Universidad Católica
San Pablo

CIENCIA DE LA COMPUTACIÓN

ALGORITMOS DE CRIPTOGRAFÍA TRADICIONAL

ÁLGEBRA ABSTRACTA

-ROBERTO ANTONIO BENAVIDES TORRES
-MARIA GRACIEL CRUZ CÁCERES
-JUAN DIEGO OBANDO ZÚÑIGA
-SHARON DANIELA VALDIVIA BEGAZO
-SOL MORELIA VELÁSQUEZ RODRÍGUEZ

Semestre: 2020-1

ALGORITMOS DE CRIPTOGRAFÍA TRADICIONAL

1. Algoritmo de Playfair:

1.1 Introducción:

El algoritmo de Playfair fue el primer sistema de cifrado en encriptar pares de letras para mensajes enviados por telegrama, fue inventado en 1854, por Charles Wheastone, pero lleva el nombre de su amigo Lord Playfair quien lo promovió para su uso militar, se encuentra en la criptografía simétrica y usa el método de sustitución

1.2 Cifrado:

El algoritmo utiliza una matriz de 5x5, utilizando el alfabeto ingles quedaría de esta forma:

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

Las letras I/J se escriben en un espacio para que el alfabeto pueda encajar en la matriz.

Tomando que:

Clave: mar

Mensaje a cifrar: se ha mareado hoy

1.-Debemos reemplazar nuestra palabra clave al inicio de la matriz y completar con el resto del alfabeto. La matriz quedaría de esta forma:

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

2.- El mensaje original se divide en pares de caracteres, todos los caracteres en cada par deben ser diferentes, en caso de igualdad se inserta una “x” donde

sea necesario, también si la cantidad de letras en la frase es impar se le inserta una “x” al final. La frase dividida en pares quedaría de esta forma:

se-ha-ma-re-ad-oh-oy

3.- Viendo la matriz generada con la clave, se presentan los siguientes casos:

a) Las dos letras en el par están en la misma fila y diferente columna, en ese caso, se desplaza una columna a la derecha (si una de las letras esta al final de la fila se reemplaza por la letra que hay al principio de la fila).

$$(a_{ij};\ a_{ik}) \longrightarrow (a_{ij}+1;\ a_{ik}+1)$$

b) Las dos letras en el par están en la misma columna y diferente fila. En ese caso se desplaza la letra una fila hacia abajo (si una de las letras esta al final de la columna se reemplaza por la letra que hay al principio de la columna).

$$(a_{ik};\ a_{jk}) \longrightarrow (a_{(i+1)k};\ a_{(j+1)k})$$

c)Las dos letras del par están en filas y columnas diferentes. Se realiza la siguiente operación (Para codificar la primera letra se mira en su fila hasta llegar a la columna que contiene la segunda letra, la letra en esa intersección cifrará a la primera letra. La segunda letra es reemplazada por la correspondiente letra que ocupa el lugar de la columna de la primera letra y de la fila de la segunda):

$$(a_{ki};\ b_{js}) \longrightarrow (a_{ks};\ b_{ji})$$

4.-Aplicando lo anterior se cifraría de la siguiente manera:

se (las dos letras están en filas y columnas distintas) se transforman en **QF**
ha (las dos letras están en filas y columnas distintas) se transforman en **EC**
ma (las dos letras están en la misma fila y diferente columna) se transforman en **AR**
re (las dos letras están en filas y columnas distintas) se transforman en **AF**
ad (las dos letras están en filas y columnas distintas) se transforman en **ME**
oh (las dos letras están en la misma columna y filas distintas) se transforman en **UO**
oy (las dos letras están en filas y columnas distintas) se transforman en **NZ**

La frase cifrada quedaría de así: QF-EC-AR-AF-ME-UO-NZ

1.3 Descifrado:

Utilizando la matriz generada con la tabla que es la siguiente:

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

Por cada dos letras vamos aplicando los siguientes casos:

a) Las dos letras en el par están en la misma fila y diferente columna, en ese caso, se desplaza una columna a la izquierda (si una de las letras esta al inicio de la fila se reemplaza por la letra que hay al final de la fila).

b) Las dos letras en el par están en la misma columna y diferente fila. En ese caso se desplaza la letra una fila hacia arriba (si una de las letras esta al final de la columna se reemplaza por la letra que hay al final de la columna).

c)Las dos letras del par están en filas y columnas diferentes. Se realiza lo siguiente: Para decodificar la primera letra se mira en su fila hasta llegar a la columna que contiene la segunda letra, la letra en esa intersección cifrará a la primera letra. La segunda letra es reemplazada por la correspondiente letra que ocupa el lugar de la columna de la primera letra y de la fila de la segunda)

1.4 Criptoanálisis:

Los puntos débiles de Playfair son los siguientes:

- Imposibilidad de que una letra sea codificada como ella misma.
- Se trata de una sustitución simple aplicada a los pares de letras en la que existe una correspondencia unívoca entre cada par de letras y su cifra.
- Cada letra puede sustituirse, exclusivamente, por las que comparten con ella línea o columna en el cuadro, lo que no hace más que ocho en total y puede revelar la estructura del cuadro.
- Dos pares de letras que sean invertidos darán lugar a dos nuevos pares de letras también invertidos. Con el ejemplo anterior, la sílaba **LE** se convertiría en **TL** mientras que la sílaba **EL** se convertiría en **LT**.

2. Algoritmo Affine:

2.1 Introducción:

El algoritmo Affine o cifrado mono alfabético genérico es un tipo de cifrado por sustitución

2.2 Cifrado:

La idea consiste en usar como función de cifrado una función afín del tipo **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.

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

Evidentemente para que la letra cifrada [y] sea también un número entre 0 y 25, trabajaremos módulo 26.

La verdadera formula será pues [y = (ax + b) (mod 26)]. Podemos observar que si [a]=1, volvemos a encontrar la cifra de Cesar donde [b] representa el desplazamiento.

El valor de [b] es un número entero comprendido entre 0 y 25. Un desfase de 26 es equivalente a un desfase de 0.

¡Cuidado! 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.

¿Por qué esta condición? Lo más sencillo es comprobar lo que ocurre se [a] toma un valor prohibido. Elijamos por ejemplo [a=2], y [b=0]. Si ciframos todas las letras del alfabeto

PLANO	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
CIFRADO	A	C	E	G	I	K	M	O	Q	S	U	W	Y	A	C	E	G	I	K	M	O	Q	S	U	W	Y

Observamos que [a] y [n] se han convertido en [A], que [b] y [o] se han convertido en [C]. etc. El problema aparecerá en el momento de descifrar el documento.

EJEMPLO:

- a=9, es un valor válido para a, porque 26 y 9 son primos entre sí, es decir su MCD es 1.
- b=4

Texto plano	h	o	l	a
x	7	14	11	0
y	15	0	25	4
Texto cifrado	P	A	Z	E

h - > y = 9 (7) + 4 = 67 (mod 26) = 15

o - > y = 9(14) + 4 = 130 (mod 26) = 0

l - > y = 9 (11) + 4 = 103 (mod 26) = 25

a - > y = 9 (0) + 4 = 4 (mod 26) = 4

2.3 Descifrado:

Para descifrar usamos la inversa del módulo, El inverso modulo n de [b] es el numero entero $[b^{-1}]$ de tal modo que $[b][b^{-1}]](\text{mod } n) = 1$. para calcularla utilizamos el algoritmo de Euclides extendido del MCD.

Es preciso invertir (mod 26) la fórmula de cifrado con el fin de expresar [x] en función de [y].

y=ax + b, ecuación para cifrado. Restemos b

y – b = ax. Para eliminar a, debemos multiplicarlo por su inversa ya que $[a^{-1}] . [a]=1$

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

La ecuación de descifrado es pues $x= [a^{-1}](y-b) (\text{mod } 26)$. Si el paréntesis (y-b) resulta negativo basta con añadir 26 antes de multiplicarlo por $[a^{-1}]$

Ejemplo de descifrado:

Descifremos el mensaje que hemos calculado anteriormente. Como [a=9], $[a^{-1}]=3$. La fórmula de descifrado es pues x=3(y-4) (mod 26)

Texto cifrado	P	A	Z	E
y	15	0	25	4
x	7	14	11	0
Texto plano	h	o	l	a

Primero calcular el inverso de a=9, por el algoritmo de Euclides. Como [a=9], $[a^{-1}]=3$

x= a-1(y-b); a=9; $a^{-1}=3$; b=4

La fórmula de descifrado es **x=3(y-4) (mod 26)**

P - > x = 3 x (15 - 4) = 3 x 11 = 33 (mod 26) = 7

A - > x = 3 x (0 - 4) = 3 x (-4) = -12 (mod 26) = 14

Z - > x = 3 x (25 - 4) = 3 x 21 = 63 (mod 26) = 11

E - > x = 3 x (4 - 4) = 3 x 0 = 0 (mod 26) = 0

El cálculo para [A] (y = 0) se da el caso que (y-b) es negativo, dado que 0-4=-4 <0.

Añadimos 26 antes de multiplicar por 3. El cálculo nos da 3(0-4+26) (mod 26) = 63 (mod 26)= 11.

2.4 Criptoanálisis:

El algoritmo afín es vulnerable a ataques criptoanalíticos, los más habituales son:

- El análisis de frecuencias
- La búsqueda en el espacio de claves

3. Cifrado de Polybios:

1.1 Introducción:

Alrededor del año 150 a. C. se encuentra tal vez el algoritmo de sustitución más antiguo del cual se tiene conocimiento y recibe el nombre de Polybios, en reconocimiento al historiador griego del mismo nombre, a quien se atribuye la creación de este cifrado.

Se trata de un algoritmo trivial, donde cada letra del alfabeto es reemplazada por las coordenadas de su posición en un cuadrado. Es un caso particular de transposición mono-alfabética.

Este algoritmo fue utilizado principalmente por nihilistas rusos encerrados en las prisiones zaristas.

El cifrado utiliza como base una tabla de sustitución como la que se muestra a continuación:

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

Este sistema está pensado para alfabetos con 25 caracteres, así que, para ajustarlo al castellano, cambiaríamos la J por la I y la Ñ por la N.

1.2 Cifrado:

Para cifrar con este algoritmo nos basamos en la posición de la tabla donde se encuentra cada letra de nuestro mensaje original, así el mensaje encriptado resultará de reemplazar cada carácter por las letras que representan la columna y la fila de esta posición.

Como característica importante, el tamaño del mensaje se duplicará al encriptarlo.

EJEMPLO:

H	O	L	A	A	T	O	D	O	S
BC	CD	CA	AA	AA	DD	CD	AD	CD	DC

Mensaje: HOLA A TODOS

Mensaje cifrado: BCCDCAAA AA DDCDADCDDC

1.3 Descifrado:

Para descifrar un mensaje, debemos escoger cada 2 caracteres, los cuales representan la columna y la fila, que luego de intersectarlas nos mostrarán la letra del mensaje original.

EJEMPLO:

CA	AE	CC	BB	DE	AA	BD	AE	DC
L	E	N	G	U	A	J	E	S

Mensaje cifrado: CAAECCBBDEAABDAEDC

Mensaje descifrado: LENGUAJES

1.4 Criptoanálisis:

- No es muy complicado romper este cifrado, ya que es cuestión de comenzar a separar el mensaje cifrado cada dos letras, las cuales indican la fila y columna de la letra del mensaje original. Por lo que básicamente es muy fácil descifrar un mensaje encriptado en este algoritmo.

4. Cifrado de Hill:

4.1 Introducción:

El cifrado de Hill fue inventado, basándose en el álgebra lineal, por el matemático norteamericano Lester S. Hill en 1929.

Es un sistema criptográfico de sustitución polialfabético, es decir, una misma letra puede ser representada en un mismo mensaje con más de un carácter.

Cada letra está representada por un número. A menudo el esquema sencillo A = 0, B = 1, ..., Z = 25 es utilizado, pero esto no es una característica esencial del cifrado. Para encriptar un mensaje, cada bloque de n letras (considerados como un vector) está multiplicado por una matriz invertible n×n (modular 26). Para desencriptar el mensaje, cada bloque es multiplicado por el inverso de la matriz usada para la encriptación.

4.2 Cifrado:

-Para iniciar el cifrado, necesitamos un mensaje y una clave.

Mensaje: CODIGO

Clave: FRVJXDCLN

-Creamos una matriz NxN, con los números que asocian a cada letra del abecedario. En este ejemplo N=3

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

$$A = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix}$$

-Dividimos el mensaje en matrices de Nx1, de igual manera se llenan con los números equivalentes a las letras de nuestro mensaje.

$$P_1=\text{"COD"}=\begin{pmatrix}2\\14\\3\end{pmatrix} \qquad P_2=\text{"IGO"}=\begin{pmatrix}6\\8\\14\end{pmatrix}$$

-Multiplicamos la matriz de la clave, con las matrices del mensaje. Y a los números que conforman nuestra matriz resultante, les aplicamos modulo para que el resultado se mantenga en el rango del abecedario.

$$A\cdot P_1=\begin{pmatrix}5&17&20\\9&23&3\\2&11&13\end{pmatrix}\begin{pmatrix}2\\14\\3\end{pmatrix}=\begin{pmatrix}308\\349\\197\end{pmatrix}=\begin{pmatrix}22\\11\\15\end{pmatrix}(\text{mod }26)$$

$$A\cdot P_2=\begin{pmatrix}5&17&20\\9&23&3\\2&11&13\end{pmatrix}\begin{pmatrix}8\\6\\14\end{pmatrix}=\begin{pmatrix}422\\252\\264\end{pmatrix}=\begin{pmatrix}6\\18\\4\end{pmatrix}(\text{mod }26)$$

-Reemplazamos los números de la matriz resultante por sus letras equivalente, obteniendo como resultado el mensaje cifrado.

Mensaje cifrado: WLPGSE

2.3 Descifrado:

Para descifrar, utilizamos la inversa de la matriz clave, sin embargo, debemos tener en cuenta que para saber si una matriz es invertible o no, su determinante debe ser diferente de cero o no divisible por los factores del tamaño del abecedario, en este caso 26, por lo que los factores serían 2 y 13.

-Como primer paso calculamos la determinante de nuestra matriz clave.

$$\begin{vmatrix}5&17&20\\9&23&3\\2&11&13\end{vmatrix}$$

$$|A|=503=\ 9\ (\text{mod }26)$$

-Al ver que nuestra matriz es invertible, calculamos su inversa.

$$A^{-1}=\begin{pmatrix} 798 & -3 & -1227 \\ -333 & 75 & 495 \\ 159 & -63 & -114 \end{pmatrix} \qquad A^{-1}=\begin{pmatrix} 18 & 23 & 21 \\ 5 & 23 & 1 \\ 3 & 15 & 16 \end{pmatrix} (\text{mod}\, 26)$$

-Luego multiplicamos esta matriz por las matrices resultantes de nuestro encriptado y finalmente reemplazamos los números de las nuevas matrices por su equivalente en letra, mostrándonos el mensaje original.

$$\begin{pmatrix} 18 & 23 & 21 \\ 5 & 23 & 1 \\ 3 & 15 & 16 \end{pmatrix}\begin{pmatrix} 22 \\ 11 \\ 15 \end{pmatrix}=\begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix} \text{ (mod 26)} \qquad =\text{COD}$$

$$\begin{pmatrix} 18 & 23 & 21 \\ 5 & 23 & 1 \\ 3 & 15 & 16 \end{pmatrix}\begin{pmatrix} 6 \\ 18 \\ 4 \end{pmatrix}=\begin{pmatrix} 6 \\ 8 \\ 14 \end{pmatrix} \text{ (mod 26)} \qquad =\text{IGO}$$

Mensaje descifrado= CODIGO

4.4 Criptoanálisis:

- Al ser un cifrado polialfabético, es decir que cada letra del mensaje tiene más de un equivalente al encriptarlo, este proceso es más eficiente y seguro que muchos otros que son monoalfabéticos. Por lo que a su vez el mensaje es más difícil de descifrar si no se conoce la clave, sin embargo, podemos saber sus dimensiones al dividir el mensaje encriptado entre dos.
- La gran vulnerabilidad de este criptosistema radica en que es muy débil ante un ataque con texto claro conocido, es decir, si el criptoanalista conoce parte del texto en claro correspondiente al texto cifrado del que dispone no tendrá mayor problema para obtener la matriz clave con la que se cifró esa parte del texto en claro y, por tanto, estaría en disposición de descifrar todos los mensajes cifrados con dicha clave. Esta vulnerabilidad se debe a la linealidad de este criptosistema, por lo que con texto claro conocido y empleando el método de Gauss Jordan no es muy difícil obtener la matriz clave.

5. Cifrado Atbash:

5.1 Introducción:

Los sistemas de cifrado de mensajes fueron muy importantes en la antigüedad, todos los pueblos querían cifrar sus comunicaciones pues todos estaban en constante temor a ser invadidos. Por eso el pueblo hebreo ideo su propio sistema de encriptado llamado "Atbash". Este sistema pertenece a la llamada criptografía clásica y es un tipo de cifrado por sustitución.

Fue un sistema muy seguro que se consideró indescifrable durante mucho tiempo. Hay que tener en cuenta que este método de cifrado se ideó para un "abyad" que es un sistema de escritura conformado solo por consonantes ya que la vocalización era más o menos arbitraria, lo que hacía que cualquier palabra cifrada en Atbash fuera pronunciable, cosa que no pasa con un alfabeto como el español o el inglés.

5.2 Cifrado:

El proceso de codificación se realiza mediante la sustitución de la posición que ocupa en el abecedario cada uno de los caracteres en el texto original, por el abecedario invertido, el cual se logra al sustituir la primera letra por la última, la segunda por la penúltima y así sucesivamente.

Original	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
Clave	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

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

5.3 Descifrado:

Para esto se realiza el mismo proceso, pero de manera inversa.

Clave	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
Original	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת

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

5.4 Criptoanálisis:

- Los ataques sobre este tipo de cifrados se suelen hacer por fuerza bruta (cuando hay un espacio reducido de claves), y por análisis de frecuencias. Los análisis de frecuencias es un procedimiento que consiste en el

aprovechamiento de estudios sobre la frecuencia de las letras o grupos de letras en los idiomas para poder establecer hipótesis y aprovecharlas en poder descifrar un texto cifrado sin tener la clave de descifrado.

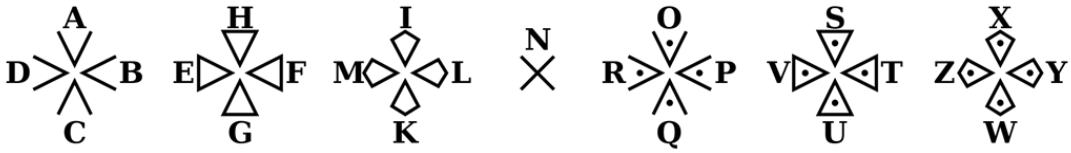
6. Cifrado Pigpen:

6.1 Introducción:

Es un cifrado por sustitución simple que cambia las letras por símbolos. Llamado también "cifrado Francmasón" ya que fue muy utilizado por los masones en el siglo XVIII para preservar la privacidad de sus archivos.

En este caso, la clave consiste en dos tic-tac-toe y dos líneas cruzadas uno de ellos con puntos en las intersecciones respectivamente, luego se coloca una letra del alfabeto en cada espacio del patrón correspondiente.

Aunque existen variantes como la que se cree, empleaban antiguamente los caballeros templarios en la que se usaban variantes de la cruz de malta.



6.2 Cifrado:

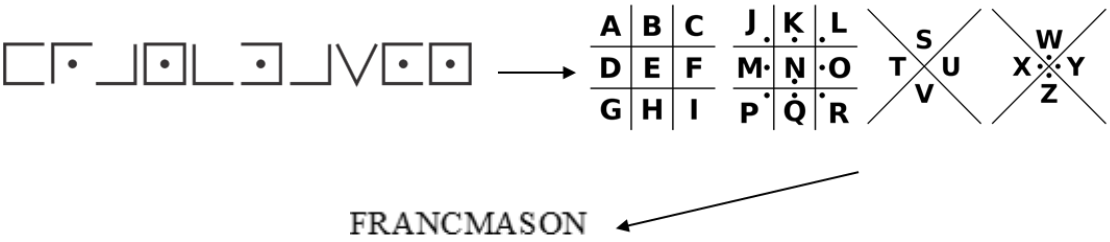
Para encriptar una letra en particular, se buscar la letra en alguna de las cuatro grillas y se escribe la porción de la misma que representa a la letra.

Ejemplo:

F R A N C M A S O N

6.3 Descifrado:

Descifrar un mensaje cifrado mediante PigPen es trivial realizar el proceso inverso si se conoce la distribución del alfabeto.



6.4 Criptoanálisis:

- Si no se sabe la distribución de las letras, entonces hay que proceder mediante la técnica de "análisis de frecuencias" que es muy común en este tipo de cifrado por sustitución.

7. Cifrado rail fence:

7.1 Introducción:

El cifrado Rail Fence también conocido como cifrado en ZigZag es una forma de cifrado por transposición. Su cifrado se realiza al colocar un texto plano en diferentes "líneas de riel" pero es sencillo de ser descifrado y se podría hacer manualmente.

7.2 Cifrado:

Se tienen n líneas de Riel (n es otorgado por la clave) colocadas una debajo de otra.

El texto plano se escribe de manera diagonal, se comienza en el riel superior hacia abajo sobre los rieles hasta llegar al riel inferior, después se continúa cambiando de dirección hacia arriba. Se continúa escribiendo en forma zigzag y cambiando de dirección en el caso que llegue al riel superior o inferior como se ha descrito anteriormente hasta que termine el mensaje que se quiere cifrar. Al final se combinan las diferentes líneas para obtener el texto cifrado

EJEMPLO:

Texto Plano: RailFenceCipher

Clave: 3

Rail Fence:

R				F				e				h		
	a		l		e		c		C		p		e	
		i				n				i				r

Texto cifrado: RFehalecCpeinir

7.3 Descifrado:

Para desencriptar el texto cifrado se puede hacer uso de una cadena de n caracteres llena de asteriscos, donde n es la longitud de la palabra la cual conserva la misma longitud del texto original. Se procede a colocar la cadena en los rieles de la misma manera que se encripta un mensaje para marcar los lugares donde van los caracteres. Se reemplaza en los espacios marcados el texto cifrado de izquierda a derecha fila por fila. Al final se puede observar el texto en zigzag antes de que las filas se combinaran, para leer el mensaje se sigue el patrón de zigzag mencionado en el cifrado.

EJEMPLO:

Texto cifrado: RFehalecCpeinir

Clave: 3

Rail Fence *:

*				*				*				*		
	*		*		*		*		*		*		*	
		*				*				*				*

Reemplazando los lugares marcados por el texto:

R				F				e				h		
	a		l		e		c		C		p		e	
		i				n				i				r

Texto Plano: RailFenceCipher

7.4 Criptoanálisis:

- Es relativamente sencillo de distinguir un mensaje encriptado por rail fence ya que la frecuencia de letras se mantiene después de ser cifrado.

- Si se sospecha que el mensaje fue cifrado por este algoritmo puede ser descifrado fácilmente por fuerza bruta, además son claves bastante sencillas por lo que este algoritmo no es muy seguro.

8. Cifrado running key

8.1 Introducción:

El cifrado Running Key es un cifrado de sustitución polialfabética. Tiene el mismo funcionamiento interno que el cifrado Vigenere, la diferencia radica en cómo es elegida la clave. Running Key cipher a diferencia de Vigenere utiliza una clave mucho más larga generalmente un fragmento de un libro. Usualmente se usará el mismo libro para codificar el mensaje, pero con pasajes aleatorios indicados en alguna parte del mensaje.

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

(tabula recta)

8.2 Cifrado:

La clave es un extracto de un texto o de un libro y se utiliza una tabula recta para cifrar el texto.

Para encriptar un mensaje se escribe la clave encima del texto a encriptar cuidando que cada letra esté encima de solo una letra, si se necesita cifrar un texto más grande se continúa copiando el resto del libro.

De la misma manera de Vigeneré se cifra cada letra del texto plano con la letra que se ubica encima de esta. Para cifrar se extrae de la tabula recta la letra ubicada en la intersección de la columna y fila otorgadas por ambas letras. Se repite el proceso hasta

terminar el mensaje. Si el mensaje fuera más largo que la clave, se sigue extrayendo contenido del texto.

EJEMPLO:

Clave: En un lugar de la Man...

Texto: RUNNINGKEYCIPHER

E	N	U	N	L	U	G	A	R	D	E	L	A	M	A	N
R	U	N	N	I	N	G	K	E	Y	C	I	P	H	E	R
V	H	H	A	T	H	M	K	V	B	G	T	P	T	E	E

Texto cifrado: VHHATHMKVBGTPTEE

8.3 Descifrado:

Para descifrar el mensaje se hace caracter por caracter. Para la primera letra se ubica la fila correspondiente que pertenece a la primera letra de la clave, en esa misma fila se ubica la primera letra del texto cifrado para extraer la letra que corresponde a la columna donde se encuentra la letra cifrada. Se repite el proceso con cada letra hasta haber descifrado todo el texto.

La función de descifrado al igual que Vigeneré:

$$ci = mi - kl \bmod n$$

Donde: i = al carácter i-ésimo del texto plano

l = al carácter l-ésimo de la clave

n = al tamaño del alfabeto

8.4 Criptoanálisis:

- La clave no se repite periódicamente a comparación del cifrado Vigeneré por lo cual hace más complicado romper el código. Si la clave viene de un lugar aleatorio se convierte en “one time pad” que teóricamente son indescifrables. A pesar de eso existen patrones en la clave y en el texto plano que pueden ser explotados.
- Para atacar el cifrado se utiliza posibles textos planos en el texto cifrado probando en las posibles soluciones en busca de texto inteligible.

9. Cifrado Monomio-binomio

9.1 Introducción:

El sistema de cifrado Monomio-binomio, también llamado tablero demediado, es un sistema de cifrado que se basa en una sustitución simple. No obstante, mientras que sistemas como el cifrado de César supone la sustitución de cada letra por otro símbolo, y sistemas como el cuadrado de Polibio o la cifra nihilista suponen la sustitución por dos símbolos correspondientes a las coordenadas de la letra sustituida, el sistema Monomio-binomio permite que algunas letras sean sustituidas por un símbolo y otras por dos símbolos. De acuerdo con David Kahn, su invención fue obra de los rusos.

9.2 Cifrado:

Para cifrar, lo primero es generar un cuadro similar al siguiente en que se ha empleado la palabra mnemotécnica DENARIOS compuesta por las 8 letras más frecuentes en castellano y se ha completado la última línea con una almohadilla (#) para representar otras posibilidades como signos de puntuación, etcétera.

-	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**
-	D	-	E	N	A	R	-	I	O	S
2	B	C	F	G	H	J	K	L	M	Ñ
7	P	Q	T	U	V	W	X	Y	Z	#

Se han dejado dos letras en la primera línea, vacías y representadas por un guion (-), para poder formar el tablero.

Para cifrar, se sustituyen las letras situadas en la primera línea por los números correspondientes a la columna. En el caso de las letras recogidas en las líneas segunda y tercera se les anteceden los números 2 y 7 respectivamente. De esta forma, todo número 2 o 7 señalará que debe escogerse el dúo de números.

9.3 Descifrado:

Para descifrar, se sustituye cada número por su respectiva letra, en caso de encontrar un 2 o un 7 se toma el dúo de números para sustituirlo con la letra correspondiente.

9.4 Criptoanálisis:

- Primero se debe analizar la frecuencia de aparición de los números teniendo así que los dos con mayor frecuencia son referencias a la tabla y no son reemplazables en letras, luego se analiza la frecuencia de aparición de los pares de números, ignorando los números obtenidos al analizar los números de mayor frecuencia, y compararlas con los diagramas más frecuentes del idioma en el cual se supone que se escribió el mensaje original
- Se deberá analizar cuál es el diagrama más ocurrente en el código cifrado y ver qué ocurre si se lo reemplaza por el diagrama más frecuente del idioma, de esta forma se van probando distintas combinaciones entre los diagramas más frecuentes en el mensaje cifrado y los diagramas más frecuentes del idioma hasta que se consigue descifrar el texto.

10. Cifrado de Alberti

10.1 Introducción:

El cifrado de Alberti es el método de cifrado descrito por Leon Battista Alberti en su tratado De Cifris en 1466. Constituye el primer cifrado por sustitución polialfabético conocido. El modo en el que se cambiaba de alfabeto no era periódico (a diferencia de otros cifrados posteriores como el de Vigenère). Para facilitar el proceso de cifrado/descifrado propone unos artilugios conocidos como discos de Alberti.

10.2 Cifrado:

Los discos de Alberti son artilugios que sirven de herramienta para realizar el cifrado de. Estos discos consisten en un armazón fijo en el que está grabado un alfabeto latín convencional ordenado y al final están las cifras 1, 2, 3 y 4. Unido a él por una pieza circular concéntrica y móvil con otro alfabeto grabado de forma que este círculo podía moverse con respecto al otro. De esta forma el usuario puede, mediante un giro del

anillo móvil, emparejar el alfabeto del círculo de arriba con tantos alfabetos del círculo de abajo como giros distintos del anillo dé, hasta un máximo igual a los caracteres del alfabeto empleado.

10.2.1 Código de recifrado y caracteres nulos:

En el anillo fijo (el del alfabeto del texto en claro) aparecen las cifras del 1 al 4. Alberti aprovecha todas las combinaciones de de 2, 3 y 4 cifras de estos números (336=4^2+4^3+4^4 grupos) para poder establecer un código y así aumentar la seguridad del sistema. A este código se le llama «código de recifrado» (en inglés superencipherment). Para aprovechar esta potencialidad tanto el receptor como el emisor deben compartir un «libro de códigos» que indique el significado del cada código usado. En este libro de códigos estarían aquellas palabras o frases de especial trascendencia en el ámbito de uso del cifrado, y por tanto a las que hay que dar mayor seguridad. Por ejemplo, el libro de códigos podría atribuir al código «21» el significado «Lanzar ataque» y al código «23» asignar el significado «Replegarse».

Por otro lado, las cifras son introducidas para despistar y serán descartados cuando el receptor realice el descifrado. Por eso se dice que son «caracteres nulos».

EJEMPLO:

Texto a cifrar: «LAGVER2RASIFARA».

Clave:

El orden del disco móvil es «gklnprtuz&xysomqihfdbace»
Se elige una letra del disco móvil como índice, únicamente conocido por el emisor y el receptor. Supongamos que es la «g».

Se hace coincidir la «g» con la letra del disco móvil que queramos, por ejemplo, la «A». Por tanto, los discos quedan así:

ABCDEFGILMNOPQRSTVXZ1234 Anillo fijo
gklnprtuz&xysomqihfdbace Anillo móvil

El mensaje cifrado comenzará con la letra «A» elegida para indicar cómo están los discos y se continúa sustituyendo hasta que se decide girar el disco. En ese momento se vuelve a poner la letra que coincide con la «g» y vuelta a empezar. Por tanto, si ciframos con la posición anterior de los discos hasta que pasamos a cifrar la letra «S» y ahí cambiamos giramos y ponemos la «g» en la «Q» obtenemos el texto cifrado:

_LAGVER2RA_SIFARA texto a cifrar
AzgthpmamgQlfiyky texto cifrado

Observar que cuando realizó el giro los discos quedan en la posición relativa:

QRSTVXZ1234ABCDEFGILMNOP Anillo fijo
gklnprtuz&xysomqihfdbace Anillo móvil

10.3 Descifrado:

Para descifrar, la letra Mayúscula representa en donde debe estar alineado el anillo móvil y con esto se empieza a sustituir cada letra con su correspondiente, cada vez q se encuentra una letra mayúscula se debe realinear el anillo móvil.

10.4 Criptoanálisis:

- En comparación con los sistemas de cifrado anteriores del tiempo de los Alberti de cifrado era imposible de romper sin el conocimiento del método. Esto fue debido a que la distribución de frecuencias de las letras fue enmascarada y análisis de frecuencia no fue de ayuda, considerando que al usar el libro de códigos el descifrado se hacía más complicado dado que para obtener esta información se debe tener dicho libro.

11. Bibliografía:

- Fundación Wikimedia,Inc. (16 de abril del 2020). Cifrado Afín. 2020, abril 17, de Wikipedia Enciclopedia Libre Recuperado de https://es.wikipedia.org/wiki/Cifrado_af%C3%ADn#Criptoan%C3%A1lisis
- Flores,A & Reséndiz,O. (5 de octubre del 2011). Playfair. 2020, abril 17, de U.N.A.M Criptografía Recuperado de https://unamcriptografia.wordpress.com/2011/10/05/playfair/
- Medina J. (26 de noviembre del 2013). La cifra Afin. 2020, abril 17, de La Güeb de Joaquín Recuperado de http://joaquin.medina.name/web2008/documentos/informatica/documentacion/seguridad/criptografia/CifraAfin/2013_08_22_LaCifraAfin.html#Refh1_La_Cifra_Afin
- Fundación Wikimedia, Inc., (11 de diciembre del 2019). Cifrado de Playfair. 2020, abril 17, de Wikipedia Enciclopedia Libre Recuperado de https://es.wikipedia.org/wiki/Cifrado_de_Playfair
- Wikipedia. (2019). Cuadrado de Polibio. 17 de abril del 2020, de Fundación Wikimedia, Inc. Sitio web: https://es.wikipedia.org/wiki/Cuadrado_de_Polibio
- Eduardo N. Castillo Caballero. (2012). Cifrado de Polybios. 17 de abril del 2020. Sitio web: https://encdesarrollo.wordpress.com/2012/10/09/cifrado-de-polybios/

- Contreras M. Daniel, Flores F. Armando y Reséndiz J. Omar. (2011). Polybios. 17 de abril del 2020, de U.N.A.M Criptografía. Sitio web: https://unamcriptografia.wordpress.com/category/tecnicas-clasicas-de-cifrado/sustitucion/monoalfabetica/monogramica/polybios/
- Santiago Fernández, Vicente Meavilla. (2004). La Criptografia Clásica(PDF). 17 de abril del 2020. Sitio Web: http://www.hezkuntza.ejgv.euskadi.eus/r43-573/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_24/9_Criptografia_clasica.pdf
- Wikipedia. (2019). Cifrado de Hill. 17 de abril del 2020, de Fundación Wikimedia, Inc. Sitio web: https://es.wikipedia.org/wiki/Cifrado_Hill.
- Garcia Larragan, M. (2016, julio 26). Criptografía (XXIV): cifrado de Hill y criptoanálisis Gauss Jordan (II). Recuperado 20 de abril de 2020, de http://mikelgarcialarragan.blogspot.com/2016/07/criptografia-xxiv-cifrado-de-hill-y.html
- Garcia Bautista, J. M. (2019, octubre 6). Élite Diario. Recuperado 18 de abril de 2020, de https://elitediario.com/el-ingenioso-cifrado-del-atbash-hebreo/
- colaboradores de Wikipedia. (2019, octubre 28). Atbash. Recuperado 18 de abril de 2020, de https://es.wikipedia.org/wiki/Atbash
- Gaines, H. F. (1956). Cryptanalysis [Pdf]. Recuperado de https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/cryptanalysis.pdf
- Wikipedia contributors. (2020, abril 7). Pigpen cipher. Recuperado 18 de abril de 2020, de https://en.wikipedia.org/wiki/Pigpen_cipher
- Bacon, H. (2014, noviembre 21). El Cifrado PigPen. Recuperado 18 de abril de 2020, de https://horaciobacon.wordpress.com/2014/11/21/un-mason-en-nueva-york-el-cifrado-pigpen/
- Cifrado "Rail Fence". (2019). Retrieved 17 April 2020, from https://www.geocachingtoolbox.com/index.php?lang=es&page=railFenceCipher
- Kumar, A. Rail Fence Cipher - Encryption and Decryption - GeeksforGeeks. Retrieved 17 April 2020, from https://www.geeksforgeeks.org/rail-fence-cipher-encryption-decryption/
- Knight, S. (2010). The Rail Fence Cipher. Retrieved 17 April 2020, from http://www.cs.trincoll.edu/~crypto/historical/railfence.html
- Running key cipher. (2020). Retrieved 17 April 2020, from https://en.wikipedia.org/wiki/Running_key_cipher
- Lyons, J. (2014). Practical Cryptography. Retrieved 18 April 2020, from http://practicalcryptography.com/ciphers/running-key-cipher/
- gitbooks. (18 de Abril de 2020). Obtenido de https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto11.html
- Wikipedia. (18 de Abril de 2020). Obtenido de https://es.wikipedia.org/wiki/Cifrado_de_Alberti

- Wikipedia. (18 de Abril de 2020). Obtenido de https://es.wikipedia.org/wiki/Monomio-binomio
- Wikiwand. (18 de Abril de 2020). Obtenido de https://www.wikiwand.com/es/Monomio-binomio
- wiki. (19 de Abril de 2020). Obtenido de https://es.qwe.wiki/wiki/Alberti_cipher#Cryptanalysis
- wikizero. (19 de Abril de 2020). Obtenido de https://www.wikizero.com/es/Cifra_VIC