
nickelodeon
GLITCH
TECHS

Administración y Seguridad de Redes

NOMBRE: MORA HERNANDEZ MARIO ALEJANDRO

INSTITUTO TECNOLOGICO GUSTAVO A. MADERO

INGENIERIA EN TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

PROF. EDGAR AGUSTIN ZEPEDA MARTINEZ

HORARIO: 11 – 13 M – J. 9 - 10 V

EJERCICIOS CRIPTOGRAFIA

ADMINISTRACION Y SEGURIDAD DE REDES

Por lo tanto, los criptógrafos se hurtaron desde el Renacimiento en buscar nuevas técnicas de cifrado, localizando entre otros los denominados polis alfabéticos. En estos, se utilizan varios alfabetos cifrados, de manera que la letra cifrada de una dada necesita de la posición de esta en el texto en claro. De todos ellos, el mas fácil es aquel que usa dos alfabetos de cifrado, uno para las letras que apropiar posiciones pares en el texto en claro y otro para las que se ubican en posiciones impares.

1. Realiza el cifrado de texto en claro “SUSTITUCION POLIALFABETICA” con este sistema.

SUSTITUCION POLIALFABETICA

ADAFEFDIGY MHÑZNÑINRGFZWN

Solución: El mensaje descifrado se debe a que usa el alfabeto para posiciones impares.

2. Descifra el siguiente mensaje

Fdaihumacpvgavhykyhvoapga

TUSCOMPAÑEROSSONUNOSVAGOS

Solución: Tanto el alfabeto par como el impar, se puede usar ambos a la vez para descifrar mensajes.

Una técnica de transposición muy empleado en otros tiempos es el conocido como TRANSPOSICION COLUMNAR. Al iniciar, se escribe el texto en claro en una tabla de un numero establecido de columnas y empleando tantas filas como sea indispensable. Finalmente, el texto cifrado se gana escribiendo primeramente las letras que han permanecido en la primera columna, a continuación las que están en la segunda columna y seguidamente hasta terminar con todas las letras de la tabla.

3. Mediante el método de transposición columnar con cinco columnas, realizar el cifrado del siguiente texto:

EJEMPLO DE TRANSPOSICION COLUMNAR

E	J	E	M	P
L	O	D	E	T
R	A	N	S	P
O	S	I	C	I
O	N	C	O	L
U	M	N	A	R

Mensaje descifrado: ELROOU JOASNM EDNICN MESCOA PTPILR

4. Descifra el siguiente mensaje:

emdcnaaiunnonavnanaesocsesa!

E	M	D	C
N	A	A	I
U	N	N	O
N	A	V	N
A	N	A	E
S	O	C	S
E	S	A	X

Mensaje cifrado: En una semana nos dan vacaciones

La manera anterior se puede enredar empleando una clave consistente en una palabra sin letras repetidas y muchas letras como columnas se quiera que tenga la tabla. Escribiendo la clave encima de la tabla, el texto cifrado sigue de escribir por columnas, pero ahora no se sigue el orden natural de las misma que se escribe ante todo la columna cuya letra de comienza vaya antes en el alfabeto, después la columna cuya letra de la clave sea la siguiente en el alfabeto, y así seguidamente.

5. Utilizando el método de transposición columnar con la clave EMISOR debes realizar el cifrado del siguiente texto en claro:

TENGO QUE HACER EXAMEN COMPLETO DE ADMINISTRACION Y SEGURIDAD DE REDES.

T	E	N	G	O
Q	U	E	H	A
C	E	R	E	X
A	M	E	N	C
O	M	P	L	E
T	O	D	E	A
D	M	I	N	I
S	T	R	A	C
I	O	N	Y	S
E	G	U	R	I
D	A	D	D	E
R	E	D	E	S

Mensaje cifrado: TQCAOTDSIEDR EUEMMOMTOGAE NEREPDIRNUDD GHELNLENAYRDE OAXCEAICSIES

Rotos los métodos de sustitución monoalfabeto por el hallazgo del criptoanálisis por los árabes, desde los años finales de la baja Edad Media, comenzaron a implementarse otros métodos de cifrado, entre los cuales se encuentran los poli alfabéticos y los nomenclátores. Estos últimos basaban en un catálogo de nombres que se ambicionaban esconder, en el que cada uno aparecía acompañado a una palabra, numero o grupo de símbolos que lo suplantan en un texto cifrado

6. Se pide que descifres el texto encriptado

Baa&hpmiyvsvoiylrlxckngkl

↓

122MVERTOINFORMADAL124123

↓

Walshingan muerto informad al Rey Felipe II

Los métodos de sustitución tipo Cesar mudan cada letra de texto en claro por aquella otra ubicada en un número fijo de posiciones tras ella en el alfabeto.

Dominando que el siguiente texto cifrado: iwxsiwyqiniptohigmjvhspsqseojefixsxmtsgivew se ha requerido por un método tipo Cesar, debes descifrarlo considerando que la siguiente tabla de frecuencias característica del español.

ESTO ES UN EJEMPLO DE CIFRADO MONOALFABETICO CESAR

Con tiempo de criptoanalizar un texto cifrado, el primer problema fundamenta en saber si se ha conseguido por un método de transposición o de sustitución. Como en el primer caso las letras no han cambiado de significado, se puede calcular el numero de veces que aparece cada una, y si ese número resultante es más o menos, al que corresponde conforme su frecuencia característica en el respectivo idioma, el cifrado será de transposición.

Utilizando la tabla anterior, con las letras mas usadas en el castellano y su regularidad de uso, argumentar brevemente si el siguiente texto cifrado se ha obtenido por medio de un método de sustitución monoalfabeto o uno de permutación:

Aproximadamente el sig. Numero de letras está en lo siguiente:

Letra	Numero	Porcentaje
E	49	13%
A	43	12%
O	32	9%
I	9	2%
S	29	8%
N	28	8%
Total de letras	368	--