INTEGRANTES DEL EQUIPO:
EMMANUEL CRUZ HERNANDEZ
LUIS EDUARDO MARTINEZ HERNANDEZ

1.-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.
a)SLYDPYQCGLQNGPYBMPY
La frase es UNAFRASEINSPIRADORA con llave k = 24

b)CVVCEMVJGKORNGOGPVCVKQP
La frase es ATTACKTHEIMPLEMENTATION con llave k = 2

c)El archivo imagen.enc que originalmente era una imagen.
El código está dentro del archivo Descifrador.py
La imagen es la siguiente:

2.Considera la siguiente tabla de cifrado de sustitución simple
a)Encripta el mensaje

Criptografía y seguridad.

Mensaje Cifrado = UKGVRJOKWQGW N IAOHKGBWB

b)Escribe la tabla correspondiente que se usa para descifrar, la primera fila debe de 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 tu tabla del inciso anterior,descifra el mensaje

RGFGMOWRRWUZIWKAWIGOMGQGUWMRRYKAWRRJUKNVRJGFVEAFAMRWRGJMI

Mensaje Descifrado = TIMING ATTACKS ARE A 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?
Como los archivos están codificados por bytes,entonces nuestro alfabeto serían todas las combinaciones de bits hasta formar 1 byte.Es decir, la tabla tendría 2^8 entradas.

3.-El texto del archivo texto.enc fue cifrado con el método de sustitu-cion simple. El original es un texto en español, encúentralo.
Usando análisis de frecuencias pudimos crear hipótesis como las siguientes:

1. La letra l es una consonante que se repite dos veces, por lo que debe ser la letra l, r o c. Sin embargo, la c queda descartada porque todas las palabras con c repetida tienen de continuación al menos 3 letras más, en este caso, sólo tiene una letra más.
2. La K es vocal, ya que está junto a una consonante en la palabra PRIIK.
3. La palabra MYG sólo aparece en esa secuencia, es decir, siempre que aparece una M va seguido de una Y. Por lo que inferimos que MYG es la palabra QUE.
4. De la razón anterior, la G es una vocal, específicamente la E.
5. Como la G es la letra E, entonces inferimos de la palabra GA que la A es una consonante, que puede ser la l, n, s.
6. Como la A debe ser una consonante, de la palabra AJ inferimos que la J es una vocal.
7. De la palabra GQ, inferimos que la letra Q es una consonante, ya que la G es la letra E. Entonces Q puede ser l, s, n.
8. De la palabra QQJIRANJ inferimos que la letra Q es la l o la r. Sin embargo, por el punto 7, descartamos las letras s y n. Esto implica que la Q es la l.
9. A partir de este momento comenzamos a ver palabras claras. Por lo que el resto consistió en ir completando palabras.

para finalmente encontrar el alfabeto siguiente:

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

El texto es:
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 proxima, 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 reñia. 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 m-1 que resuelve la congruencia, donde m es el módulo.

a)123 + 513 ≡ x (mod 763)
→ 635 ≡ x (mod 763)
si restamos 635 - 763 → 635 ≡ - 128 (mod 763)

b)(222)^3 ≡ x (mod 581)
→10941048 ≡ x (mod 581)
Si dividimos 10941048 entre 581 y tomamos el residuo que es 237→ x = 237 (mod 581)

c)x-21 ≡ 23 (mod 37)
→ x ≡ 23 + 21 (mod 37)
→ x ≡ 44 (mod 37)
Si dividimos 44 entre 37 y tomamos el residuo que es 7→ x = 7

d)x^2 ≡ 5 (mod 11)
Sumamos 11 del lado derecho hasta encontrar un cuadrado→ x^2 ≡ 5 + 11 (mod 11)
→ x^2 ≡ 5 + 11 + 11 +11 + 11 (mod 11)
→ x^2 ≡ 7^2 (mod 11)
Por propiedades tenemos → x ≡ 7 (mod 11)
si restamos 11 - 7 tenemos 4 ≡ 7 (mod 11)
Por lo tanto x = 4

e)x^3 - $2x^2$ + x -2 ≡ 0 (mod 11)
Probando por fuerza bruta tenemos:
→ 1 - 2 + 1 -2 ≡ 0 → -2 ≡ 0 → No se cumple
→ 8 - 8 + 2 -2 ≡ 0 → 0 ≡ 0 → Si se cumple
Por lo tanto x = 2

5.-Sea m que pertenece a Z

a)Supón que m es impar. Encuentra el entero entre 1 y m – 1 que es igual a 2^{-1}≡ (mod m).
Como m es un número impar tenemos que m = 2k + 1 para alguna k en los enteros, luego

por definición de congruencia y como m divide a 2k+1 tenemos $2k + 1 \equiv 0 \pmod{m}$,si sumamos un uno a ambos lados tenemos $2k + 2 \equiv 1 \pmod{m}$, entonces si factorizamos tenemos $2(k + 1) \equiv 1 \pmod{m}$,luego como k+1 es menor a m y como se cumple $2(k + 1) \equiv 1 \pmod{m}$ entonces 2^{-1} es igual a k+1.

b)De forma más general, supón que $m \equiv 1 \pmod{b}$.Encuentra el entero entre 1 y m – 1 que es igual a $b^{-1} \pmod{m}$.
Como se cumple por hipótesis que $m \equiv 1 \pmod{b}$,entonces por definición podemos expresarlo como bk = m-1 para alguna k en los naturales,luego si despejamos tenemos bk + 1 = m,entonces por definición de divisibilidad y de congruencia tenemos $bk+1 \equiv 0 \pmod{m}$,luego si despejamos y multiplicamos por un menos 1 tenemos $b(-k) \equiv 1 \pmod{m}$,por lo tanto el inverso multiplicativo de b es -k.

6.-Explica porqué las siguientes funciones no sirven para encriptar mensajes considerando que los espacios de mensajes y llaves son iguales

a) $E(k,m) = km \pmod{N} = c$
Esta forma para encriptar no sirve, porque sin la restricción de que mcd(k, N) = 1 entonces al desencriptar el mensaje existirían demasiadas formas de desencriptar el mensaje o ninguna. Debido a que no se está pidiendo la restricción de que mcd(k, N) = 1, entonces puede ocurrir que se encripte con una k cuyo mcd(k,N) > 1 y esto provocaría que existieran exactamente 0 o N formas de desencriptar el mensaje. Esto sucede así por lo siguiente:
Para desencriptar el mensaje m se tiene que calcular el inverso de k, es decir queremos quitar a m del lado de k, visto con ecuaciones tenemos:
$mk \cong c \pmod{N}$
donde m es la incógnita de la ecuación. Por el teorema de [1] tenemos que existen exactamente 0 o N soluciones para m.Por lo tanto, existen exactamente 0 o N formas de desencriptar el mensaje.

b)$E(k, m) = (k + m)^2 \pmod{N} = c$
Esta forma para encriptar no sirve, porque se tienen dos formas de desencriptar el mensaje.Se tienen dos formas de desencriptar el mensaje por lo siguiente:
Para desencriptar el mensaje se debe despejar a m de la ecuación,entonces al despejar tenemos
$(c – k^2) = m(2k + m)$
Pero como se puede apreciar de la ecuación anterior, existen dos soluciones para m. Esto nos llevaría a que existen dos formas de desencriptar el mensaje.Por lo tanto esta forma para encriptar no sirve.

7.-**Considera el cifrado afın 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.
Para encriptar el mensaje m=100, usamos la fórmula de encriptado afín, definida como $c=(mk_1+k_2) \bmod N$.

Tenemos así lo siguiente: c=(100*99 + 20) mod 101 = (9900 + 20) mod 101 = 9920 mod 101 = 22. Por lo que el mensaje m=100, al cifrar se ve como c=22.
Para desencriptar el mensaje c=23 usamos la función inversa del cifrado afín, dada por $m=(c-b)a^{-1}$ mod N.
Tenemos así lo siguiente: $m=(23-20)*(99)^{-1}$ mod 101.
El inverso de 99 en álgebra modular lo encontramos con el algoritmo de Euclides extendido.
Usamos la función llamada phi de Euler:
$99x \equiv 1$ mod 101 podemos expresarlo con la función de Euler como
$99^{\phi(101)} \equiv 1$ mod 101 donde $\phi(101)=101-1=100$
$99^{100} \equiv 1$ mod 101
$99*99^{99} \equiv 1$ mod 101
El inverso de 99 es 99^{99} mod 101 =
369729637649726772657187905628805440595668764281741102430259972423552570455277523421410650010128232727940978889548326540119429996769494359451621570193644014418071060667659301384999779999159200499899 mod 101 = 50.
Por lo que el inverso de 99 es 50.
Con esto tenemos m=(23-20)*50 mod 101=3*50 mod 101= 150 mod 101 = 49.
Por lo que el mensaje cifrado c=23 es m=49.

b) Describe un ataque de texto claro conocido para recuperar la llave (k1, k2). 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, ¿cuantos puntos de una recta se necesitan para determinar su ecuación?
Se necesitan solo dos puntos para determinar la ecuación.
El ataque de texto claro conocido consiste en lo siguiente:
Para cada carácter del texto claro, se transforma a su equivalente en decimal,digamos un x.
Para cada caracter del texto cifrado, se transforma a su equivalente en decimal, digamos un y.
Después calculamos la primera llave k1 utilizando la fórmula de la pendiente, k1 = y2-y1/x2-x1.Para esto necesitamos dos puntos x,y de los pasos anteriores.
Después calculamos la segunda llave k2 utilizando la fórmula de la recta, y1 = k1*x1 + k2.Despejando tenemos k2 = y1 - k1*x1.
Finalmente, habremos recuperado la llave (k1,k2).

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.
El codigo está dentro del archivo AudioDes.py la llave es (197,255)
Y el mp3 desencriptado es el archivo audio.mp3

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?

-Cesar:
Solo se necesita un mensaje en claro.

Si se tiene el mensaje en claro y el mensaje cifrado es trivial obtener la llave, este proceso consiste en ver una letra en el mensaje en claro y una en el cifrado y ver cual es la separación que tienen.Una vez encontrada esta separación se habrá encontrado la llave.

-Sustitución simple:
Solo se necesita un mensaje en claro que sea lo suficientemente largo(lo suficiente como para que tenga todas las letras del alfabeto de entrada).
Si se tiene un mensaje en claro que sea lo suficientemente largo, lo único que se debe de hacer para obtener la llave es hacer la correlacion de que letra se sustituye por cual.Al finalizar este proceso se tendrá la llave.

-Vigenére:
Solo se necesita un mensaje en claro que sea lo suficientemente largo(lo suficiente como para que tenga todas las letras del alfabeto de entrada).
Si se tiene un mensaje en claro que sea lo suficientemente largo, lo que se debe de hacer para obtener la llave es obtener la longitud de la llave(esto se hace viendo las coincidencias de las letras), después se ponen las palabras en bloques del tamaño de la llave y finalmente se aplica un análisis de frecuencias a cada columna(porque cada columna es un cifrado césar). Al finalizar esto se tendrá la llave.

Referencias:

[1] Shoup, Victor (2005), A Computational Introduction to Number Theory and Algebra, Cambridge University Press, Theorem 2.4, p. 15, ISBN 9780521851541