Criptografia y seguridad

Miranda Sánchez Kevin Ricardo (No. de Cuenta: 314011163) and
Rivas Leòn Alexis (No. de Cuenta: 314340520)

Facultad de Ciencias, UNAM

Fecha de entrega: 10-Febrero-2020

1. **Descifra los siguientes mensajes que fueron cifrado 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.**

   a) El problema se soluciono con un programa, el cual se anexa llamado cesar.py. La llave de este problema es 19, y el mensaje es:
   "*unafraseinspiradora*"

   b) El problema se soluciono con un programa, el cual se anexa llamado cesar.py. La llave de este problema es 15, y el mensaje es:
   "*attacktheimplementation*"

   c) La imagen descifrada es la siguiente:

   Se realizó un programa en Python3 llamada imageDecipher.py que se anexa, por medio de las imagenes creadas nos percatamos que la llave era 217

2. **Considera la siguiente tabla de cifrado de sustitución simple**

   a) Encripta el mensaje
   Criptografia y seguridad.
   UKGVRJOKWQGW N IAOHKGBWB

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

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

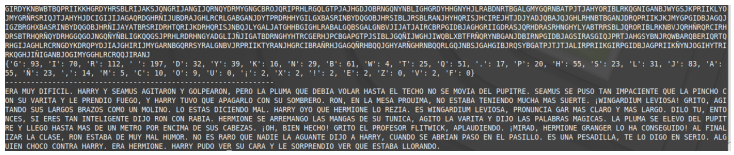
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	D	J	Q	L	M	I	U	S	O	R	V	N	Y	G	V	F	T	X	W	C	P	A	Z	H	K

c) Usando tu tabla del inciso anterior, descifra el mensaje:
RGFGMOWRRWUZIWKAWIGOMGQGUWMRRYKAWRRJUKNVRJGFVEAFAMRWRGJMI
TIMINGATTACKSAREASIGNIFICANTTHREATTOCRYPTOIMPLEMENTATIONS

TIMING ATTACKS AREA SIGNIFICANT THREAT TO CRYPTO IMPLEMENTATIONS

d) ¿Cómo sería una tabla de cifrado si los mensajes fueran cadenas de bytes (archivos) en vez de las 26 letras del alfabeto? ¿De qué tamaño sería la tabla? Dado que las cadenas de bytes son de 0 a 255 basta con cambiar los letras por los números y el tamaño de la tabla sería de 256.

3. **El texto del archivo texto.enc fue cifrado con el método de sustitución simple. El original es un texto en español, encuéntralo.** El problema fue resuelto mediante un análisis de frecuencia con el apoyo de un programa que ha sido anexado, llamado texto.py. El programa consiste en recorrer todo el texto y contar el numero de ocurrencias de cada caracter. Una vez contado, se hicieron experimentos que consistían en reemplazar la letra de más ocurrencia con la que en español lo era. Conforme se iba ocurriendo posibles sustituciones, se dejaban en el código como posible respuesta.



ERA MUY DIFICIL. HARRY Y SEAMUS AGITARON Y GOLPEARON, PERO LA PLUMA QUE DEBIA VOLAR HASTA EL TECHO NO SE MOVIA DEL PUPITRE. SEAMUS SE PUSO TAN IMPACIENTE QUE LA PINCHO CON SU VARITA Y LE PRENDIO FUEGO, Y HARRY TUVO QUE APAGARLO CON SU SOMBRERO. RON, EN LA MESA PROUIMA, NO ESTABA TENIENDO MUCHA MAS SUERTE. ¡WINGARDIUM LEVIOSA! GRITO, AGITANDO SUS LARGOS BRAZOS COMO UN MOLINO. LO ESTAS DICIENDO MAL. HARRY OYO

QUE HERMIONE LO REZIA. ES WINGARDIUM LEVIOSA, PRONUNCIA GAR MAS CLARO Y MAS LARGO. DILO TU, ENTONCES, SI ERES TAN INTELIGENTE DIJO RON CON RABIA. HERMIONE SE ARREMANGO LAS MANGAS DE SU TUNICA, AGITO LA VARITA Y DIJO LAS PALABRAS MAGICAS. LA PLUMA SE ELEVO DEL PUPITRE Y LLEGO HASTA MAS DE UN METRO POR ENCIMA DE SUS CABEZAS. ¡OH, BIEN HECHO! GRITO EL PROFESOR FLITWICK, APLAUDIENDO. ¡MIRAD, HERMIONE GRANGER LO HA CONSEGUIDO! AL FINALIZAR LA CLASE, RON ESTABA DE MUY MAL HUMOR. NO ES RARO QUE NADIE LA AGUANTE DIJO A HARRY, CUANDO SE ABRIAN PASO EN EL PASILLO. ES UNA PESADILLA, TE LO DIGO EN SERIO. ALGUIEN CHOCO CONTRA HARRY. ERA HERMIONE. HARRY PUDO VER SU CARA Y LE SORPRENDIO VER QUE ESTABA LLORANDO.

4. **En cada inciso encuentra el valor de x entre 0 y $m1$ que resuelve la congruencia, donde m es el módulo**

   a) $123 + 513 \equiv x(mód763)$
   $123 + 513 = 636$ entonces $636 \equiv x(mód763)$ por la propiedad de reflexividad nos da $x \equiv 636(mód763)$ entonces $636(mód763)$ es 636 entonces $x \equiv 363$

   b) $222^3 \equiv x(mód581)$
   $222^3 = 10941048$ entonces $10941048 \equiv x(mód581)$ por la propiedad de reflexividad $x \equiv 10941048(mód581)$ y $10941048(mód581) = 237$ por lo que $x \equiv 237$

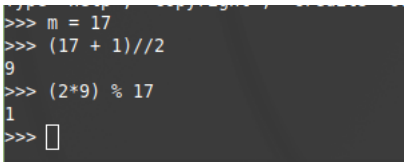
   c) $x - 21 \equiv 23(mód37)$
   $23(mód37) = 23$ entonces $x - 21 = 23$ por lo que $x = 21 + 23$ por lo tanto $x = 44$

   d) $x^2 \equiv 5(mód11)$
   $5(mód11) = 5$ entonces $x^2 \equiv 5$ que es lo mismo que $x^2 = 5$ por lo tanto $x = \sqrt{5}$

   e) $x^3 - 2x^2 + x - 2 \equiv 0(mód11)$.
   Primero factorizamos $(x-2)(x^2+1) \equiv 0(mód11)$ luego tenemos que $(x-2) = 0$ por la tanto $x \equiv 2(mod11)$

5. **Sea m $\in$ Z.**

   a) **Supón que m es impar. Encuentre el entero entre 1 y m-1 que es igual a 2-1(mod m).**
   El entero sería (m+1)/2
   Ejemplo:



   El inverso multiplicativo modular de un número entero a módulo m es un número entero b tal que ab $\equiv$ 1 (mód) m
   Entonces bastaba con encontrar un numero, que le ganara por 1 al modulo. Este número sería un numero divisible por 2.

   b) **De forma más general, supón que m $\equiv$ 1 (mod b). Encuentra el entero entre 1 y $m-1$ que es igual a** $b-1$ $(modm)$ Sabemos que para algún entero k=$\frac{m-1}{b}$, tenemos que $m = k*b+1$, o en otras palabras $1-m-k*b$
   $(-k)*b-1=(-1)*m$

   Es decir, hemos encontrado que $(-k)*b$ es igual a 1 $(modm)$. Es decir, $[-(m-1)/b]*b=1(modm)$ Sin embargo, necesitamos el residuo equivalente a $[-(m-1)/b]$ que está entre 1 y m-1.
   Entonces, $m+[-(m-1)/b]=[m*b-m+1]/b=[m*(b-1)+1]/b$
   Esto, en general, estará entre 1 y m-1.

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

   - $E(k,m) \equiv km$ (mód N) NO se puede porque se puede agarrar cualquier número arbitrario entre el conjunto de $1...N-1$ pero solo funciona si k y m son primos relativos
   - $E(k,m) \equiv (k+m)^2$ (mód N) esta no se puede usar para cifrar ya que se puede devolver el mismo elemento para cifrar, por ejemplo sea $N=5$ entonces $\{0,...,4\}$ la llave 0 entonces:
     $(0+4)^2=16 \longrightarrow 16$(mód 5) = 1
     $(0+1)^2 \longrightarrow 1$ (mód 5) = 1

7. **Considera el cifrado afín con una llave k = (k1,k2)**

   a) **Usando N = 101 y k = (99, 20), cifra el mensaje m = 100 y descifra el criptotexto c = 23.**
   El cifrado de m = 100 es $c \equiv 99*100+20 \equiv 9920 \equiv 22$ $(mód$ 101)

El inverso de k_1 es $99^{-1} \equiv 50 \pmod{101}$, el decifrado de c=23 es m $\equiv$ 50*(23-20) $\equiv$ 49

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 de una recta se necesitan para determinar su ecuación?** Supongamos que tenemos 3 coordenadas:
(m_1, c_1),(m_2, c_2),(m_3, c_3)
Lo que nos da un sistema de congruencias.

$$\begin{bmatrix} c_1 & m_1 & 1 \\ c_2 & m_2 & 1 \\ c_3 & m_3 & 1 \end{bmatrix} \begin{bmatrix} 1 - k_1 - k_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} (modn)$$

Al usar el módulo de álgebra lineal, esto implica que el determinante de la matriz satisface

$$det \begin{bmatrix} c_1 & m_1 & 1 \\ c_2 & m_2 & 1 \\ c_3 & m_3 & 1 \end{bmatrix} \equiv 0(modm)$$

$$D = det \begin{bmatrix} c_1 & m_1 & 1 \\ c_2 & m_2 & 1 \\ c_3 & m_3 & 1 \end{bmatrix}$$

Esto es divisible por el numero primo p. Si se puede factorizar D, entonces, en el peor de los casos, tiene algunos valores posibles de comprobación de datos. Entonces, tres pares pueden ser suficientes para romper el cifrado.

De manera más general, si se tiene diferentes pares, puede calcular valores determinantes D1,. . . , Dn 2 mediante el uso de diferentes pares en la última fila de la matriz. Esto le da un montón de números que son divisibles por p, y dentro de poco tiempo casi seguro encontrará que máximo común divisor (D1,..., Dn 2) es igual a p

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

   - Para el de Cesar y el de sutitución simple, solo es uno ya que en este tipo de ataque teniendo el texto cifrado y el texto original basta con ver los dos textos y ver la letra y lo que regresa y así poder ver el desplazamiento.
   - Mientras que para Vigenere para conocer la clave se necesitaría saber la logitud l de la clave para esto necesitariamos al menos l textos

cifrados para saber esto y estimar la perioricidad de los patrones en el texto cifrado