Criptografía y Seguridad
Tarea 01

Luis Fernando González Montiel
Ezequiel Martinez Vite

25 de febrero de 2020

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

   a) SLYDPYQCGLQNGPYBMPY
   Solución:
   Haciendo el análisis de frecuencia...
   Y=4
   P=3
   Q=2
   L=2
   G=2
   Esto quiere decir que muy probablemente Y es una vocal, ya sea la 'e' o la 'a', probando con cada una, es decir, con dezplazamiento k=20 para la e en Y, no resulto algo decifrado con sentido, asi que probe el desplazamiento k=24 para a en Y, dando de resultado.
   SLYDP YQCGL QNGPY BMPY
   unafr asein spira dora
   Es decir: Una Frase Inspiradora, con K=24.

   b) CVVCEMVJGKORNGOGPVCVKQP
   Solución:
   Haciendo el análisis de frecuencia...
   V=5
   G=3
   C=3
   O=2
   K=2
   Costó demasiado trabajo ya que no es ninguna de las letras más usadas en el español hasta que lo realice por fuerza bruta y tomó sentido en inglés.
   CVVCE MVJGK ORNGO GPVCV KQP
   attac kthei mplem entat ion
   Es decir: Attack The Implementation, con K=2.

   c) El archivo imagen.enc que originalmente era una imagen.
   Solución:
   En el directorio se encuentra el programa que se uso para decifrar la imagen.enc llamado cesarImag.py

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

   a) Encripta el mensaje

Criptografia y seguridad.

Solución:
cript ograf iayse gurid ad
UKGVR JOKWQ GWNIA OHKGB WB

b) Escribe la tabla correspondiente que se usa para descifrar, la primera fila debe ser el alfabeto en orden.
Solución:
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 tu tabla del inciso anterior, descifra el mensaje
RGFGMOWRRWUZIWKAWIGOMGQGUWMRRYKAWRRJUKNVRJGFVEAFAMRWRGJMI
Solución:
RGFGM OWRRW UZIWK AWIGO MGQGU WMRRY KAWRR JUKNV RJGFV EAFAM RWRGJ MI
TIMING ATTACKS AREA SIGNIFICANT THREAT TO CRYP TO 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?
Solución:
Sería en hexadecimal y sería una tabla de tamaño de 256.

3. El texto del archivo texto.enc fue cifrado con el método de sustitu- ción simple. El original es un texto en español, encuéntralo.

Solución:

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

a) 123 + 513 ≡ x (mód 763).
Solución:
636=x(mód 763)
b) $222^3 \equiv$ x (mód 581).
Solución:
10,941,048 = x (mód 581)
237 = x (mód 581)

c) x - 21 ≡ 23 (mód 37).
Solución:
x = 23+21 (mód 37)
x = 44 (mód 37)
x= 7 (mód 37)

d) $x^2 \equiv 5$ (mód 11).
Solución:
x= +-4 (mód 11)
x= -4 (mód 11) → x= 7 (mód 11)
x= 4 (mód 11) ó x= 7 (mód 11)

e) x^3 - $2x^2$ + x - 2 ≡ 0 (mód 11).
Solución:

x^2(x-2)+1(x-2) = 0(mód 11)
(x^2+1) = 0 ó x-2 = 0
x^2 = 10 No hay solución x = 2
x = 2

5. Sea m ∈ Z.

   a) Supón que m es impar. Encuentra el entero entre 1 y m - 1 que es igual a 2^{-1}(mód m).
   SOLUCIÓN:
   Como suponemos que m es impar (2k+1) y estamos buscando su inverso de 2 con el (mód m) entonces podemos verlo como (2,m)=1
   Aqui nos servirá mucho ver el problema como el algoritmo extendido de euclides como
   1 = 2x+ my, si hacemos 0 = my mañosamente nos va a quedar que 1 ≡ 2x (mód m) y despejando quedaría
   1/2 = x (mód m)

   b) De forma más general, supón que m ≡ 1 (mód b). Encuentra el entero entre 1 y m - 1 que es igual a b -1 (mód m).
   •textscSolución:
   Tomando a m ≡ 1 (mód b), también podemos ver a bx = 1-m es decir,
   m = 1-bx
   1-bx ≡ m(0) (mód b)
   1-bx ≡ (0) (mód b)
   -bx ≡ -1 (mód m)
   bx ≡ 1 (mód m)
   entonces X = b^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}.

   a) E(k, m) = km (mód N).
   SOLUCIÓN:
   En este caso no porque no se pueden ocupar fracciones en modulo.

   b) E(k, m) = $(k + m)^2$ (mód N).
   SOLUCIÓN:
   Para este caso es similar al anterior ya que la sumatoria de la llave puede ser una fracción y elevado al cuadrado seguiría siendo fracción, hay algunos casos en los que el resultado no sería fracción, pero en otros si, entonces por esto no es posible.

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 criptotexto c = 23
   SOLUCIÓN:
   c1 = (99*mi + 20) (mód 101)
   = (99*1 + 20) (mód 101)
   = 119 (mód 101)
   c1 = 18

   c2,3 = (99*0 +20) (mód 101)
   = 20 (mód 101)
   c2,3 = 20
   Entonces el mensaje m=100 cifrado se veria como c=182020

   Y para decifrar el c= 23 use un for

```
for m in range(1,101):
```

```
if (99*m+20) % 101 == 23:
    print (m)
```

Dando el mensaje m=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?
Solución:
Solo se requieren 2 puntos porque es lo que hace falta para descubrir una recta con la fórmula de la recta.

c) Aplica tu ataque al archivo cifrado audio.enc, que originalmente es un audio en formato MP3. Es posible que tengas que modificar un poco el ataque.
Solución:
En el directorio se encuentra el programa que se uso para decifrar el audio.enc llamado afinCancion.py

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

   Solución:
   César: Se necesita un mensaje claro.
   Sustitución: Se necesita un mensaje claro.
   Vigenére: Se necesita parejas (Mr,Cr) Ci=Ek(mi) de mensajes claros.