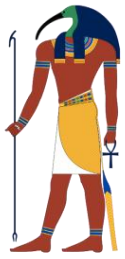

Píldora nº 21: ¿Qué es la cifra por matrices de Hill?

Escena 1: La figura de Lester Hill

Lester Hill fue un matemático neoyorquino que nace en 1891 y fallece a los 70 años en 1961. Profesor en las universidades de Yale, Princeton, Montana y Hunter College, gran parte de su investigación la dedica a la criptografía, siendo su aporte más conocido el invento en 1929 del sistema de cifra que lleva su nombre, basado en operaciones con matrices.

Se trata de una cifra por sustitución poligrámica mediante la multiplicación de matrices, de la que también crea una máquina con engranajes y cadenas para operar con claves de seis letras. Como la clave debía quedar fija para cada máquina, su sistema no pudo competir con otras máquinas de cifrar de la época con mayor fortaleza, como era el caso de la Enigma con rotores intercambiables y ajustables. Aunque el sistema de cifra de Hill puede llegar a tener espacios de clave inmensos, mayores incluso que los sistemas de cifra modernos, su talón de Aquiles es que no resiste un ataque con texto en claro conocido.

Escena 2: El cifrado y descifrado propuesto por Hill

Hill plantea el problema de la cifra como un conjunto de cuatro ecuaciones, cifrando bloques de cuatro letras.

$$y_1 = 8\,x_1 + 6\,x_2 + 9\,x_3 + 5\,x_4 \bmod 26$$

$$y_2 = 6\,x_1 + 9\,x_2 + 5\,x_3 + 10\,x_4 \bmod 26$$

$$y_3 = 5\,x_1 + 8\,x_2 + 4\,x_3 + 9\,x_4 \bmod 26$$

$$y_4 = 10\,x_1 + 6\,x_2 + 11\,x_3 + 4\,x_4 \bmod 26$$

Donde x_i es cada una de las cuatro letras del bloque de texto en claro, y_i es el resultado de la cifra y los valores (8, 6, 9, 5) (6, 9, 5, 10) (5, 8, 4, 9) (10, 6, 11, 4) forman la clave aleatoria K

para cifrar cada bloque de cuatro letras. Para ello utiliza el alfabeto de 26 elementos con las letras mayúsculas del inglés, pero distribuidas de una manera particular definida por Hill.

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
5	23	2	20	10	15	8	4	18	25	0	16	13	7	3	1	19	6	12	24	21	17	14	22	11	9

Así, el mensaje DELAY OPERATIONS que originalmente usó su creador, vendrá expresado por estos cuatro vectores: DELA (20 10 16 5), YOPE (11 3 1 20), RATI (6 5 24 18) y ONSU (3 7 12 21), en donde la letra U=21 ha sido usada como relleno. La cifran del primer bloque de cuatro letras se muestra a continuación:

$y_1 = 8\ x_1 + 6\ x_2 + 9\ x_3 + 5\ x_4 \bmod 26$

$y_1 = (8 \times 20) + (6 \times 10) + (9 \times 16) + (5 \times 5) \bmod 26 = 4 + 8 + 14 + 25 \bmod 26 = 25;\ y_1 = J$

$y_2 = 6\ x_1 + 9\ x_2 + 5\ x_3 + 10\ x_4 \bmod 26$

$y_2 = (6 \times 20) + (9 \times 10) + (5 \times 16) + (10 \times 5) \bmod 26 = 16 + 12 + 2 + 24 \bmod 26 = 2;\ y_2 = C$

$y_3 = 5\ x_1 + 8\ x_2 + 4\ x_3 + 9\ x_4 \bmod 26$

$y_3 = (5 \times 20) + (8 \times 10) + (4 \times 16) + (9 \times 5) \bmod 26 = 22 + 2 + 12 + 19 \bmod 26 = 3;\ y_3 = O$

$y_4 = 10\ x_1 + 6\ x_2 + 11\ x_3 + 4\ x_4 \bmod 26$

$y_4 = (10 \times 20) + (6 \times 10) + (11 \times 16) + (4 \times 5) \bmod 26 = 18 + 8 + 20 + 20 \bmod 26 = 14;\ y_4 = W$

El primer bloque de texto en claro DELA se ha cifrado como JCOW. Finalmente la cifra del mensaje DELAY OPERATIONS será JCOW ZLVB DVLE QMXC. Para descifrar y_i con esta clave y encontrar los valores x_i del mensaje, se usará en este caso otro sistema de cuatro ecuaciones:

$x_1 = 23\ y_1 + 20\ y_2 + 5\ y_3 + 1\ y_4 \bmod 26$

$x_2 = 2\ y_1 + 11\ y_2 + 18\ y_3 + 1\ y_4 \bmod 26$

$x_3 = 2\ y_1 + 20\ y_2 + 6\ y_3 + 25\ y_4 \bmod 26$

$x_4 = 25\ y_1 + 2\ y_2 + 22\ y_3 + 25\ y_4 \bmod 26$

Observa que la clave para el descifrado (23 20 5 1) (2 11 18 1) (2 20 6 25) (25 2 22 25) es diferente a la clave usada en el cifrado. Si la clave para cifrado era aleatoria, ¿cómo se obtiene entonces la clave para el descifrado? La respuesta está en que la cifra de Hill es una cifra por multiplicación de matrices y esa matriz clave de descifrado deberá ser la matriz inversa a la matriz clave cifrado en el módulo, en este caso 26.

Escena 3: Cifrando y descifrando con Hill usando matrices

Podemos representar en forma de matrices los dos sistemas de ecuaciones propuestos por Hill para el cifrado y el descifrado:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \bmod 26 \qquad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 23 & 20 & 5 & 1 \\ 2 & 11 & 18 & 1 \\ 2 & 20 & 6 & 25 \\ 25 & 2 & 22 & 25 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} \bmod 26$$

En otras palabras, para cifrar y descifrar se realizarán dos operaciones matriciales diferentes:

Cifrado: $[y] = [k]\,[x] \bmod n$ Descifrado: $[x] = [k^{-1}]\,[y] \bmod n$

La matriz inversa de k en el cuerpo de cifra n, que se escribe k^{-1} es: $k^{-1} = [\text{adj}\,(k)]^T/\det k \bmod n$.

Escena 4: Condiciones que debe cumplir la matriz clave K

La cifra poligrámica de Hill con d caracteres requerirá una matriz clave k que tenga inversa en ese cuerpo de cifra.

$$k = \begin{pmatrix} k11 & k12 & \ldots & k1d \\ k21 & k22 & \ldots & k2d \\ \ldots & \ldots & \ldots & \ldots \\ kd1 & kd2 & \ldots & kdd \end{pmatrix} \bmod n$$

Los valores k_{ij} serán números enteros aleatorios que se encuentren dentro del módulo de cifra n, aunque en general puede ser cualquier número entero.

Como en la ecuación de la inversa aparece la expresión (1/det k), la matriz k deberá cumplir las siguientes condiciones para que sea válida:

a) No puede ser singular, es decir su determinante no puede ser cero en tanto se encuentra en el denominador de la ecuación de la matriz inversa.
b) El determinante de k no podrá tener factores en común con el módulo n porque en ese caso no existiría el inverso en el cuerpo de cifra.

Madrid, diciembre de 2014

Autor del guion: *Jorge Ramió Aguirre*

Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*

creative commons
Attribution
Noncommercial
No derivative works