Breve Descripción y Comentario del Cifrado Afín

Fco. M. García Olmedo
Universidad de Granada
España

21 de noviembre de 2017

Resumen

Contiene una exposición somera del cifrado según el llamado "Criptosistema Afín".

Índice

Índice de figuras

1. Descripción del Cifrado Afín

Los criptosistemas afines son un ejemplo de cifrado monoalfabético por sustitución. El algoritmo parte de una biyección entre el alfabeto —para fijar ideas supondremos el alfabeto latino de 41 símbolos— y el segmento inicial de números naturales con 41 números. Ejemplo de ello está dado en la Figura 1.

El **cifrado** consiste en asociar al número que representa a cada letra del texto llano otro número, que es su cifra, y presentarlo como la letra que corresponde a este nuevo número; de esta forma se obtiene el texto cifrado. La regla de transformación de números es la dada por la fórmula $C(x) = (ax + b) \pmod N$, donde: N es el número de letras del alfabeto (41 en este caso), a es un número natural tal que $0 \leq a \leq N - 1$ cumpliendo $(a, N) = 1$ y b es un número natural tal que $0 \leq b \leq N - 1$.[1]

La función de **descifrado** sería $D(x) = (a'x + b') \pmod N$, donde $a' = a^{-1} \pmod N$ y $b' = -a^{-1}b \pmod N$. Si el número a elegido cumpliese $1 < (a, N)$, es fácil ver que más de un texto llano se podría cifrar en el mismo texto cifrado, de forma que no se podría recuperar de forma única el texto llano del cifrado.

Una vez calculadas estas llaves, para descifrar basta usar la función de cifrado con estas nuevas llaves.

[1] La notación (m, n) se usa para representar el máximo común divisor de los números enteros m y n.

2. Ejemplo

Se expone a continuación un **ejemplo de Cifrado.** Si se escoge la llave de cifrado $\langle 13, 5\rangle$ para cifrar con ella el recado:

```
el poder desgasta ... a quien no lo tiene
```

resulta el mensaje cifrado

```
2.eh9p27ep2fnrfsregggereu5:2wew9e.9es:2w2
```

3. Casos Particulares

Tienen especial interés estos dos casos particulares del sistema de cifrado afín:

1. $a = 1$; el cifrado afín da lugar en este caso a una mera traslación del alfabeto, el conocido como sistema de "Cifrado de Cesar" que hemos aludido y que era el utilizado por Provenzano.

2. $b = 0$; el cifrado afín da lugar en este caso a una transformación lineal, nombre que indica que esta transformación lleva sumas en sumas: si C_i es el cifrado de P_i para $i = 1, 2$, entonces $C_1 + C_2$ es el cifrado de $P_1 + P_2$ (por supuesto, sumamos módulo N).

	0	g	7	n	14	u	21	1	28	8	35
a	1	h	8	o	15	v	22	2	29	9	36
b	2	i	9	p	16	w	23	3	30	,	37
c	3	j	10	q	17	x	24	4	31	.	38
d	4	k	11	r	18	y	25	5	32	;	39
e	5	l	12	s	19	z	26	6	33	:	40
f	6	m	13	t	20	0	27	7	34		

Figura 1: Enumeración del alfabeto.