Códigos y Criptografía (GIINF)

Practica Cifrado Afín

1. Convertir la siguiente cadena a números, usando la identificación con Z 27 :

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*
0	1	2	3	4	5	6	7	8	9	10	11	12	13
ñ	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*	
14	15	16	17	18	19	20	21	22	23	24	25	26	

Cadena a cifrar: 'Hola, buenos dias'
Cadena cifrada: 7 15 11 0 1 21 4 13 15 19 3 8 0 19

2. ¿Cuáles de los siguientes valores representan una clave válida para el cifrado afín?:

Para saber si son clave válida debemos de aplicar el teorema de Bezout:

- k=3 , d=2

  Esta clave no es valida, pues a la hora de operar el resto de la division de 27/3 es igual a cero. Con lo cual no tiene inverso modular en Z27.

- k=2 , d=2

  Esta clave si es valida puesto que el mcd(2,27) es igual a 1. Son primos relativos y por ello tiene inversa.

3. Cifrar el texto del ejercicio 1 con el método afín, usando para ello la clave que haya resultado válida en el apartado anterior.

Cadena a cifrar: 'Hola, buenos dias'

Para ellos usamos la formula: $X \rightarrow k \cdot X+d \bmod 27$, donde X es el numero de entrada, k es 2 y d es 2.

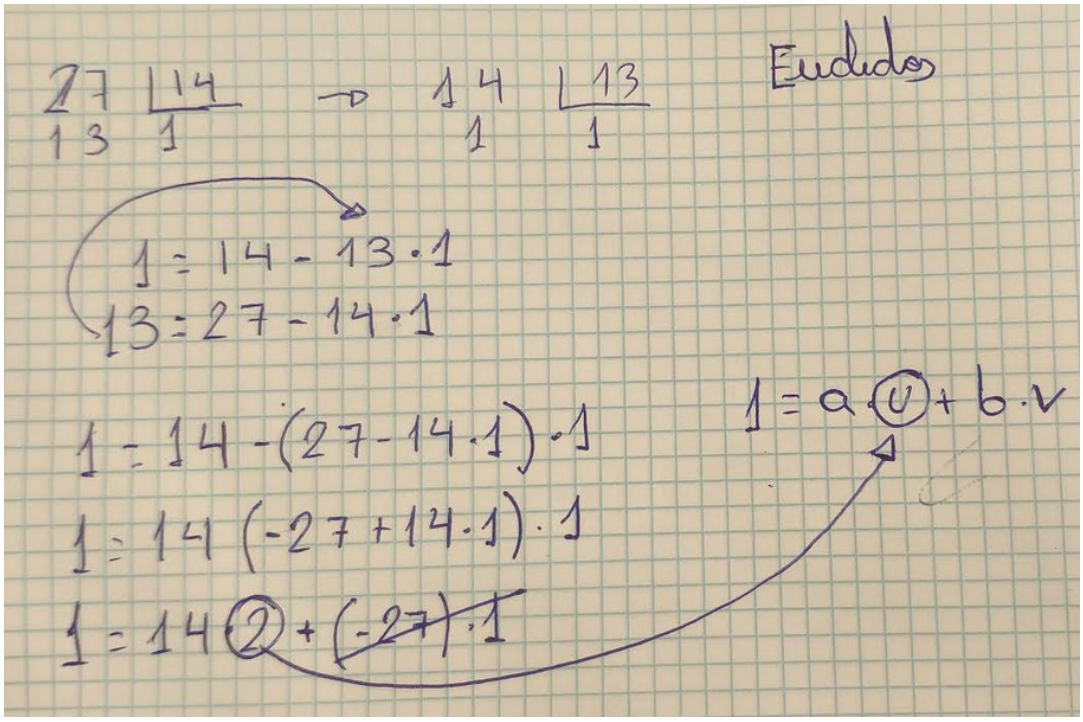
- $X=7 \rightarrow 2 \cdot 7+2 \bmod(27)$ ------> **16**
- $X=15 \rightarrow 2 \cdot 15+2 \bmod(27)$ ------> **5**
- $X=11 \rightarrow 2 \cdot 11+2 \bmod(27)$ ------> **24**
- $X=0 \rightarrow 2 \cdot 0+2 \bmod(27)$ ------> **2**
- $X=1 \rightarrow 2 \cdot 1+2 \bmod(27)$ ------> **4**
- $X=21 \rightarrow 2 \cdot 21+2 \bmod(27)$ ------> **17**
- $X=4 \rightarrow 2 \cdot 4+2 \bmod(27)$ ------> **10**
- $X=13 \rightarrow 2 \cdot 13+2 \bmod(27)$ ------> **1**
- $X=15 \rightarrow 2 \cdot 15+2 \bmod(27)$ ------> **5**
- $X=19 \rightarrow 2 \cdot 19+2 \bmod(27)$ ------> **13**
- $X=3 \rightarrow 2 \cdot 3+2 \bmod(27)$ ------> **8**
- $X=8 \rightarrow 2 \cdot 8+2 \bmod(27)$ ------> **18**
- $X=0 \rightarrow 2 \cdot 0+2 \bmod(27)$ ------> **2**
- $X=19 \rightarrow 2 \cdot 19+2 \bmod(27)$ -----→ **13**

4. Descifrar el siguiente mensaje 'j d q b j d w h i l z', sabiendo que se ha cifrado mediante el método afín siendo las claves k = 14 y d = 7.
NOTA: Hay que comprobar previamente que se trata de una clave válida.

Para saber si es clave valida usamos el método de euclides hasta encontrar el resto de 1, lo que significa que son primos relativos.

27/14, da como resultado 1 de cociente y 13 de resto.
14/13, da como resultado 1 de cociente y **1 de resto.(Tiene inverso y es clave valida)**

Para descifrar se usara la expresión: Descifrado: $X \rightarrow k^{-1} (X + (-d)) \bmod 27$



➔ -d(Opuesto de d),-7 = 20 mod(27)
➔ k(Inverso de k),14 = 2 mod(27)

- X= j → 2 (9 + (20)) mod 27 ---- 4
- X= d → 2(3 + (20)) mod 27 ---- 19
- X= q→ 2(17 + (20)) mod 27 ---- 20
- X= b→ 2(1 + (20)) mod 27 ---- 15
- X= j→ 2(9 + (20)) mod 27 ---- 4
- X= d→ 2(3 + (20)) mod 27 ---- 19
- X= w → 2(23 + (20)) mod 27 —- 5
- X= h→ 2(7 + (20)) mod 27 ---- 0
- X= i→ 2(8 + (20)) mod 27 ---- 2
- X= l→ 2(11 + (20)) mod 27 ---- 8
- X= z→ 2(26 + (20)) mod 27 ---- 11

Mensaje en numérico **'4 19 20 15 4 19 5 0 2 8 1'**
Mensaje en letra **'esto es facil'**

5. Se ha interceptado el siguiente criptograma: ’a e j m j w y j ñ e h e f f j m b k’.
Vamos a tratar de criptoanalizarlo mediante un análisis de frecuencias.
Para ello:

Pasamos de texto a digitos:
’a e j m j w y j ñ e h e f f j m b k’ = '0 4 9 12 9 23 25 9 14 4 7 4 5 5 9 12 1 10'
Tenemos un total de 18 letras o 18 dígitos transformados.

(a) Escribe una tabla de frecuencias de las letras del criptograma y ordenarlas de mas a menos frecuente.

Letra	Cantidad de Apariciones	Porcentaje de apariciones
j	4	4/18=**0.222**
e	3	3/18=**0.166**
m	2	2/18=**0.111**
f	2	2/18=**0.111**
a	1	1/18=**0.055**
b	1	1/18=**0.055**
w	1	1/18=**0.055**
y	1	1/18=**0.055**
ñ	1	1/18=**0.055**
h	1	1/18=**0.055**
k	1	1/18=**0.055**

(b) Compara la tabla con las frecuencias de las letras en español e identifica dos posibles parejas.

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*
12.53	1.42	4.68	5.86	13.68	0.69	1.01	0.70	6.25
j	*k*	*l*	*m*	*n*	*ñ*	*o*	*p*	*q*
0.44	0.02	4.97	3.15	6.71	0.31	8.68	2.51	0.88
r	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
6.87	7.98	4.63	3.93	0.90	0.01	0.22	0.90	0.52

Ilustración 1: Frecuencias mas usadas en Español

X1 → Y1 = j → e = **9 → 4**
X2 → Y2 = e → a = **4 → 0**

(c) Construye la matriz correspondiente a esas dos identificaciones e intentemos calcular la inversa modular.

$$\left.\begin{aligned} y_1 &= k\,x_1 + d \\ y_2 &= k\,x_2 + d \end{aligned}\right\}$$

$$\begin{pmatrix} k \\ d \end{pmatrix} = \begin{pmatrix} 9 & 1 \\ 4 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 4 \\ 0 \end{pmatrix} - - - \begin{pmatrix} k \\ d \end{pmatrix} = \begin{pmatrix} 11 & 16 \\ 10 & 18 \end{pmatrix} \begin{pmatrix} 4 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} k \\ d \end{pmatrix} = \begin{pmatrix} 44 \\ 40 \end{pmatrix} - - - \begin{pmatrix} k \\ d \end{pmatrix} = \begin{pmatrix} 17 \\ 13 \end{pmatrix}$$

Comprobamos con euclides la K y efectivamente mcd(17,27)=1

(d) Intentamos criptoanalizar usando la matriz anterior.

Una vez sacados los valores de **K** y **D** usamos la formula de descifrado del método afín para descifrar el mensaje. Puede ser que estos valores no sean coherentes a la hora de realizar el descifrado y por ello ser necesario volver a calcular los valores de **K** y **D**.

(e) ¿Qué haríamos en caso de obtener un texto sin sentido?

Si encontramos un texto sin sentido puede ocurrir dos cosas, que sea un texto que evidentemente haya sido creado a mala voluntad para despistar, o que aquellos valores sacados de K y D no sean los correctos para este descifrado con lo que conllevaría volver a re-calcular estos valores basándonos en nuevas parejas del frecuencias del lenguaje y volver a probar. Puede ser que nos tiremos muchos intentos hasta encontrar unos buenos valores.