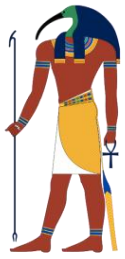

Píldora nº 17: ¿Qué es la cifra afín?

Escena 1: Cifradores por sustitución genéricos

Se conocen como cifradores por sustitución genéricos monográmicos monoalfabéticos a aquellos sistemas de cifra clásica que obtienen el alfabeto de cifrado a partir de la ecuación (c = a*m + b mod n), en donde a es una constante de multiplicación, b una constante de desplazamiento y n el cuerpo de cifra. Como en inglés se utiliza la palabra decimation para esta operación de multiplicación, cuyo significado es aniquilar selectivamente o diezmar, es común que en español se use decimación, si bien esta palabra no está recogida en la RAE.

Así, cuando la constante de desplazamiento b es igual a 0, hablaremos de una cifra por decimación pura; si la constante de decimación a es igual a 1, hablaremos de una cifra por desplazamiento puro y si no se dan estas dos condiciones, hablaremos de una cifra afín.

Si a un alfabeto módulo 27 se le aplica una decimación a igual a 2, las letras se distribuyen ahora en saltos de dos espacios debido a esa multiplicación del código por 2. Si ahora se le añade un desplazamiento b igual a 4, se obtiene el alfabeto final para la ecuación de cifra c = 2*m + 4 mod 27.

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
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
A	C	E	G	I	K	M	Ñ	P	R	T	V	X	Z	B	D	F	H	J	L	N	O	Q	S	U	W	Y
E	G	I	K	M	Ñ	P	R	T	V	X	Z	B	D	F	H	J	L	N	O	Q	S	U	W	Y	A	C

Escena 2: Condiciones para la cifra por decimación pura y cifra afín

En tanto existe en estos sistemas una multiplicación del código numérico de la letra a cifrar por un número, será necesario que la constante de decimación a tenga inverso multiplicativo en n, esto es que mcd (a, n) = 1.

Por ejemplo, en módulo 27 será válida la ecuación de cifra c = 11*m – 3 mod 27 porque el inverso de 11 en 27 es igual a 5, pero no será válida la ecuación c = 6*m - 3 mod 27 pues no existe ahora el inverso de 6 en 27. Podríamos cifrar un mensaje, pero no seremos capaces de descifrarlo.

Escena 3: Cifrado en modo afín

Si ciframos el mensaje HOLA con la cifra afín c = 11*m - 3 mod 27, se obtiene TAKX.

H = 7	7*11 – 3 = 74 mod 27 = 20	T
O = 15	15*11 – 3 = 162 mod 27 = 0	A
L = 11	11*11 – 3 = 118 mod 27 = 10	K
A = 0	0*11 – 3 = -3 mod 27 = 24	X

Escena 4: Descifrado en modo afín

La operación de descifrado en modo afín será m = (c – b) * inv (a, n) mod n.

Como por el ejemplo anterior sabemos que inv (11, 27) = 5, descifraremos el criptograma TAKX siguiendo esta ecuación y recuperamos el texto en claro HOLA.

T = 20	[20 – (-3)]*5 = 115 mod 27 = 7	H
A = 0	[0 – (-3)]*5 = 15 mod 27 = 15	O
K = 10	[10 – (-3)]*5 = 65 mod 27 = 11	L
X = 24	[24 – (-3)]*5 = 135 mod 27 = 0	A

Escena 5: Espacio de claves y fortaleza

El sistema afín en módulo 27 tendrá 26 valores válidos para la constante b y 17 valores válidos para la constante a por lo que podremos formar hasta 26*17, es decir 442 alfabetos diferentes. Sin embargo, la cifra seguirá siendo muy débil incluso ante ataques por fuerza bruta.

Madrid, noviembre de 2014

Autor del guion: *Jorge Ramió Aguirre*

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