GUÍA 1: CRIPTOGRAFÍA CLÁSICA

Ejercicio 1:

Dar una definición formal de los algoritmos `Gen`, `Enc` y `Dec` para los siguientes esquemas:

- **Cifrado de rotación**
- **Cifrado de sustitución monoalfabética**
- **Cifrado de Vigenère**

Ejercicio 2:

¿Por qué la composición de dos sistemas de sustitución simple no provee más seguridad que el uso de uno solo? Ejemplificar.

Ejercicio 3:

Descifrar el siguiente criptograma, sabiendo que fue encriptado usando el cifrado de rotación, que se corresponde a un texto en español (27 letras) y los espacios fueron suprimidos ¿Cuál fue la estrategia que utilizaste?

VKXYKBKXGKSGWAKQQGYIUYGYWAKXKGQRKSZKJKYKKYIUSYKMAÑX

Ejercicio 4:

a) **Cifrar según Vigenère el mensaje M = UN VINO DE MESA con la clave K = BACO sin usar la tabla, sólo con operaciones modulares.**
b) **En un sistema de cifra de Vigenère la clave a usar puede ser CERO o bien COMPADRE, ¿cuál de las dos conviene usar y por qué?**
c) **Mostrar, con un ejemplo, que la composición de dos cifrados Vigenère resulta en otro cifrado Vigenère**

Ejercicio 5:

Teniendo en cuenta que la frecuencia (aproximada) de aparición de letras en castellano es la siguiente:

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
%	13	1	4	5	13	1	1	1	7			5	3	7	0	9	3	1	7	8	4	4	1			1	

Decir, para cada criptograma, si se ha obtenido mediante técnicas de sustitución monoalfabética, sustitución polialfabética o de transposición. (No hay que descifrarlos)

Los criptogramas son:

Criptograma 1

KOZFVPCYVCWVZHMZLCIOHIFIZGJCZTVVXIGJLZHYZLGVMNVLYZ

Criptograma 2

HHMBIWSIPSNNTAWVITQWMEAQVNSPGQJNWELXMJDIBYUGNNRMEUDEM
ZIBTMYMBMWURBTIZXNCWZIUPZUQNRMEGJLWRVROPMREUMXXXAXDIP
UVFEASMBSASCETAEWOYYAKUSWEABSASCRECIOMEWTQOMYALMTXRAG
EWSQQHJDXMVJEAFIRNDUIANW

Criptograma 3

DERTNYLANAOTAABADEAXCEEAIDEJLXHRSUAUJUMXELAATECRTRNAZBI
RESOX

Ejercicio 6:

Se recibe el siguiente criptograma:

JGAZN WINHY LZDYV BBJLC QHTNK UDQXM OXJNO ZMUSP NONYJ MTEJH QHQFO
OPUPB CYAÑJ ONCNN QHNMO NDHKU TJMQC MOPNF AOXNT NLOAZ MJDQY MOZCJ
RNBAO QTUIE NFAIX TLXJG AZMJA XJVAZ MUDNM YLNLJ MUMUY HVUMH TÑIGD
XDQUC LSJPI BCUSF NUGXX GEEXK AEJME SJÑEN ASLHL BAEYJ ROJXA CQTCN
MYPUC UNMJW OYNHZ NKUOG AJDUJ XENRY TENJS CNMON TYJNM JYFXF IGJMI
BUUSN TFAPN FAFKU ROJNY CTUYN BYSGJ VACAU CGQWA ZMJJH JHSNT PAPXM
GNECO GJUTE NCNGJ GEGAJ SPNUL GDMAÑ JDOFD NPUNN PNTGE NMJSN TTOFD

KIOXS SQNNF BATOC XMMNV ÑEZNM EZBOS NTUSQ BUDBT JRBBU YPQZI OQFTB ANIBV MEDDY RUMUP NAULB OMAED HVHNF OCJOS NMJ.

Si se conoce que ha sido cifrado mediante el algoritmo de Vigenère, se pide:

a. **Comprobar la longitud de la clave.**
b. **Encontrar la clave del sistema y desencriptar sólo los diez primeros caracteres.**

Para ello tener en cuenta lo siguiente:

- ***listar todas las secuencias repetidas de por lo menos 3 caracteres, junto con la distancia a la que se encuentran.***
- ***Ayuda: Aparecen cuatro cadenas de cuatro caracteres que se repiten en el criptograma: JGAZ, NMON, PNFA y AZMJ.***
- ***Estimar cuál puede ser la longitud y obtener la frecuencia de aparición de cada letra como primera de cada bloque.***

Ejercicio 7:

Se cuenta con un texto cifrado que es producto de transposición por columnas (cada ***"n"*** columnas se reacomodó el texto original) y un cifrado de rotación.

a) ¿Qué estrategia usarías para recuperar el mensaje original?

b) Si el texto cifrado tiene "***m***" caracteres, ¿cuántas pruebas requeriría un ataque de fuerza bruta?

Ejercicio 8:

Mostrar que los siguientes cifrados son muy fáciles de quebrar mediante un ataque de **texto plano elegido (chosen-plaintext attack)**.

- **cifrado de sustitución monoalfabética**
- **cifrado de Vigenère**