INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

CRIPTOGRAPHY

Grupo:

3CV1

Alumnos:

Caballero Huesca Carlos Eduardo

Martínez García Brando Josué

Cifrado de Vigenére.

Este cifrado consiste en realizar la suma (módulo el número de caracteres en el alfabeto) de la clave y el texto en claro, una vez que se ha asignado un valor entero a cada carácter del alfabeto.

Ejemplo:

Sea:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

E	R	A
4	18	0

Clave

E	N	T	O	N	C	E	S	U	N	A	A	L	D	E	A
4	13	20	15	13	2	4	19	21	13	0	0	11	3	4	0

Mensaje

E	N	T	O	N	C	E	S	U	N	A	A	L	D	E	A
E	R	A	E	R	A	E	R	A	E	R	A	E	R	A	E

4	13	20	15	13	2	4	19	21	13	0	0	11	3	4	0
4	18	0	4	18	0	4	18	0	4	18	0	4	18	0	4

Clave + Mensaje mod #Caracteres del Alfabeto

8	4	20	19	4	2	8	10	21	17	18	0	15	21	4	4
I	E	T	S	E	C	I	K	U	Q	R	A	O	U	E	E

IETSECIKUQRAOUEE

Criptograma

El mensaje se recupera realizando la resta (módulo el número de caracteres en el alfabeto de la clave y el criptograma.

8	4	20	19	4	2	8	10	21	17	18	0	15	21	4	4
I	**E**	**T**	**S**	**E**	**C**	**I**	**K**	**U**	**Q**	**R**	**A**	**O**	**U**	**E**	**E**
E	**R**	**A**	**E**	**R**	**A**	**E**	**R**	**A**	**E**	**R**	**A**	**E**	**R**	**A**	**E**
4	18	0	4	18	0	4	18	0	4	18	0	4	18	0	4

4	13	20	15	13	2	4	19	21	13	0	0	11	3	4	0
E	**N**	**T**	**O**	**N**	**C**	**E**	**S**	**U**	**N**	**A**	**A**	**L**	**D**	**E**	**A**

Clave - Mensaje mod #Caracteres del Alfabeto

ENTONCESUNAALDEA → ***Mensaje***

Ejemplo 2.

Clave: COM Mensaje: HARRY JAMES POTTER

H	**A**	**R**	**R**	**Y**	**J**	**A**	**M**	**E**	**S**	**P**	**O**	**T**	**T**	**E**	**R**
7	0	18	18	25	9	0	12	4	19	16	15	20	20	4	18
C	**O**	**M**	**C**	**O**	**M**	**C**	**O**	**M**	**C**	**O**	**M**	**C**	**O**	**M**	**C**
2	15	12	2	15	12	2	15	12	2	15	12	2	15	12	2

9	15	3	20	13	21	2	0	16	21	4	0	22	8	16	20
J	**O**	**D**	**T**	**N**	**U**	**C**	**A**	**P**	**U**	**E**	**A**	**V**	**I**	**P**	**T**

J	**O**	**D**	**T**	**N**	**U**	**C**	**A**	**P**	**U**	**E**	**A**	**V**	**I**	**P**	**T**
9	15	3	20	13	21	2	0	16	21	4	0	22	8	16	20
C	**O**	**M**	**C**	**O**	**M**	**C**	**O**	**M**	**C**	**O**	**M**	**C**	**O**	**M**	**C**
2	15	12	2	15	12	2	15	12	2	15	12	2	15	12	2

7	0	18	18	25	9	0	12	4	19	16	15	20	20	4	18
H	**A**	**R**	**R**	**Y**	**J**	**A**	**M**	**E**	**S**	**P**	**O**	**T**	**T**	**E**	**R**

Para romper con este cifrado, hay que observar y cuantificar la frecuencia de aparición de cada letra en determinado idioma. Teniendo esto observamos que símbolos se repiten más y suponer

que es una de las letras con más frecuencia. Y también es común que antes o después de una vocal exista una consonante. Con estos criterios podemos ir descartando y proponer candidatos para descifrar el mensaje.

Cifrado Hill

El cifrado de Hill fue inventado en el año de 1929 por el matemático Lester S. Hill.

Este cifrado utiliza el álgebra lineal, especialmente el álgebra de matrices, esta tecnica permite el cifrado polialfabetico esto quiere decir que una letra puede tener diferentes valores en una misma palabra, dependiendo de cómo se encripte.

Las reglas que se utilizan para el cifrado son las siguientes.

Asignarle a cada letra su correspondencia en número a partir del cero.

La clave a utilizar puede ser de varias letras, dependiendo del mensaje, pero debe ser posible colocarlas en una matriz de n x n.

La matriz utilizada debe tener matriz inversa, ya que se necesitará para poder descifrar el mensaje en claro.

Todas las operaciones aritméticas se harán con módulos los cuales se tomarán en módulo n, donde n es el tamaño del alfabeto utilizado.

Ejemplo

Vamos a encriptar las palabras latinoamericana

Para lo cual hacemos su respectiva correspondencia en números.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

La palabra quedará 11,0,19,8,13,14,0,12,4,17,8,2,0,13,0

Lo ponemos en forma de matriz

$$A=\begin{pmatrix} 11 & 8 & 0 & 17 & 0 \\ 0 & 13 & 12 & 8 & 13 \\ 19 & 14 & 4 & 2 & 0 \end{pmatrix}$$

Y nuestra matriz de clave será

$$B=\begin{pmatrix} 3 & 8 & 2 \\ 10 & 0 & 3 \\ 8 & 5 & 1 \end{pmatrix}$$

Convertimos la matriz del mensaje en bloques, en 5 bloques de 3

$$C1=\begin{pmatrix}11\\0\\19\end{pmatrix} \quad C2=\begin{pmatrix}8\\13\\14\end{pmatrix} \quad C3=\begin{pmatrix}0\\12\\4\end{pmatrix} \quad C4=\begin{pmatrix}17\\8\\2\end{pmatrix} \quad C5=\begin{pmatrix}0\\13\\0\end{pmatrix}$$

Ahora multiplicamos la matriz del código por cada uno de los bloques de la matriz

$$(B)(C1)=\begin{pmatrix}3&8&2\\10&0&3\\8&5&1\end{pmatrix}\begin{pmatrix}11\\0\\19\end{pmatrix}=\begin{pmatrix}71\\167\\107\end{pmatrix} \bmod 26=\begin{pmatrix}19\\11\\3\end{pmatrix} \quad \begin{matrix}T\\L\\D\end{matrix}$$

$$(B)(C2)=\begin{pmatrix}3&8&2\\10&0&3\\8&5&1\end{pmatrix}\begin{pmatrix}8\\13\\14\end{pmatrix}=\begin{pmatrix}144\\122\\143\end{pmatrix} \bmod 26=\begin{pmatrix}14\\18\\13\end{pmatrix} \quad \begin{matrix}O\\S\\N\end{matrix}$$

$$(B)(C3)=\begin{pmatrix}3&8&2\\10&0&3\\8&5&1\end{pmatrix}\begin{pmatrix}0\\12\\4\end{pmatrix}=\begin{pmatrix}104\\12\\64\end{pmatrix} \bmod 26=\begin{pmatrix}0\\12\\12\end{pmatrix} \quad \begin{matrix}A\\M\\M\end{matrix}$$

$$(B)(C4)=\begin{pmatrix}3&8&2\\10&0&3\\8&5&1\end{pmatrix}\begin{pmatrix}17\\8\\2\end{pmatrix}=\begin{pmatrix}119\\176\\178\end{pmatrix} \bmod 26=\begin{pmatrix}15\\20\\22\end{pmatrix} \quad \begin{matrix}P\\U\\W\end{matrix}$$

$$\begin{pmatrix}3&8&2\end{pmatrix}\begin{pmatrix}0\end{pmatrix}=\begin{pmatrix}104\end{pmatrix} \quad \begin{pmatrix}0\end{pmatrix} \quad A$$

(B)(C5)=	10	0	3	13	= 0	mod 26 =	0	A
	8	5	1	0	65		13	N

Por lo que la palabra queda: TLDOSNAMMPUWAAN

Para descifrar el código utilizamos la matriz inversa de la matriz clave

La calculamos con la formula $A^{-1}=C^{T}\cdot\left(\det(A)\right)^{-1}$

Primero determinamos el valor del determinante de la matriz, que en este caso es 167, sacamos mod 26 y da 11

Ahora para sacar la matriz inversa multiplicamos 11*19 mod 26 =1, por lo tanto 19 es la inversa.

Posteriormente sacamos la matriz de cofactores.

$$M=\begin{pmatrix} -15 & 14 & 50 \\ 2 & -13 & 49 \\ 24 & 11 & -80 \end{pmatrix}$$

La matriz transpuesta de cofactores es

$$M^{T}=\begin{pmatrix} -15 & 2 & 24 \\ 14 & -13 & 49 \\ 50 & 49 & -80 \end{pmatrix} *19$$

Aplicando la formula

$$A^{-1}=\begin{pmatrix} -285 & 38 & 456 \\ 266 & -247 & 931 \\ 950 & 391 & -1520 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 1 & 12 & 14 \\ 6 & 13 & 21 \\ 14 & 1 & 14 \end{pmatrix}$$

Está matriz es la que utilizamos para descifrar

El sistema de Hill plantea a los criptoanalistas problemas mucho mayores el espacio de claves es mucho mayor, en este caso es de 4C25, es decir las permutaciones de 4 elementos tomados de entre 25 posibles. Y usando una matriz más grande la cantidad de posibles claves se puede hacer tan grande como sea necesario para hacer que sea imposible un ataque por fuerza bruta.

Lo mejor que puede hacer un criptoanalista es tratar de conseguir un código para el cual se conozca una parte del mensaje. Y ver si con ambos datos es capaz de encontrar cual fue la matriz utilizada para encriptar el mensaje.

Cifrado Afin

En aritmética modular, se considera que dos enteros relativos son congruentes modulo n si presentan la misma resta en la división euclidiana por n. Trabajar con modulo n significa trabajar con números enteros comprendidos en el intervalo [0; n-1] incluidos los limites.

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**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Usar como función de cifrado una función afín del tipo ; $\boldsymbol{y = ax + b}$ en las que [a] y [b] son constantes, y en las que [x] e [y] son números correspondientes a las letras del alfabeto en base a esta tabla.

**Nota: si [a]=1, volvemos a encontrar la cifra de Cesar donde [b] representa el desplazamiento. Y el valor de [b] es un número comprendido entre el 0 y el 25.

No podemos utilizar cualquier valor para [a]; [a] y 26 deben ser primos entre sí, lo que significa que no deben tener divisores comunes que no sean 1. Los valores posibles para [a] son pues 1, 3, 5, 7, 11, 15, 17, 19, 21, 23, y 25.

Ejemplo.

Texto en Claro	**H**	**O**	**L**	**A**
X	7	14	11	0
Y	15	0	25	4

$\boldsymbol{a = 9; b = 4;\ y = ax + b}$

H $\quad y = 9(7) + 4 = 67 \bmod 26 = 15 \rightarrow \mathbf{P}$

O $\quad y = 9(14) + 4 = 130 \bmod 26 = 0 \rightarrow \mathbf{A}$

L $\quad y = 9(11) + 4 = 103 \bmod 26 = 25 \rightarrow \mathbf{Z}$

A $\quad y = 9(0) + 4 = 4 \bmod 26 = 0 \rightarrow \mathbf{E}$

Fórmula de descifrado

Invertir (mod 26) la fórmula de cifrado con el fin de expresar [x] en función de [y]

$$y = ax + b$$
$$y - b = ax$$
$$Sabemos\ que\ [a^{-1}][a] = 1$$
$$[a^{-1}](y - b) = x$$
$$\boldsymbol{x = [a^{-1}](y - b)(mod\ 26)}$$

Si $(y - b)$ resulta negativo basta con sumarle 26 antes de multiplicarlo por $[a^{-1}]$

Ejemplo.

Ejemplo

Palabra cifrada: circunferencia

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Haciendo su correspondencia: 2,8,17,2,20,13,5,4,17,4,13,2,8,0

Utilizando la fórmula Y=ax + b (mod 26)

Tomamos a=5 y b=2

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

Texto cifrado

MQJMYPBWJWPMQC

Para descifrar utilizamos la fórmula

x= $[a^{-1}]$(y-b) (mod 26)

Necesitamos encontrar el a^{-1} a=5 por lo que a^{-1} =21

21*5 mod 26=1

Utilizamos la fórmula

X=21(12-2)mod 26= 2

X=21(16-2)mod 26= 8

X=21(9-2)mod 26= 17

X=21(12-2)mod 26= 2

X=21(24-2)mod 26= 20

X=21(15-2)mod 26= 13

X=21(1-2)mod 26= 5

X=21(22-2)mod 26= 4

X=21(9-2)mod 26= 17

X=21(22-2)mod 26= 4

X=21(15-2)mod 26= 13

X=21(12-2)mod 26= 2

X=21(16-2)mod 26= 8

X=21(2-2)mod 26= 0

Para romper con este cifrado al igual que con el de Vigenere, hay que observar y cuantificar la frecuencia de aparición de cada letra en determinado idioma. Teniendo esto observamos que símbolos se repiten más y suponer que es una de las letras con más frecuencia. Y también es común que antes o después de una vocal exista una consonante. Con estos criterios podemos ir descartando y proponer candidatos para descifrar el mensaje.