08/02/2020

Tarea #1

Integrantes:

- Luna Vázquez Felipe Alberto
- Mario Antonio Hurtado Gutiérrez

Ejercicios:

2. Descifra los siguientes mensajes que fueron cifrados con el método de César, probando diferentes desplazamientos hasta que el mensaje tenga sentido. Escribe el mensaje claro y la llave (desplazamiento) que se usó para cifrar.

Para hacer más efectivo y rápido el descifrado se usó un programa en Python 3 que prueba con todos los posibles desplazamientos, $K \in \{0, \ldots, 26\}$, de igual manera prueba con los desplazamientos hacia "la izquierda", esto es $K \in \{0, \ldots, -26\}$. El programa imprime en pantalla todas las sustituciones.

El programa usado se encuentra en la carpeta "src". Se llegan a los siguientes resultados:

a) S L Y D P Y Q C G L Q N G P Y B M P Y

Con llave $K = 24$ se llega al mensaje "Una base inspiradora"

b) C V V C E M V J G K O R N G O G P V C V Q P

Con llave $K = 2$ se llega al mensaje "Attack the imple mente tien"

c) El archivo imagen.enc que originalmente era una imagen

Se obtuvo una imagen en clave de la serie de Dark, con Jonas afuera del portal. La $K = 77$ y la imagen se escribe en "src/resultados"

2. Considera la siguiente tabla de cifrado de sustitución simple

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
W	P	V	B	A	Q	O	Y	G	C	Z	E	F	H	J	V	D	K	I	R	H	L	T	S	M	X

08/02/2020

a) Encripta el mensaje "criptografia y seguridad"

Usando el programa "ejercicio-2.py" se llega al siguiente resultado:
"V K G V K J O K W Q G W N I A O H K G B W B"

b) Escribe la tabla correspondiente que se usa para descifrar y la primera fila debe ser el alfabeto en orden

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
E	D	J	Q	L	M	I	V	S	O	R	V	N	Y	G	B	F	T	X	W	C	P	A	Z	H	K

c) Usando la tabla del inciso anterior descifra el mensaje

R G F G M O W R R W U E I W K A W I G O A G Q G U W M
R R Y K A W R K J U K N V K J G F V E A F A M R G R G
J M I

Usando el programa "ejercicio-2.py" se llega al siguiente resultado:
"Timing attacks are a significant threat to crypto implementations"

d)

3. El texto del archivo texto.enc fue cifrado con el método de sustitución simple. El original es un texto en español, descíbrelo.

Se hizo un análisis usando la técnica de frecuencias, después se programó el archivo "ejercicio-3.py" con las aproximaciones. Y al final se buscó el texto completo en Internet.

Resultó ser el siguiente texto de "Los hermanos Marx":

"Era muy difícil. Marx y Stanos agitaron y golpearon, pero la pluma que debía volar hasta el techo no se movió del pupitre. Stanos se puso"...

El texto completo se encuentra en la carpeta "resultados / harry.txt"

08/02/2020

5. Sea $m \in \mathbb{Z}$.

a) Supón que m es impar. Encuentra el entero entre 1 y $m-1$ que es igual a $2^{-1} \pmod m$.

Tenemos entonces que por definición pasa lo siguiente

$m = 2k+1$
$\Rightarrow 2^{-1} \pmod m$
$\Rightarrow 2^{-1} \equiv 1 \pmod m$

Como m es impar entonces sabemos que pasa lo siguiente

$2 \nmid m$ entonces $(2, m) = 1$

Por el algoritmo extendido de euclides

$1 = 2x + my$

$1 \equiv 2x + \cancel{my}^{0} \pmod m$

$1 \equiv 2x$

$x = 2^{-1} \pmod m$

b) De forma más general, supón que $m \equiv 1 \pmod b$. Encuentra el entero entre 1 y $m-1$ que es igual a $b^{-1} \pmod m$.

Tenemos lo siguiente

$m \equiv 1 \pmod b$
$\Rightarrow b \mid m-1$
$\Rightarrow bx = m-1$ con $m > mb - x > 0$ y $x \in \mathbb{Z}^+$
$\Rightarrow 1 = m - bx$
$\Rightarrow 1 \equiv m - bx \pmod m$
$\Rightarrow 1 \equiv -bx \pmod m$
$\Rightarrow -x = b^{-1} \pmod m$

6. Explica por qué las siguientes funciones no sirven para encriptar mensajes considerando que los espacios de mensajes y llaves son iguales a $\mathbb{Z}/N = \{0, 1, \ldots, N-1\}$.

08/02/2020

a) $E(k, m) = km \pmod{n}$

b) $E(k, m) = (k+m)^2 \pmod{n}$

4. En cada inciso encuentra el valor de x entre 0 y m-1 que resuelve la congruencia, donde m es el módulo

b) $221^3 \equiv x \pmod{581}$

$\Rightarrow 10895567 \equiv x \pmod{581}$
$\Rightarrow 581n + 20$ donde $n \in \mathbb{Z}$ → Solución general
$\Rightarrow x \equiv 20 \pmod{581}$ → Solución particular

c) $x - 21 \equiv 23 \pmod{37}$

$\Rightarrow x \equiv 23 + 21 \pmod{47}$
$\Rightarrow x \equiv 37n + 7$ donde $n \in \mathbb{Z}$ → Solución general
$\Rightarrow x \equiv 7 \pmod{37}$ → Solución particular

a) $123 + 513 \equiv x \pmod{763}$

$\Rightarrow 636 \equiv x \pmod{763}$
$\Rightarrow x = 763n + 636$ donde $n \in \mathbb{Z}$ → Solución general
$\Rightarrow x \equiv 636 \pmod{763}$ → Solución particular.