufus King, Leonidas.
> George Cabot, Portius.
> Aaron Burr, Saevius.
> Richard Henry Lee, Marcus.
> [James] Monroe, Sydney.
> Ralph Izard, Themistocles.
> Representatives.
> James Madison, Tarquin.
> [Fisher] Ames, Valerius.
> Abraham Baldwin, Hampden.
> John Lawrence, Solon.
> [John F.] Mercer, Tacitus.
> [William Vans] Murray, Livy.
> Thomas Fitzsimmons, Cicero.
> Egbert Benson, Cromwell.
> Jeremiah Wadsworth, Titius.
> Jonathan Trumbull, Quintus.
> [William B.] Giles, Chronus.
> You see that I have avoided characteristic names.
>
> Alexander Hamilton to Gouverneur Morris, 22 June 1792

Book Code based on Entick's Spelling Dictionary

In June 1799, Hamilton received from his father-in-law, General Philip Schuyler, "a lengthy and complex code system using Entick's Spelling Dictionary" (Weber p.146 n.9).

Projected Hamilton-King Cipher

In 1800, Hamilton was preparing a cipher for correspondence with Rufus King, then US minister in London.

> If the projected cipher was established, I should now have very much to say to you. But for this the arrangement is not yet mature. Soon, however, I hope to make it so, by forwarding to you the counterpart, which is in preparation. I must, however, give you some sketch of our affairs.
>
> Alexander Hamilton to Rufus King, 5 January 1800

First posted on 26 August 2009. Last modified on 26 August 2009.

Articles on Historical Cryptography