Cifrado de Hill

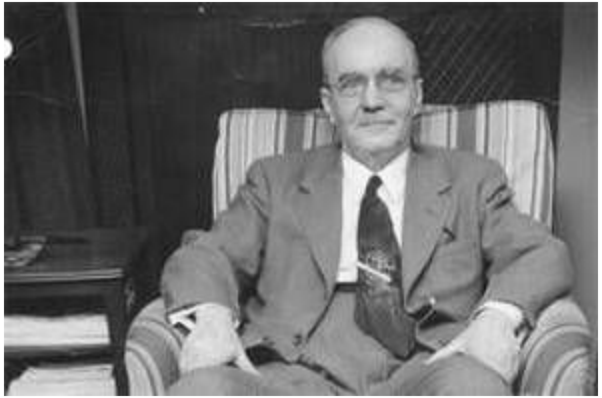
Canek García [kaan.ek@ciencias.unam.mx]

Agenda

- Breve historia
- Criptosistema
- Ejemplo
- Referencias

Breve historia...

- El algoritmo data de 1929 y fue descrito por el matemático Lester S. Hill a través de un artículo publicado en el diario de Nueva York.
- Es un cifrado de sustitución poligráfica basado en el álgebra lineal, específicamente las reglas del álgebra de matrices con la intención de mejorar las técnicas de cifrado utilizadas entonces.



Criptosistema

Cifrado

1. Asignar un valor numérico a cada letra del alfabeto a utilizar iniciando en 0.
2. La **clave** a utilizar debe constar de tantas letras como se desee siempre que sea posible calcular los equivalentes numéricos de cada una de ellas en una matriz de **N**x**N**, es decir una **matriz cuadrada** (**K**).
3. El **mensaje** (**Mcla**) se divide en **diagramas**, **trigramas** o **N-gramas** necesarios, tal que sus equivalentes sean colocados en matrices de **Nx1**
4. El **criptograma** se obtiene multiplicando las matrices **K** * **Mcla**, esto es:

$$C(Nx1) = K\ (NxN) * Mcla(Nx1)$$

Descifrado

- El mensaje en claro se recupera llevando a cabo el proceso inverso.

Nota: Todos las operaciones aritméticas se realizan con módulo **N**, donde **N** corresponde al tamaño del alfabeto que se esté empleando.

Ejemplo

Ejemplo

N = **27**
Mensaje (Mcla) = **CONSUL**
Clave (K) = **FORTALEZA**

1.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
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	26

2. Formar la matriz cuadrada para la **Clave (K)**:

$$K = \begin{pmatrix} 5 & 15 & 18 \\ 20 & 0 & 11 \\ 4 & 26 & 0 \end{pmatrix}$$

3. Obtener **N-gramas** (en este ejemplo trigramas) de **Mensaje (Mcla)**:

M1 = CON

M2 = SUL

$$M_1 = \begin{pmatrix} 2 \\ 15 \\ 13 \end{pmatrix} \quad M_2 = \begin{pmatrix} 19 \\ 21 \\ 11 \end{pmatrix}$$

4. Obtenemos el **criptograma** multiplicando **$K*M_1$** y **$K*M_2$**:

$$K * M_1 = \begin{pmatrix} 5 & 15 & 18 \\ 20 & 0 & 11 \\ 4 & 26 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 15 \\ 13 \end{pmatrix} = \begin{pmatrix} 469 \\ 183 \\ 398 \end{pmatrix} = \begin{pmatrix} 10 \\ 21 \\ 20 \end{pmatrix} mod\ 27 = \begin{pmatrix} K \\ U \\ T \end{pmatrix}$$

$$K * M_2 = \begin{pmatrix} 5 & 15 & 18 \\ 20 & 0 & 11 \\ 4 & 26 & 0 \end{pmatrix} \begin{pmatrix} 19 \\ 21 \\ 11 \end{pmatrix} = \begin{pmatrix} 608 \\ 501 \\ 622 \end{pmatrix} = \begin{pmatrix} 14 \\ 15 \\ 1 \end{pmatrix} mod\ 27 = \begin{pmatrix} \tilde{N} \\ O \\ B \end{pmatrix}$$

5. Recuperamos el criptograma: **KUTÑOB**

Descifrando:

1. Calcular K^{-1} :

$$K^{-1} = \begin{pmatrix} -286 & 468 & 165 \\ 44 & -2 & -70 \\ 165 & 305 & -300 \end{pmatrix} * 7 = \begin{pmatrix} -2002 & 3276 & 1155 \\ 308 & -504 & 2135 \\ 3640 & -490 & -2100 \end{pmatrix} = \begin{pmatrix} 23 & 9 & 21 \\ 11 & 9 & 2 \\ 22 & 23 & 6 \end{pmatrix} mod\ 27$$

2. Multiplicar por los N-gramas obtenidos en el criptograma:

$$K^{-1} * C_1 = \begin{pmatrix} 23 & 9 & 21 \\ 11 & 9 & 2 \\ 22 & 23 & 6 \end{pmatrix} \begin{pmatrix} 10 \\ 21 \\ 20 \end{pmatrix} = \begin{pmatrix} 839 \\ 339 \\ 823 \end{pmatrix} = \begin{pmatrix} 2 \\ 15 \\ 13 \end{pmatrix} mod\ 27 = \begin{pmatrix} C \\ O \\ N \end{pmatrix}$$

$$K^{-1} * C_2 = \begin{pmatrix} 23 & 9 & 21 \\ 11 & 9 & 2 \\ 22 & 23 & 6 \end{pmatrix} \begin{pmatrix} 14 \\ 15 \\ 1 \end{pmatrix} = \begin{pmatrix} 478 \\ 291 \\ 659 \end{pmatrix} = \begin{pmatrix} 19 \\ 21 \\ 11 \end{pmatrix} mod\ 27 = \begin{pmatrix} S \\ U \\ L \end{pmatrix}$$

Referencias

- https://es.wikipedia.org/wiki/Cifrado_Hill
- https://unamcriptografia.wordpress.com/category/tecnicas-clasicas-de-cifrado/sustitucion/monoalfabetica/poligramica/hill/