Criptografía

Cifrados de 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
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	0

Figura 1: Lester S. Hill

En lo sucesivo asumiremos que cada letra de un texto o un texto cifrado se le asigna su respectivo lugar en el alfabeto, excepto por la Z, la cual valdrá 0, como se puede ver en la tabla.
En los cifrados de Hill más simples, se toman pares sucesivos de texto y se transforman en texto cifrado de acuerdo al siguiente procedimiento

1. Se elige una matriz $A \in M_{2\times 2}(\mathbb{Z})$, digamos $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, la cual ejecutará el codificado.
2. Dado un texto, se agrupan las letras por pares, se agrega un *comodín* para llenar completar un par, y se reemplaza cala letra por su respectivo valor de acuerdo a la tabla.
3. Se toman los pares y se forman los vectores $\mathbf{p} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$. Se forma el producto $A\mathbf{p}$. Llamaremos al vector $\mathbf{p}$ un **vector de texto** y $A\mathbf{p}$ el correspondiente **vector cifrado**.
4. Se convierte cada cifrado en su equivalente alfabético.

Ejemplo 1. *Usemos la matriz* $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$, *para cifrar el mensaje* HOLA MUNDO

Nota 1. *Como el mensaje se agrupó por pares y se usó una matriz* 2×2, *estamos hablando de un* **2-cifrado de Hill**. *Es posible agrupar en tripletas el mensaje y usar una matriz de* 3×3, *en este caso tendríamos un* **3-cifrado de Hill**. *Podemos continuar sucesivamente y agrupar el mensaje en grupos de tamaño* n *y usar una matriz de* $n \times n$, *tendríamos un* **n-cifrado de Hill**.

Definición 1. *Si* a *es un elemento en* $\mathbb{Z}_m$, *entonces* a^{-1} *es su inverso multiplicativo (o recíproco) de* a *módulo* m *si* $a \cdot a^{-1} = a^{-1} \cdot a \equiv 1 \mod m$

Criptografía

Nota 2. *El elemento* $4 \in \mathbb{Z}_{26}$ *no tiene inverso, lo mismo sucede con los elementos pares. La tabla a continuación enlista los inversos en* $\mathbb{Z}_{26}$.

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Decodificando

Para devolver el mensaje a su forma original se toma una matriz A cuyas entradas son elementos de $\mathbb{Z}_m$, diremos que A es **invertible módulo** m si existe una matriz B con entradas en $\mathbb{Z}_m$ tal que

$$A \cdot B = B \cdot A \equiv I \mod m$$

En este tipo de cifrado es importante saber cuándo una matriz es invertible módulo m.

Teorema 1. *Una matriz* A *de tamaño* $n \times n$ *con entradas en* $\mathbb{Z}_m$ *es invertible módulo* m *si y solo si* $\det A \equiv r \mod m$ *tiene inverso multiplicativo en* $\mathbb{Z}_m$.

Corolario 2. *Una matriz* A *de tamaño* $n \times n$ *con entradas en* $\mathbb{Z}_m$ *es invertible módulo* m *si y solo si el residuo de* $\det A \mod m$ *no tiene factores primos en común con* m.

Corolario 3. *Una matriz* A *de tamaño* $n \times n$ *con entradas en* $\mathbb{Z}_{26}$ *es invertible módulo* 26 *si y solo si el residuo de* $\det A \mod 26$ *no es divisible por* 2 *o* 13.

Ejemplo 2. *Determinar la inversa de la matriz*

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \mod 26.$$

Ejemplo 3. *Decodificar el mensaje, el cual fue encriptado usando la matriz del ejemplo anterior*

GTNKGKDUSK

¿Quieres saber más?

1. Sinkov, A.; *Elementary Cryptanalysis, a mathematical approach.* Mathematical Association fo America, 2009.

2. Konheim, A.; *Cryptography, a primer.* Wiley- Interscience, New York 1981.

3. Smart, N.; *Cryptography Made Simple.* Springer, New York 2016.