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 desarrollo 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 impenetrable"

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

Se obtuvo una imagen en clase de la serie de Dark, con Jonas afuera del portal. La $k = 114$ la imagen se escribe en "src/resultados"

3. 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	X	H	L	T	S	N	X

08/06/2020

a) Encripta el mensaje "Criptografia y seguridad"

Usando el programa "ejercicio-2.py" se llega al siguiente resultado:
"U 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, 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	U	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 M G Q G U W M
R R Y K A W R K J U K N V R J G F V E A F A M R G R G
J M !

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

d) Con un código de caracteres de 8 bits (1 byte) se pueden representar hasta $2^8 = 256$ caracteres (código Ascii extendido). Esto sería el tamaño de la tabla.

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

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

Resultó ser el siguiente texto de "Las hermanas Mercy":

Era muy difícil. Harry y Seamus agitaron y golpearon, pero la pluma que debía volar hasta el techo no se movió del pupitre. Seamus 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 $m \equiv 7 \pmod 6$. Encuentra el entero entre 1 y $m-1$ que es igual a $6^{-1} \pmod m$.

Tenemos lo siguiente

$$m \equiv 7 \pmod 6$$
$$\Rightarrow 6 \mid m-7$$
$$\Rightarrow 6x = m-7 \text{ con } m > mb - x > 0 \text{ y } x \in \mathbb{Z}^+$$
$$\Rightarrow 7 = m - 6x$$
$$\Rightarrow 7 \equiv m - 6x \pmod m$$
$$\Rightarrow 7 \equiv -6x \pmod m$$
$$\Rightarrow -x = 6^{-1} \pmod m$$

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) $E(k, m) = km \pmod N$

Tenemos que si N resulta no ser primo no sería un cifrado correcto ya que este puede tener varias congruencias válidas, por lo que la función no sería biyectiva. En caso de que N sea primo todo marcharía correctamente.

b) $E(k, m) = (k+m)^2 \pmod N$

Tenemos que la raíz de $(k+m)^2$ produce dos posibles valores, positivo y negativo, por lo que si usamos esta función para cifrar la correspondencia no sería biyectiva. En particular con 0 y 1.

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

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

$\Rightarrow 109\,41048 \equiv x \pmod{581}$

$\Rightarrow 273 \equiv x \pmod{581}$

$\Rightarrow 237 \equiv x \pmod{581}$

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

d) $x^2 \equiv 5 \pmod{11}$

$\Rightarrow x = 11n + 4$ con $n \in \mathbb{Z}$ → Solución general

$\Rightarrow x \equiv 4 \pmod{11}$ → Solución particular

e) $\Rightarrow x = 11n + 2$ con $n \in \mathbb{Z}$ → Solución general

$\Rightarrow x \equiv 2 \pmod{11}$ → Solución particular

08/02/2020

8. Muestra que los esquemas de César, sustitución simple y Vigenère pueden romperse fácilmente en un ataque de texto claro elegido. ¿cuántos mensajes claro se necesitan para romper la llave en cada caso?

→ Sustitución simple y César: Al usar uno o más textos citados y encontrando solo una letra en claro a partir de esto podríamos descifrar todos los textos (si no cambian de llave).

→ Esquema de Vigenère: Al dividir el criptograma en bloques de tamaño n, cada columna es un cifrado de César, por lo que por lo anterior es fácil deducir que necesitamos al menos un mensaje en claro que contenga todas las letras del alfabeto.

7. Considera el cifrado afín con una llave $K = (K_1, K_2)$

a) Usando $N = 101$ y $K = (99, 20)$, cifra el mensaje $m = 100$ y descifra el cripto texto $c = 23$

Tenemos entonces que el cifrado afín se basa en la siguiente fórmula

$$C_i = K_1 * M_i + K_2 \pmod N$$

donde ahora sabemos que $K_1 = 99$, $K_2 = 20$ y $N = 101$

$C_1 = (99 * M_1 + 20) \bmod 101$
$C_1 = (99 * 1 + 20) \bmod 101$
$C_1 = (99 + 20) \bmod 101$
$C_1 = (119) \bmod 101$
$C_1 = 18 = C_3$

$C_0 = (99 * M_0 + 20) \bmod 101$
$C_0 = (99 * 0 + 20) \bmod 101$
$C_0 = (0 + 20) \bmod 101$
$C_0 = 20 \bmod 101$
$C_0 = 20$

En tonces el mensaje cifrado $M_c = 18\ 20\ 20$"

Ahora, usando el script "ejercicio-7.py" se obtuvo que el inverso de $K_1 = 99$ es 50

$M_c = (50 * 2 + 20) \bmod 101$

$M_c = (120) \bmod 101$

$M_c = (19)$

$M_c = (50 * 3 + 20) \bmod 101$

$M_c = (69)$

El mensaje descifrado es "19 69"

22/02/2020

b) Describe un ataque de texto claro conocido para recuperar la llave (k_1, k_2). Observa que la función de cifrado es la ecuación de una recta en el plano, donde las coordenadas corresponden a una letra en claro y una letra cifrada, ¿cuántos puntos se necesitan?

Supongamos que ya tenemos nuestro cifrado texto y nuestro texto cifrado. A continuación podemos tomar dos letras que sean los puntos (x_1, y_1), (x_2, y_2) de la ecuación:

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

Para lo que para encontrar la recta sólo necesitamos esos dos puntos

c) Aplica tu ataque al archivo cifrado audio.enc que originalmente es un texto en formato .mp3.

Investigando en la Wikipedia se encuentra que los cabeceros de un archivo .mp3 son 255 y 251 y en el audio cifrado se tiene 242 y 190. Entonces ya tenemos nuestros "dos puntos" por lo que procedemos con nuestro ataque.

$242 = 255k + B \bmod 256$
$190 = 251k + B \bmod 256$ Restando ambas ecuaciones

$52 = 4k \bmod 256$ Despejando k

$52 \bmod 256 = 4k$
$13 * 4 \bmod 256 = 4k$ Sustituyendo k
$13 \bmod 256 = k$
$13 = k$

$\therefore K = (13, 255)$

$242 = 255 * 13 + B \bmod 256$
$242 - 255 * 13 \bmod 256 = B$
$242 - 3315 \bmod 256 = B$
$-3073 \bmod 256 = B$
$255 = B$

El script "genricio-7.py" descifra el audio y lo exporta a la carpeta "resultados".

La canción resultante es "Such Great Heights de The Postal Service"