UNIVERSIDAD CENTRAL DEL ECUADOR

COMPUTACIÓN - OCTAVO SEMESTRE

Criptografía y Seguridad de la Información

Algoritmos Criptográficos Básicos

Integrantes:

- Arias Joffre
- Fiallos Fátima
- Flores Byron
- Hurtado Kevin
- Lechón Cristian
- Pila Jordi
- Pujota Angelo
- Tipán Edgar

Docente: Ing. Giovanny Moncayo Unda, MSc

21/04/2025

Cifrados por Transposición (Ejercicio 1)

Son una parte esencial de la criptografía que utiliza la mezcla sistemática de caracteres de texto sin formato o bits para proteger los datos mediante la alteración de sus posiciones en función de alguna forma definida o algoritmo. Además, a diferencia de los códigos sustitutivos donde diferentes letras sustituyen a otras, en estos, simplemente cambia sobre las letras originales, por lo tanto, no se parece en absoluto a ningún mensaje.

La utilización de estas estrategias en metodologías de cifrado relativamente primitivas, que en su simplicidad formaron la base para formas más sofisticadas de codificación

Técnica de Cifrado de Transposición

La Técnica de Cifrado de Transposición es un método de cifrado utilizado para cifrar un mensaje o información. Este método de cifrado se realiza jugando con la posición de las letras del texto sin formato. Las posiciones de los caracteres presentes en el texto sin formato se reorganizan o cambian para formar el texto cifrado. Utiliza algún tipo de función de permutación para lograr el propósito de cifrado. Es muy fácil de usar y tan fácil de implementar.

Cifrado de Transposición por Filas (Ejercicio 2)

El Cifrado de Transposición por Filas es una técnica criptográfica clásica que pertenece a la familia de los cifrados por transposición. En este método, el mensaje original se escribe dentro de una matriz de tamaño determinado, llenando la información **fila por fila**, es decir, de izquierda a derecha y de arriba hacia abajo.

Una vez que el mensaje ha sido distribuido en la matriz, puede leerse en el mismo orden o ser reorganizado de acuerdo con un patrón definido, generando así el mensaje cifrado. En los casos donde el mensaje no completa la totalidad de la matriz, se utilizan caracteres de relleno, comúnmente asteriscos, para ocupar los espacios restantes y mantener la estructura del cifrado.

Este cifrado no modifica el contenido de los caracteres, sino únicamente su posición, lo que contribuye a ocultar el mensaje original mediante un reordenamiento sistemático. Su implementación es sencilla y, aunque no ofrece una seguridad elevada por sí solo, es útil como base para técnicas de cifrado más avanzadas.

Cifrado de Transposición por Columnas (Ejercicio 3)

El Cifrado de Transposición por Columnas es otra variante fundamental dentro de las técnicas clásicas de cifrado por transposición. En este método, el texto sin formato se introduce en una matriz según un número determinado de columnas, llenando la

matriz **por filas**, y luego se reorganizan las **columnas** siguiendo una secuencia específica establecida por una clave.

La clave de cifrado puede estar basada en un orden numérico, una palabra o cualquier otro criterio definido previamente, y se utiliza para permutar las columnas de la matriz antes de extraer el mensaje cifrado. Esta técnica no altera las letras del mensaje original, sino que se limita a modificar su disposición dentro del texto final.

El cifrado por columnas proporciona una mayor complejidad y, por lo tanto, una seguridad más robusta en comparación con otros métodos de transposición más simples. Su simplicidad estructural, combinada con la posibilidad de aplicar múltiples niveles de transposición, lo hace ideal para su estudio y aplicación en la enseñanza de los principios básicos de la criptografía.

El cifrado César (Ejercicio 4)

En el siglo I a.c. aparece un método de cifrado conocido con el nombre genérico de cifrado de César en honor al emperador Julio César y en el que ya se aplica una transformación al texto en claro de tipo mono alfabética. El cifrado del César aplica un desplazamiento constante de tres caracteres al texto en claro, de forma que el alfabeto de cifrado es el mismo que el alfabeto del texto en claro, pero desplazado 3 espacios hacia la derecha módulo n, con n el número de letras del mismo. A continuación, se muestra el alfabeto y la transformación que realiza este cifrador por sustitución de caracteres para el alfabeto castellano de 27 letras.

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

Así con este alfabeto podemos cifrar el siguiente mensaje:
Mensaje original: MENSAJE DE PRUEBA
Mensaje cifrado: OHPVDM GH SUXHED

Al describir el cifrado de César se utilizó un concepto muy usado en las matemáticas y más en criptografía: el módulo.

El módulo es una operación binaria que se realiza en los enteros positivos y se representa de la siguiente forma: c = a mod b de tal forma que a, b y c son enteros positivos.

El valor de c al realizar la operación c = a modulo b es igual al residuo de dividir a entre b. Se puede observar claramente que 0 <= c < b.

Cifrado De Vigenére (Ejercicio 5)

El cifrado de Vigenère está basado en el cifrado del Cesar, por lo cual es un cifrado de sustitución. A diferencia del cifrado del cesar, en el cual cada símbolo del texto plano le es sumada una constante k, en el cifrado de Vigenèrese tiene un cifrado del Cesar por cada símbolo de una palabra clave.Con lo cual, si la palabra clave tiene

una longitud m, se tienen m corrimientos diferentes sobre el texto encriptado. De esta forma, no siempre un mismo símbolo en el texto claro se convierte en el mismo símbolo en el texto encriptado.

A	0	J	9	R	18
B	1	K	10	S	19
C	2	L	11	T	20
D	3	M	12	U	21
E	4	N	13	V	22
F	5	Ñ	14	W	23
G	6	O	15	X	24
H	7	P	16	Y	25
I	8	Q	17	Z	26

Tabla 1.

Si cada símbolo del alfabeto representara un número del 0 al 26, como se muestra en la Tabla 1, se seguiría el siguiente procedimiento: cada letra del texto plano se le sumaría una letra de la clave y como la clave suele ser de menor longitud que el texto plano se repetiría para lograr el tamaño del texto plano. Un ejemplo de esto se muestra en la Tabla 2.

H	O	L	A	Q	U	E	T	A	L
K	E	Y	K	E	Y	K	E	Y	K
Q	S	J	K	U	S	Ñ	X	Y	U

Tabla 2. Ejemplo de cifrado.

En el ejemplo de la tabla 2, se muestra en la primera fila el texto plano a cifrar, en la siguiente fila la clave de cifrado “KEY” repetida hasta lograr la longitud del texto plano y en la última fila se muestra el texto cifrado. Para hacer el cifrado la letra ‘H’ (7) se le suma la letra ‘K’ (10) y se obtiene ‘Q’ (17), a la ‘O’ (15) se le suma la ‘E’ (4) y se obtiene la ‘S’ (19), a la ‘L’ (11) se le suma la ‘Y’ (25) y se obtiene la ‘J’ $(11 + 25 \equiv 36 \equiv 9\ (mod\ 27))$ y así sucesivamente.

Formalmente el cifrado de Vigenère se puede expresar de la siguiente manera. Suponga que n representa la cantidad de símbolos del alfabeto, m representa la longitud de la clave, S_i corresponde al carácter en la posición i del texto plano, K_i corresponde al carácter i de lapalabra clave, y C_i corresponde al carácter i del texto encriptado. Entonces:

$$C_i \equiv S_i + K_{i\ mod\ m}\ (mod\ n) \qquad (3)$$

Para la desencriptación el texto conociendo la clave:

$$C_i \equiv S_i - K_{i\ mod\ m}\ (mod\ n) \qquad (4)$$

Cifrado de Polibio (Ejercicio 6)

Este cifrado fue creado por el historiador griego, Polibio, en el siglo II antes de Cristo. Polibio ideó este sistema para poder transmitir mensajes ocultos a larga distancia mediante señales ópticas y acústicas. Por ello, el emisor y receptor tendrán que haber acordado una clave que en este caso será una matriz 5×5 omitiendo un carácter del alfabeto. Un caso práctico de este cifrado se dio en el siglo XIX-XX por los nihilistas rusos encerrados en las prisiones rusas.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

1. Proceso de cifrado

1. Tomar cada letra del mensaje claro.
2. Localizar su posición (fila, columna) en la matriz.
3. Sustituir la letra por el par numérico que representa su posición

2. Proceso de descifrado

1. Dividir el texto cifrado en pares de dígitos.
2. Para cada par, identificar la fila y columna correspondientes.
3. Recuperar la letra de la matriz.

Ejemplo:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y

MENSAJE ORIGINAL

HOLA

CRIPTOGRAMA

2 3 3 5 3 2 1 1

Bibliografía

- Biblat - Bibliografía latinoamericana. Accedido el 18 de abril de 2025. [En línea]. Disponible: https://biblat.unam.mx/hevila/Revistadigitaluniversitaria/2006/vol7/no7/5.pdf
- “Vista de cripto-análisis sobre métodos clásicos de cifrado”. Revistas UTP. Accedido el 18 de abril de 2025. [En línea]. Disponible: https://revistas.utp.edu.co/index.php/revistaciencia/article/view/6681/3985
- “Cifrado de polibio - web del museo de informática 2.0”. Web del Museo de Informática 2.0. Accedido el 19 de abril de 2025. [En línea]. Disponible: https://museo.inf.upv.es/blog/2021/05/14/cifrado-de-polibio/
- GeeksforGeeks. “Transposition Cipher Techniques in Cryptography - GeeksforGeeks”. GeeksforGeeks. Accedido el 19 de abril de 2025. [En línea]. Disponible: https://www.geeksforgeeks.org/transposition-cipher-techniques-in-cryptography/