Evaluación 3: Parte 1

Carrillo García Aldo

Hernández Flores Luis Ángel

Macedo Madrigal Rodrigo

Polo Monroy Ricardo

Vázquez Andrés Mónica

2020 Enero

1. Ejercicio 1

Mediante un análisis de frecuencias decifrar el siguiente texto que fue cifrado usando una traslación de la forma $C \equiv P + K$ mód 27:

SIBMW ZPILM UCTMZ WAMAP TXWZB IUBMM UMSMA BCLPW LMSIK ZPXBW SWÑPI

Solución:

Lo primero que tenemos que revisar el el número de ocurrencias de cada letra dentro de la frase, así, haciendo un conteo obtenemos:

Letra	Repeticiones
M	9
W	5
B	5
P	4
Z	4
I	4
A	3
U	3
L	3
S	3
X	2
T	2
C	2
K	1

Una vez obtenidos estos valores, podemos notar que la letra con mayor número de repeticiones es M con un total de 9.
Luego, con los valores obtenidos en clase sabemos que la letra que mas se repite dentro del lenguaje Español es la E y usamos sus respectivos valores dentro del abecedario.

$$E = 4 \ y \ M = 12 \tag{1}$$

Como la M corresponde a la E, hacemos el desplazamiento $12 - 4 = 8$ y así nos queda la traslación utlizada para encriptar el mensaje es de la forma

$$C \equiv P + 8 \text{ mód } 27$$

Y podemos obtener que la traslación que necesitamos para obtener el mensaje es:

$$C \equiv P - 8 \text{ mód } 27$$

la cual usaremos para obtener el mensaje deseado.

Ahora podemos construir todo nuestro abecedario con el desplazamiento obtenido

Alfabeto Original	Posición	Alfabeto trasladado
A	0	I
B	1	J
C	2	K
D	3	L
E	4	M
F	5	N
G	6	Ñ
H	7	O
I	8	P
J	9	Q
K	10	R
L	11	S
M	12	T
N	13	U
Ñ	14	V
O	15	W
P	16	X
Q	17	Y
R	18	Z
S	19	A
T	20	B
U	21	C
V	22	D
W	23	E
X	24	F
Y	25	G
Z	26	H

Una vez obtenida la tabla anterior, podemos decifar el mensaje:

"LA TEORIA DE NUMEROS ES IMPORTANTE EN EL ESTUDIO DE LA CRIPTOLOGÍA"

2. Ejercicio 2

Madiante un análisis de frecuencias, desencriptar el siguiente texto que fue encriptado usando una transformación afín:

TFVS FMKK BUKB CKÑL BFSK MFGL KTFM CKUO ÑMFV DOBO KNMF VIII

Solución:

Realizando un análisis de frecuencias, observamos que cada letra tiene el siguiente número de apariciones en el text:

Letra	Número de apariciones
G	1
D	1
N	1
T	2
S	2
U	2
C	2
Ñ	2
L	2
V	3
O	3
I	3
B	4
M	5
F	7
K	8

Así, podemos observar que las letras que mas se repiten son la K con 8 apariciones y la F con 7.

Con esta información podemos asociar a las letras del abecedario que mas se repiten, en este caso la E en primer lugar y en segundo lugar la A.

$$\mathrm{E} = 4 \rightarrow \mathrm{K} = 10$$

$$\mathrm{A} = 0 \rightarrow \mathrm{F} = 5$$

Y usando una transformación afín, obtenemos que

$$10 \equiv a * 4 + b \text{ mód } 27$$
$$5 \equiv a * 0 + b \text{ mód } 27$$

Así, como $b \equiv 5$ mód 27, podemos asignar a la primera congruencia, obteniendo que

$$10 \equiv 4a + 5 \text{ mód } 27$$

Y lo único que haría falta encontrar sería el valor de "a" tal que $5 \equiv 4a$ mód 27. Si $a = 8$ entonces tenemos que

$$a \equiv 8 \text{ mód } 27$$
$$b \equiv 5 \text{ mód } 27$$

Por lo que la transformación de encriptación es:

$$C \equiv 8P + 5 \text{ mód } 27$$

Ahora, con esta información necesitamos encontrar una transformación para desencriptar el mensaje:

$$P \equiv 8^{-1}(C - 5) \text{ mód } 27 \rightarrow P \equiv 17(C - 5) \text{ mód } 27$$

Siendo esta última nuestra transformación para desencriptar.

Así, obtenemos

Letra Cifrada	Posición en el alfabeto	Transformación aplicada	Letra descifrada
T	20	12	M
F	5	0	A
V	22	19	S
S	19	22	V
M	12	11	L
K	10	4	E
B	1	13	N
U	21	2	C
C	2	3	D
Ñ	14	18	R
L	11	21	U
G	6	17	Q
O	15	8	I
D	3	20	T
N	13	1	B
I	8	24	X

Y utilizando la tabla anterior, solos nos queda descifrar el texto, obteniendo

"MÁS VALE ENCENDER UNA VELA QUE MALDECIR LAS TINIEBLAS XXX"

3. Ejercicio 3

¿Qué transformación de cifrado se obtiene si se aplica la transformación $C \equiv 4P + 11$ mód 27 seguida de la transformación $C \equiv 10P + 20$ mód 27?

Solución:

Para resolver este caso iremos paso por paso, primero aplicaremos la transformación $C \equiv 4P+11$ mód 27 a A $= 0$ obteniendo

$$C \equiv 4P + 11 \text{ mód } 27$$

$$C \equiv 4 * 0 + 11 \text{ mód } 27$$

$$C \equiv 11 \text{ mód } 27$$

Una vez obeteniendo este valor, asignamos P = 11 y aplicamos la segunda tranformación $C \equiv 10P + 20$ mód 27, así

$$C \equiv 10P + 20 \text{ mód } 27$$
$$C \equiv 10 * 11 + 20 \text{ mód } 27$$
$$C \equiv 130 \text{ mód } 27$$
$$C \equiv 22 \text{ mód } 27$$

De esta forma, una vez aplicadas las dos transformaciones a la letra $A = 0$ obenemos que su valor cifrado será de 22. Si definimos nuestra transformación definitiva como

$$C_3 \equiv a * P + b \text{ mód } 27$$

Obtenemos en el caso de A que, $22 \equiv a * 0 + b$ mód $27 \rightarrow 22 \equiv b$ mód 27, obteniendo uno de los valores de la transformación final.

Ahora, aplicando ambas transformaciones iniciales a $B = 1$ obtenemos que

$$C \equiv 4P + 11 \text{ mód } 27$$
$$C \equiv 4 * 1 + 11 \text{ mód } 27$$
$$C \equiv 15 \text{ mód } 27$$

y

$$C \equiv 10P + 20 \text{ mód } 27$$
$$C \equiv 10 * 15 + 20 \text{ mód } 27$$
$$C \equiv 170 \text{ mód } 27$$
$$C \equiv 8 \text{ mód } 27$$

Y con estos valores, podemos concluir que al aplicar la tranformación definitiva a $B = 1$, obtendríamos que

$$C_3 \equiv a * P + b \text{ mód } 27$$
$$8 \equiv a * 1 + b \text{ mód } 27$$

Pero nosotros ya conocemos el valor de $b = 22$ así tenemos que:

$$8 \equiv a * 1 + b \text{ mód } 27$$

$$8 \equiv a + 22 \text{ mód } 27$$

$$-14 \equiv a \text{ mód } 27$$

$$13 \equiv a \text{ mód } 27$$

Y así, podemos concluir que la transformación final, luego de aplicar las dos proporcionadas en el problema es la de:

$$C_3 \equiv 13P + 22 \text{ mód } 27$$