Introduction to Hill cipher

We have explored three simple substitution ciphers that generated ciphertext *C* from plaintext *p* by means of an arithmetic operation modulo 26.

Caesar cipher: The Caesar cipher is an additive cipher. $C = p + (key) \bmod 26$. The number of keys is 26 – one of which produces plaintext. Decryption is accomplished by adding the additive inverse of the key to ciphertext $p = C + (-key) \bmod 26$.

Multiplicative cipher: $C = (key) \times p \bmod 26$. The number of keys is 12 – one of which produces plaintext. Decryption is accomplished by multiplying ciphertext by the multiplicative inverse of the key $p = C \times (key)^{-1} \bmod 26$.

Affine cipher: The affine cipher composes the multiplicative cipher and the Caesar cipher. (We will do the multiplicative cipher first and the Caesar cipher second.) $C = (multiplicative\ key) \times p + (additive\ key) \bmod 26$. The number of keys is $12 \times 26 = 312$ -- one of which produces plaintext.

Each of these can be attacked by frequency analysis – each ciphertext letter inherits all the frequency characteristics of the plaintext letter it replaces. It is easy to spot high frequency letters (e, t, a, o, i, n, s). a standard guess if that the highest frequency ciphertext letter corresponds to plaintext e and the next highest to plaintext t. For the Caesar cipher or the multiplicative cipher, it is only necessary to know one plaintext/cipehrtext correspondence ($\text{e} \leftrightarrow ?$) to solve for the key. For the affine cipher, only two plaintext/ciphertext correspondences are necessary to solve for the keypair $(multiplicative\ key, \quad additive\ key)$. A bit of trial and error usually produces the key.

One way to destroy the value of frequency analysis is to encrypt a string of letters as one block.

Here is an additive cipher that encrypts a block of four letters. Our plaintext messages split into blocks of four is

$$\begin{array}{cccc|cccc|cccc|cccc} n & o & r & t & h & e & r & n & k & e & n & t & u & c & k & y \end{array}$$

Numbers are substituted for letters by a = 1, b = 2, … , z = 26.

$$\begin{array}{cccc|cccc|cccc|cccc} n & o & r & t & h & e & r & n & k & er & n & t & u & c & k & y \\ 14 & 15 & 18 & 20 & 8 & 5 & 18 & 14 & 11 & 5 & 14 & 20 & 21 & 3 & 11 & 25 \end{array}$$

The key adds to each component of the block – thought of as a column vector – component-wise. For example, if the key were $\begin{bmatrix} 3 \\ 21 \\ 9 \\ 17 \end{bmatrix}$:

$$\begin{array}{c} n \\ o \\ r \\ t \end{array}\begin{bmatrix} 14 \\ 15 \\ 18 \\ 20 \end{bmatrix} + \begin{bmatrix} 3 \\ 21 \\ 9 \\ 17 \end{bmatrix} = \begin{bmatrix} 17 \\ 10 \\ 1 \\ 11 \end{bmatrix}\begin{array}{c} Q \\ J \\ A \\ K \end{array} \bmod 26$$

The block nort encrypts as QJAK.

Our message encrypts as:

$$\begin{array}{cccc|cccc|cccc|cccc} n & o & r & t & h & e & r & n & k & e & n & t & u & c & k & y \\ Q & J & A & K & K & Z & A & E & N & Z & W & K & X & X & T & P \end{array}$$

Decryption is accomplished by adding the additive inverse of the (vector) key to the ciphertext.

$$\text{plaintext} \underset{+\begin{bmatrix} 23 \\ 5 \\ 17 \\ 9 \end{bmatrix}}{\overset{+\begin{bmatrix} 3 \\ 21 \\ 9 \\ 17 \end{bmatrix}}{\rightleftarrows}} \text{CIPHERTEXT}$$

To encrypt a four-letter block, the key is a 4×1 matrix. There are $26^4 = 456076$ possible keys – one of which produces plaintext.

If we know one plaintext/ciphertext block correspondence, we can solve for the key.

This additive cipher is not truly a block cipher because changing one plaintext letter of a plaintext block changes only one letter of the corresponding ciphertext block.

A multiplicative cipher using matrices produces a true block cipher. Consider

$$\begin{bmatrix}5&6&4&1\\2&1&0&3\\1&8&9&2\\2&4&6&7\end{bmatrix}\begin{bmatrix}14\\15\\18\\20\end{bmatrix}\begin{matrix}\text{n}\\\text{o}\\\text{r}\\\text{t}\end{matrix}=\begin{bmatrix}18\\25\\24\\24\end{bmatrix}\begin{matrix}\text{R}\\\text{Y}\\\text{X}\\\text{X}\end{matrix}\bmod 26$$

and our message encrypts as

$$\begin{array}{cccc|cccc|cccc|cccc}\text{n}&\text{o}&\text{r}&\text{t}&\text{h}&\text{e}&\text{r}&\text{n}&\text{k}&\text{e}&\text{n}&\text{t}&\text{u}&\text{c}&\text{k}&\text{y}\\\text{R}&\text{Y}&\text{X}&\text{X}&\text{Z}&\text{X}&\text{D}&\text{H}&\text{E}&\text{I}&\text{I}&\text{F}&\text{J}&\text{P}&\text{L}&\text{I}\end{array}$$

Changing one letter of the plaintext block can change the entire ciphertext block because matrix multiplication “mixes” plaintext. Each plaintext letter is used in the calculation of each ciphertext letter. Claude Shannon in his 1949 paper “Communications Theory of Secrecy Systems” called this property diffusion.

Recall that for our simple substitution multiplicative cipher not all of the elements of the integers modulo 26 (i.e., 1, 2, … , 26) could be used as keys. That is because only those 12 elements that are relatively prime to 26 have multiplicative inverses modulo 26 (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25). A similar problem arises here; not all 4×4 matrices can be used as multiplicative encryption keys. Recall that a matrix has an inverse if and only if its determinant has an inverse. For the integers modulo 26 that means that a matrix can be a multiplicative key if and only if its determinant is one of 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, or 25. For the key above, the determinant is 23.

The method that we have just described is called the Hill cipher. It was described in a 1929 paper “Cryptography in an algebraic alphabet” by Lester S. Hill, who was a member of the mathematics faculty of Hunter College in New York City. The paper appeared in *The American Mathematical Monthly*.

Notice that if four four-block plaintext/ciphertext correspondences are known, then the resulting system of linear equations can be solved for the 16 entries in the encryption key.

How many encryption keys are there? For our example, there are

$$26^{16} = 43{,}608{,}742{,}899{,}428{,}874{,}059{,}776$$

4×4 matrices. The number of invertible matrices can be determined using results found in a paper that appeared in *Cryptologia* in January 2005 by Overby, Traves, and Wojdylo "On the keyspace of the Hill cipher." For 4×4 matrices there are

$$12{,}303{,}585{,}972{,}327{,}392{,}870{,}400$$

possible keys.

In a 1931 paper – also in the *Monthly* – Hill extends his ideas. He suggests using involutory (self-inverse) matrices as keys. This severely restricts the size of the keyspace. (See the paper by Overby, Traves, and Wojdylo.)

Why would Hill suggest involutory keys? The answer is that the calculation of the key inverse from the key is burdensome. Recall how the inverse of a matrix is constructed. Here is an example using a 2×2 encryption key.

Say, the encryption key is $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$.

It is easy to verify that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{bmatrix}$.

Notice that to calculate the inverse of the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ we must be able to divide by the determinant of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ = *ad* – *bc*; i.e., we must have a multiplicative inverse for the determinant *ad* – *bc*. Because we are working modulo 26, that means that the determinant *ad* – *bc* must be one of 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, or 25. Otherwise, the multiplication cannot be undone; encryption cannot be undone.

The determinant of $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ is $9 \times 7 - 4 \times 5 = 63 - 20 = 43 \equiv 17 \bmod 26$. Because 17 has a multiplicative inverse modulo 26, this matrix has an inverse. The inverse of the matrix is

$$\begin{bmatrix} \frac{7}{17} & \frac{-4}{17} \\ \frac{-5}{17} & \frac{9}{17} \end{bmatrix} \bmod 26.$$

Dividing by 17 modulo 26 is the same as multiplying by the multiplicative inverse of 17 modulo 26. Recall that the multiplicative inverse of 17 is 23 modulo 26. So, the inverse of the matrix is

$$\begin{bmatrix} \frac{7}{17} & \frac{-4}{17} \\ \frac{-5}{17} & \frac{9}{17} \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \times 23 & -4 \times 23 \\ -5 \times 23 & 9 \times 23 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 161 & -92 \\ -115 & 207 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \bmod 26$$

For the encryption key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ the decryption key is $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix}$.

$$\text{plaintext} \underset{\times\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix}}{\overset{\times\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}}{\rightleftarrows}} \text{CIPHERTEXT}$$

Calculating the determinant of an $n \times n$ matrix with $n > 2$ and is more difficult, and calculating the inverse of an $n \times n$ matrix with $n > 2$ differs from calculating the inverse of a 2×2 matrix.

In his 1931 paper, Hill also extended his ideas to affine encryption. For example,

$$\begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 4 & 11 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} 8 \\ 3 \end{bmatrix}$$

Where the plaintext block is $x_1 x_2$ and the ciphertext block is $Y_1 Y_2$.