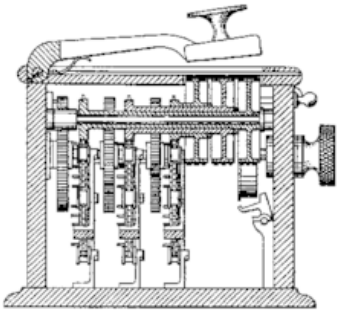
Hill cipher

In classical cryptography, the **Hill cipher** is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once.



Hill's cipher machine, from figure 4 of the patent

The following discussion assumes an elementary knowledge of matrices.

Contents

Encryption

Each letter is represented by a number modulo 26. Though this is not an essential feature of the cipher, this simple scheme is often used:

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number	0	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

To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible $n \times n$ matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible $n \times n$ matrices (modulo 26). The cipher can, of course, be adapted to an alphabet with any number of letters; all arithmetic just needs to be done modulo the number of letters instead of modulo 26.

Consider the message 'ACT', and the key below (or GYB/NQK/URP in letters):

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Thus the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

which corresponds to a ciphertext of 'POH'. Now, suppose that our message is instead 'CAT', or:

$$\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix}$$

This time, the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$$

which corresponds to a ciphertext of 'FIN'. Every letter has changed. The Hill cipher has achieved Shannon's diffusion, and an n-dimensional Hill cipher can diffuse fully across n symbols at once.

Decryption

In order to decrypt, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFK/VIV/VMI in letters). (See matrix inversion for methods to calculate the inverse matrix.) We find that, modulo 26, the inverse of the matrix used in the previous example is:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \pmod{26} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}$$

Taking the previous example ciphertext of 'POH', we get:

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

which gets us back to 'ACT', as expected.

Two complications exist in picking the encrypting matrix:

1. Not all matrices have an inverse (see invertible matrix). The matrix will have an inverse if and only if its determinant is not zero.
2. The determinant of the encrypting matrix must not have any common factors with the modular base.

Thus, if we work modulo 26 as above, the determinant must be nonzero, and must not be divisible by 2 or 13. If the determinant is 0, or has common factors with the modular base, then the matrix cannot be used in the Hill cipher, and another matrix must be chosen (otherwise it will not be possible to decrypt). Fortunately, matrices which satisfy the conditions to be used in the Hill cipher are fairly common.

For our example key matrix:

$$\begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} \equiv 6(16 \cdot 15 - 10 \cdot 17) - 24(13 \cdot 15 - 10 \cdot 20) + 1(13 \cdot 17 - 16 \cdot 20) \equiv 441 \equiv 25 \pmod{26}$$

So, modulo 26, the determinant is 25. Since this has no common factors with 26, this matrix can be used for the Hill cipher.

The risk of the determinant having common factors with the modulus can be eliminated by making the modulus prime. Consequently, a useful variant of the Hill cipher adds 3 extra symbols (such as a space, a period and a question mark) to increase the modulus to 29.

Example

Let

$$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

be the key and suppose the plaintext message is HELP. Then this plaintext is represented by two pairs

$$HELP \rightarrow \begin{pmatrix} H \\ E \end{pmatrix}, \begin{pmatrix} L \\ P \end{pmatrix} \rightarrow \begin{pmatrix} 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 11 \\ 15 \end{pmatrix}$$

Then we compute

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 8 \end{pmatrix} \pmod{26},$$ and

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 11 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 19 \end{pmatrix} \pmod{26}$$

and continue encryption as follows:

$$\begin{pmatrix}7\\8\end{pmatrix}, \begin{pmatrix}0\\19\end{pmatrix} \to \begin{pmatrix}H\\I\end{pmatrix}, \begin{pmatrix}A\\T\end{pmatrix}$$

The matrix K is invertible, hence K^{-1} exists such that $KK^{-1} = K^{-1}K = I_2$. The inverse of K can be computed by using the formula $\begin{pmatrix}a & b\\c & d\end{pmatrix}^{-1} = (ad-bc)^{-1}\begin{pmatrix}d & -b\\-c & a\end{pmatrix}$

This formula still holds after a modular reduction if a modular multiplicative inverse is used to compute $(ad-bc)^{-1}$. Hence in this case, we compute

$$K^{-1} \equiv 9^{-1}\begin{pmatrix}5 & 23\\24 & 3\end{pmatrix} \equiv 3\begin{pmatrix}5 & 23\\24 & 3\end{pmatrix} \equiv \begin{pmatrix}15 & 17\\20 & 9\end{pmatrix} \pmod{26}$$

$$HIAT \to \begin{pmatrix}H\\I\end{pmatrix}, \begin{pmatrix}A\\T\end{pmatrix} \to \begin{pmatrix}7\\8\end{pmatrix}, \begin{pmatrix}0\\19\end{pmatrix}$$

Then we compute

$$\begin{pmatrix}15 & 17\\20 & 9\end{pmatrix}\begin{pmatrix}7\\8\end{pmatrix} \equiv \begin{pmatrix}7\\4\end{pmatrix} \pmod{26}, \text{ and}$$

$$\begin{pmatrix}15 & 17\\20 & 9\end{pmatrix}\begin{pmatrix}0\\19\end{pmatrix} \equiv \begin{pmatrix}11\\15\end{pmatrix} \pmod{26}$$

Therefore,

$$\begin{pmatrix}7\\4\end{pmatrix}, \begin{pmatrix}11\\15\end{pmatrix} \to \begin{pmatrix}H\\E\end{pmatrix}, \begin{pmatrix}L\\P\end{pmatrix} \to HELP.$$

Security

The basic Hill cipher is vulnerable to a known-plaintext attack because it is completely linear. An opponent who intercepts n plaintext/ciphertext character pairs can set up a linear system which can (usually) be easily solved; if it happens that this system is indeterminate, it is only necessary to add a few more plaintext/ciphertext pairs. Calculating this solution by standard linear algebra algorithms then takes very little time.

While matrix multiplication alone does not result in a secure cipher it is still a useful step when combined with other non-linear operations, because matrix multiplication can provide diffusion. For example, an appropriately chosen matrix can guarantee that small differences before the matrix multiplication will result in large differences after the matrix multiplication. Indeed, some modern ciphers use a matrix multiplication step to provide diffusion. For example, the MixColumns step in AES is a matrix multiplication. The function *g* in Twofish is a combination of non-linear S-boxes with a carefully chosen matrix multiplication (MDS).

Key space size

The key space is the set of all possible keys. The key space size is the number of possible keys. The effective key size, in number of bits, is the binary logarithm of the key space size.

There are 26^{n^2} matrices of dimension n × n. Thus $\log_2(26^{n^2})$ or about $4.7n^2$ is an upper bound on the key size of the Hill cipher using n × n matrices. This is only an upper bound because not every matrix is invertible and thus usable as a key. The number of invertible matrices can be computed via the Chinese Remainder Theorem. I.e., a matrix is invertible modulo 26 if and only if it is invertible both modulo 2 and modulo 13. The number of invertible n × n matrices modulo 2 is equal to the order of the general linear group GL(n,$\mathbf{Z}_2$). It is

$$2^{n^2}(1-1/2)(1-1/2^2)\cdots(1-1/2^n).$$

Equally, the number of invertible matrices modulo 13 (i.e. the order of GL(n,$\mathbf{Z}_{13}$)) is

$$13^{n^2}(1-1/13)(1-1/13^2)\cdots(1-1/13^n).$$

The number of invertible matrices modulo 26 is the product of those two numbers. Hence it is

$$26^{n^2}(1-1/2)(1-1/2^2)\cdots(1-1/2^n)(1-1/13)(1-1/13^2)\cdots(1-1/13^n).$$

Additionally it seems to be prudent to avoid too many zeroes in the key matrix, since they reduce diffusion. The net effect is that the effective keyspace of a basic Hill cipher is about $4.64n^2 - 1.7$. For a 5 × 5 Hill cipher, that is about 114 bits. Of course, key search is not the most efficient known attack.

Mechanical implementation

When operating on 2 symbols at once, a Hill cipher offers no particular advantage over Playfair or the bifid cipher, and in fact is weaker than either, and slightly more laborious to operate by pencil-and-paper. As the dimension increases, the cipher rapidly becomes infeasible for a human to operate by hand.

A Hill cipher of dimension 6 was implemented mechanically. Hill and a partner were awarded a patent (U.S. Patent 1,845,947 (https://www.google.com/patents/US1845947)) for this device, which performed a 6×6 matrix multiplication modulo 26 using a system of gears and chains.

Unfortunately the gearing arrangements (and thus the key) were fixed for any given machine, so triple encryption was recommended for security: a secret nonlinear step, followed by the wide diffusive step from the machine, followed by a third secret nonlinear step. (The much later Even-Mansour cipher also uses an unkeyed diffusive middle step). Such a combination was actually very powerful for 1929, and indicates that Hill apparently understood the concepts of a meet-in-the-middle attack as well as confusion and diffusion. Unfortunately, his machine did not sell.

See also

Other practical "pencil-and-paper" polygraphic ciphers include:

- Playfair cipher
- Bifid cipher
- Trifid cipher

References

- Lester S. Hill, Cryptography in an Algebraic Alphabet, *The American Mathematical Monthly* Vol.36, June–July 1929, pp. 306–312. (PDF (https://web.archive.org/web/20110719235517/http://w08.middlebury.edu/INTD1065A/Lectures/Hill%20Cipher%20Folder/Hill1.pdf))
- Lester S. Hill, Concerning Certain Linear Transformation Apparatus of Cryptography, *The American Mathematical Monthly* Vol.38, 1931, pp. 135–154.
- Jeffrey Overbey, William Traves, and Jerzy Wojdylo, On the Keyspace of the Hill Cipher, *Cryptologia*, Vol.29, No.1, January 2005, pp59–72. (CiteSeerX (http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.133.1840)) (PDF (http://jeff.over.bz/papers/undergrad/on-the-keyspace-of-the-hill-cipher.pdf))

External links

- "Hill Cipher Web App (http://massey.limfinity.com/207/hillcipher.php)" implements the Hill cipher and shows the matrices involved
- "Hill Cipher Explained (http://massey.limfinity.com/207/hillcipher.pdf)" illustrates the linear algebra behind the Hill Cipher
- "Hill's Cipher Calculator (https://archive.is/20130215131917/http://asecuritysite.com/security/coding/hill)" outlines the Hill Cipher with a Web page