UNIVERSIDAD CENTRAL DEL ECUADOR

CRIPTOGRAFÍA Y SEGURIDAD DE LA INFORMACIÓN

NOMBRE: GRUPO 01

FECHA: 11-06-2024

TEMA: Documentación las técnicas de cifrado

PREGUNTA 1

La generación de permutaciones es una técnica fundamental en matemáticas y computación, especialmente en problemas relacionados con la teoría de grafos, criptografía y análisis combinatorio. El algoritmo aquí presentado genera todas las permutaciones posibles de una palabra sin espacios, y luego las ordena alfabéticamente para mostrar las primeras diez. Este tipo de problema se puede abordar utilizando el principio de recursión y el análisis de combinaciones, conceptos fundamentales en criptografía [10]. Además, el análisis de permutaciones tiene aplicaciones directas en criptografía, ya que permite crear claves de cifrado en algoritmos como el AES [11].

El problema consiste en recibir una palabra de longitud n como entrada, y generar todas las permutaciones posibles de la palabra, ordenándolas alfabéticamente. Posteriormente, el algoritmo debe mostrar el número total de permutaciones y las primeras 10. Este tipo de algoritmo es útil en criptografía, donde las permutaciones se utilizan para analizar diferentes configuraciones posibles en algoritmos de cifrado.

El algoritmo presentado es una forma eficiente de generar permutaciones de una palabra y ordenarlas alfabéticamente. Este tipo de procesos tiene aplicaciones en la criptografía y en la generación de claves de cifrado, tal como se analiza en la literatura especializada [10], [11].

PREGUNTA 2

El cifrado por permutación de filas es una técnica que organiza el texto en una matriz de tamaño n×n y luego reorganiza las filas siguiendo un patrón específico de permutación. Este proceso genera un mensaje cifrado en el que los caracteres son desplazados según el orden de la permutación aplicada a las filas de la matriz, como se menciona en el trabajo de Stallings (2017) [1]. Este tipo de cifrado pertenece a la categoría de cifrado por transposición, ya que solo altera la posición de los caracteres sin modificar su valor, tal como se describe en Paar y Pelzl (2011) [2].

La permutación se lleva a cabo desplazando las filas de la matriz una posición hacia abajo, de modo que la última fila ocupa la primera posición, mientras que las filas restantes se desplazan hacia abajo. Este reordenamiento genera un texto cifrado basado únicamente en el cambio de posición de los caracteres, sin alterarlos (Koblitz, 2004) [3].

En el contexto de la criptografía moderna, los algoritmos basados en redes de sustitución-permutación, como el AES (Advanced Encryption Standard), emplean tanto sustituciones como permutaciones en varias rondas para garantizar la seguridad, según Gutiérrez (2003) [4].

PREGUNTA 3

El cifrado por permutación de filas es una técnica que organiza el texto en una matriz de tamaño nxn y luego reorganiza las filas siguiendo un patrón específico de permutación. Este proceso genera un mensaje cifrado en el que los caracteres son desplazados según el orden de la permutación aplicada a las filas de la matriz, como se menciona en el trabajo de Stallings (2017) [7].

Este tipo de cifrado pertenece a la categoría de cifrado por transposición, ya que solo altera la posición de los caracteres sin modificar su valor, tal como se describe en Paar y Pelzl (2011) [8]. La permutación se lleva a cabo desplazando las filas de la matriz una posición hacia abajo, de modo que la última fila ocupa la primera posición, mientras que las filas restantes se desplazan hacia abajo. Este reordenamiento genera un texto cifrado basado únicamente en el cambio de posición de los caracteres, sin alterarlos (Koblitz, 2004) [9]. En el contexto de la criptografía moderna, los algoritmos basados en redes de sustitución-permutación, como el AES (Advanced Encryption Standard), emplean tanto sustituciones como permutaciones en varias rondas para garantizar la seguridad, según Gutiérrez (2003).

El cifrado por permutación de columnas es un método de cifrado simétrico que consiste en reorganizar las columnas de un texto plano para crear un cifrado de texto. Este método se basa en la idea de que la posición relativa de los elementos en un array o matriz determina su significado. En su trabajo sobre cifrado, Stallings (2017) señala que "el cifrado por transposición es un método clásico en el que se reordena la secuencia de caracteres del texto original siguiendo un esquema predefinido. El mensaje se coloca en una tabla de dimensiones determinadas por una clave y luego se lee en un orden diferente, lo que genera el mensaje cifrado" [7]. Por otra parte, Schneier (1996) explica que "una de las técnicas de cifrado más simples es la transposición, donde los caracteres del mensaje se reorganizan sin alterar su valor. Un ejemplo de esto es la permutación de columnas, en la que el mensaje se escribe en una cuadrícula y luego se lee en un orden distinto al de las filas originales" [8]. En cambio, Stinson y Paterson (2018) afirman que "los cifrados por transposición, como la permutación de columnas, son cifrados simétricos en los cuales los caracteres del texto claro se reordenan en posiciones diferentes, sin cambiar el contenido de los caracteres mismos. En conclusión el cifrado de un mensaje por permutación de columnas es una técnica específica de transposición donde el mensaje original se coloca en una matriz de un número determinado de columnas, y luego se reorganizan las columnas de acuerdo con un patrón o clave preestablecida. El mensaje cifrado se obtiene leyendo las columnas en un orden diferente al de su disposición original.

PREGUNTA 4

El **cifrado nono alfabético** es un tipo de cifrado de sustitución en el que cada letra del mensaje original (texto claro) se reemplaza por una letra única de un alfabeto distinto, de forma constante a lo largo del mensaje. Su principal ventaja radica en su simplicidad y facilidad de implementación, pero esta misma característica se convierte en una desventaja cuando se trata de la seguridad. consiste en asignar las letras que van a componer el mensaje cifrado a las letras del alfabeto de forma aleatoria. Esto no es más que hacer una permutación de las letras del alfabeto. [13]

Algoritmo de César.

El algoritmo de César, llamado así porque es el que empleaba Julio César para enviar mensajes secretos, es uno de los algoritmos criptográficos más simples. Consiste en sumar 3 al número de orden de cada letra. De esta forma a la A le corresponde la D, a la B la E, y así sucesivamente. Si asignamos a cada letra un número (A = 0,B = 1. . .), y consideramos un alfabeto de 26 letras, la transformación criptográfica sería:

C= (M+3) mod 26

obsérvese que este algoritmo ni siquiera posee clave, puesto que la transformación siempre es la misma. Obviamente, para descifrar basta con restar 3 al número de orden de las letras del criptograma.

Cifrado Monoalfabético General.

Es el caso más general de cifrado monoalfabético. La sustitución ahora es arbitraria, siendo la clave k precisamente la tabla de sustitución de un símbolo por otro. En este caso tenemos N! posibles claves. [14]

Aunque el cifrado monoalfabético puede haber sido útil en tiempos antiguos, hoy en día se considera inseguro y obsoleto debido a su susceptibilidad a los ataques. Para lograr mayor seguridad, se utilizan métodos más complejos como el cifrado polialfabético o los algoritmos modernos de criptografía simétrica y asimétrica.

PREGUNTA 5

Para el desarrollo de esta pregunta en el enunciado se da a conocer que debemos utilizar el método de sustitución Poli alfabético de Vigenère.

CIFRADO DE VIGENÈRE

El método de Vigenère es un sistema de sustitución poli alfabético, lo que significa que, al contrario que en un sistema de sustitución mono alfabético, cada carácter del texto a cifrar NO se sustituye siempre por el mismo carácter en el texto cifrado, es decir, es un sistema en el que hay implicados varios alfabetos y dependiendo de ciertas circunstancias se aplica uno u otro. [5]

Como funciona: [6] 1º) Se basa en la siguiente tabla:

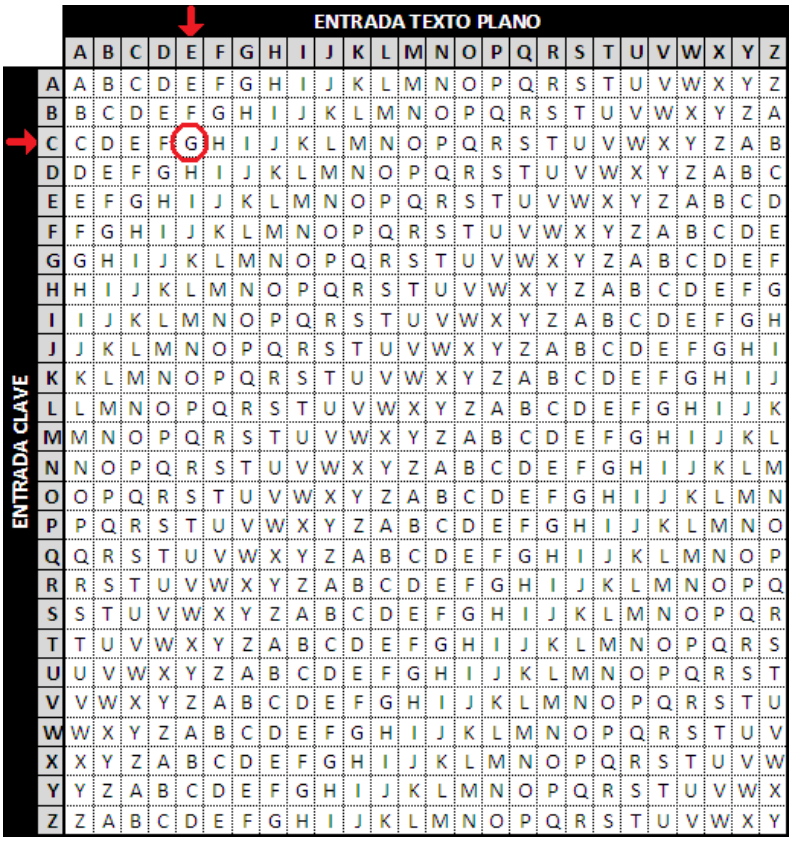
ENTRADA CLAVE	ENTRADA TEXTO PLANO																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P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

2º) Por ejemplo, para cifrar el mensaje "EJEMPLO CIFRADO" con la clave "CLAVE", ponemos la clave encima del texto a cifrar repitiendo la clave tantas veces como haga falta hasta cubrir completamente el texto a cifrar, de la siguiente manera:

Clave -->	C	L	A	V	E	C	L		A	V	E	C	L	A	V
Texto a cifrar -->	E	J	E	M	P	L	O		C	I	F	R	A	D	O

Y ahora para obtener el texto cifrado sólo queda sustituir cada carácter del texto a cifrar por el carácter de la tabla anterior que se encuentra en la intersección entre la columna que corresponde al carácter a cifrar y la fila correspondiente al carácter de la clave que está justo encima, vamos como en el juego de los barcos.

Por ejemplo: a la primera "E" del texto a cifrar, que tiene justo encima la "C" de la clave, le correspondería como carácter en el texto cifrado la letra "G". Es decir:



Si repetimos esto para cada uno de los caracteres del texto a cifrar obtenemos el siguiente mensaje cifrado o criptograma:

Clave -->	C	L	A	V	E	C	L	A	V	E	C	L	A	V
Texto a cifrar -->	E	J	E	M	P	L	O	C	I	F	R	A	D	O
Texto cifrado -->	G	U	E	H	T	N	Z	C	D	J	T	L	D	J

O de igual manera podemos ayudarnos usando la siguiente formula que es la que se utiliza para plasmar esta técnica de cifrado en la computación [6]

Ci = (Pi + Ki) mod 26

Donde:

- (Ci): es la letra cifrada en la posición (i) del texto cifrado.

- (Pi): es la letra en la posición (i) del texto plano.

- (Ki): es la letra en la posición (i) de la clave repetida (si la clave es más corta que el mensaje, se repite hasta igualar la longitud del mensaje).

- (mod 26): indica que el resultado debe estar dentro del rango de 0 a 25 (las posiciones de las letras del alfabeto).

Cada letra en el mensaje y la clave se convierte en un valor numérico: A = 0, B = 1, C = 2, y así sucesivamente hasta Z = 25.

Ejemplo:

Supongamos que queremos cifrar el mensaje "HELLO" con la clave "KEY".

1. Convertimos el texto y la clave en números:
   - Texto plano "HELLO": H=7, E=4, L=11, L=11, O=14
   - Clave "KEY" (repetida para igualar la longitud): K=10, E=4, Y=24, K=10, E=4
2. Aplicamos la fórmula para cada letra:
   - (C1 = (7 + 10) mod 26 = 17) → R
   - (C2 = (4 + 4) mod 26 = 8) → I
   - (C3 = (11 + 24) mod 26 = 9) → J
   - (C4 = (11 + 10) mod 26 = 21) → V
   - (C5 = (14 + 4) mod 26 = 18) → S

3. El mensaje cifrado es "RIJVS".

PREGUNTA 6

Se uso el mismo procedimiento de la pregunta 5

BIBLIOGRAFÍA

[1] W. Stallings, *Criptografía y seguridad en las comunicaciones digitales*, 7ª ed. Madrid, España: Pearson, 2017.

[2] C. Paar y J. Pelzl, *Criptografía: Un enfoque práctico*, 2ª ed. Barcelona, España: Ediciones Reverté, 2011.

[3] N. Koblitz, *Curso de teoría de números y criptografía*, 2ª ed. Madrid, España: McGraw-Hill, 2004.

[4] J. Gutiérrez, "Las Redes Substitución-Permutación y el AES (Advanced Encryption Standard)," *Protocolos criptográficos y seguridad de redes*, vol. 86, 2003.

[5] M. García. “Criptografía (I): Cifrado Vigenère y criptoanálisis Kasiski”. El blog de García Larragan y Cía. Accedido el 6 de noviembre de 2024. [En línea]. Disponible: https://mikelgarcialarragan.blogspot.com/2015/03/criptografia-i.html

[6] UPM. Píldora formativa 19: ¿Qué es la cifra de Vigenère? (4 de marzo de 2015). Accedido el 6 de noviembre de 2024. [Video en línea]. Disponible: https://www.youtube.com/watch?v=8Pb5U64iwV4

[7] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. New Jersey: Pearson Education, 2017, pp. 44-45.

[8] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York: John Wiley & Sons, 1996, pp. 35-36.

[9] D. R. Stinson and M. B. Paterson, Cryptography: Theory and Practice, 4th ed. Boca Raton: CRC Press, 2018, pp. 49-50.

[10] J. M. Huidobro, Introducción a la protección de la información: Criptografía, 1ª ed. Madrid, España: Editorial ABC, 2015.

[11] A. García y M. López, Fundamentos de criptografía moderna, 3ª ed. Barcelona, España: Ediciones UOC, 2018.

[12] F. Sánchez, Algoritmos y estructuras de datos para criptografía, 2ª ed. Ciudad de México, México: Editorial Limusa, 2020.

[13] J. Martin. “Método de Cifrado Mono Alfabético | PDF | Cifrado | Criptoanálisis”. Scribd. Accedido el 6 de noviembre de 2024. [En línea]. Disponible: https://es.scribd.com/document/242886926/Metodo-de-cifrado-mono-alfabetico-docx

[14] “Seguridad Informatica”. UACJ. Accedido el 6 de noviembre de 2024. [En línea]. Disponible: https://www.uacj.mx/CGTI/CDTE/JPM/Documents/IIT/infseguridad/U5-1.html