UNIVERSIDAD CENTRAL DEL ECUADOR

Facultad: Ingeniería y ciencias aplicadas

Carrera: Computación (R)

Semestre: Octavo

Materia: Programación Web

Docente: Geovany Moncayo

Integrantes:

José Alejandro Jiménez Loor

Romina Mishell Guevara Guanuchi

Alexis Fernando Guanoluisa Espin

Tema: Técnicas de cifrado

Fecha de Entrega: 06-11-2024

1) Técnica de permutación

1. Introducción

La generación de permutaciones de una palabra es un proceso que consiste en reordenar todos los caracteres de dicha palabra para obtener todos los posibles anagramas. Esto puede ser usado como una técnica de cifrado básico para ocultar el mensaje en el desorden generado, ya que aumenta la dificultad para interpretar el texto sin una clave o patrón específico.

2. Algoritmo de Permutación

Para una palabra de longitud nn, el número de permutaciones posibles es n!n! (factorial de nn), lo que representa todas las combinaciones posibles de ordenación de los caracteres. Esto es relevante en el cifrado porque cada anagrama puede interpretarse como una variación del mensaje original, y en teoría, el orden correcto solo puede ser conocido por el remitente y el destinatario **[1]**.

Ejemplo:

Dada la palabra "ABC", las permutaciones posibles son "ABC", "ACB", "BAC", "BCA", "CAB" y "CBA".

Complejidad del Algoritmo

Para un algoritmo de permutación de nn caracteres, la complejidad computacional es de O(n×n!)O(n×n!). Esto se debe a que el algoritmo debe recorrer todas las posibles combinaciones de caracteres, un proceso que se vuelve intensivo con palabras de gran longitud **[2]**.

3. Uso en Técnicas de Cifrado

En el contexto del cifrado, la permutación de caracteres de una palabra puede ser empleada como una técnica de ofuscación. Aunque no es un cifrado seguro en el sentido criptográfico moderno, los anagramas son útiles en sistemas donde se busca confundir al lector o añadir una capa de dificultad en la lectura sin una clave específica **[3]**.

La técnica se complementa en cifrados como los basados en transposición, donde los caracteres se reorganizan según un patrón complejo. Los anagramas pueden combinarse con cifrados más avanzados para fortalecer la seguridad.

4. Algoritmos de Permutación en Código

Un algoritmo común para generar permutaciones de una palabra de longitud nn es el método de retroceso (backtracking), que explora todas las posiciones posibles de cada carácter, asegurando la generación de todas las combinaciones posibles sin repeticiones **[4].**

5. Consideraciones Prácticas y Limitaciones

La generación de anagramas como técnica de cifrado tiene limitaciones claras en palabras de longitud elevada, debido al incremento exponencial del tiempo de ejecución. Para

longitudes grandes, el enfoque de permutación directa puede ser ineficaz, por lo que se recomienda su uso en conjunto con otros cifrados o en palabras de longitud limitada **[5]**.

2) Cifrado de un mensaje por permutación de filas

criptografía transposicional, en la que el orden de los caracteres en el mensaje se altera sin cambiar los caracteres en sí. Para aplicar esta técnica, se organiza el mensaje en una matriz y se permutan las filas de acuerdo con una clave secreta.

1.Creación de la Matriz: Se divide el mensaje en bloques de tamaño fijo que llenen una matriz de filas y columnas.

2.Permutación de las Filas: La clave de cifrado indica el orden en que se deben reorganizar las filas de la matriz. Por ejemplo, si la clave es [3, 1, 2], la tercera fila del mensaje se convertirá en la primera, la primera en la segunda y la segunda en la tercera.

3.Extracción del Mensaje Cifrado: Una vez permutadas las filas, el texto cifrado se extrae leyendo la matriz de manera específica (por ejemplo, por filas o columnas consecutivas).

Ejemplo:

Mensaje: "HELLO WORLD" , Matriz de 3 x 4:

- División del mensaje "HEL", "LOW", y "ORLD".
- Aplicar la clave de permutación de filas y reorganizamos.
- Extraer el mensaje cifrado de la matriz reordenada.

Seguridad y Vulnerabilidades

El cifrado por permutación de filas es relativamente fácil de descifrar mediante análisis de patrones, ya que no se altera el contenido del mensaje original, solo el orden de los caracteres. La seguridad de esta técnica puede mejorarse combinándola con otras técnicas de cifrado, como la sustitución de caracteres, para generar un cifrado más fuerte.

3) Cifrado de Mensajes Mediante Permutación de Columnas

Este código implementa un cifrado por transposición de columnas, donde los caracteres de un mensaje se organizan en una matriz cuadrada $n \times n$, el cual se lee por columnas para crear el mensaje cifrado. Los espacios vacíos en la matriz se completan con asteriscos para asegurar un tamaño uniforme.

El cifrado por transposición reorganiza las letras del texto claro para ocultar su significado original sin cambiar los caracteres en sí mismos **[6].** Un enfoque común es la permutación de columnas, que ofrece una estructura fácil de implementar en una matriz cuadrada.

En este código:

1. Se convierte el mensaje en minúsculas y sin espacios.
2. Se verifica que el tamaño de la matriz sea adecuado para contener el mensaje.

3. Se construye la matriz, se llena con el mensaje y se completa con asteriscos en espacios vacíos.
4. Finalmente, se lee la matriz columna por columna para obtener el mensaje cifrado.

Este método permite una implementación simple de cifrado y puede ser una herramienta útil en aplicaciones que requieren un nivel básico de seguridad en el manejo de datos.

4) Cifrado de una cadena de caracteres mediante un método de sustitución

Mono alfabético

El cifrado mono alfabético es una técnica clásica de cifrado por sustitución en la cual cada carácter del texto original es reemplazado por otro carácter de acuerdo con un alfabeto fijo de sustitución **[7]**.

1. Definición del Alfabeto de Sustitución: Para cifrar, se establece una correspondencia fija entre cada letra del alfabeto original y otra letra.

2. Cifrado del Mensaje: Cada letra en el texto original se reemplaza con su correspondiente en el alfabeto de sustitución. Por ejemplo, si usamos un desplazamiento de 3 (como en el cifrado César), cada "A" en el texto plano se convierte en "D", cada "B" en "E", y así sucesivamente.

3. Descifrado del Mensaje: Para recuperar el texto original, se aplica la sustitución inversa, usando el alfabeto de sustitución en sentido opuesto.

Ejemplo:

Mensaje: "HOLA MUNDO" y una clave que desplaza el alfabeto tres posiciones hacia la derecha:

- **Texto original:** HOLA MUNDO
- **Clave de sustitución:** D reemplaza a A, E a B, etc.
- **Texto cifrado:** KRND PXQGR

El cifrado mono alfabético es vulnerable a ataques de análisis de frecuencia, ya que mantiene la frecuencia relativa de las letras del idioma original. Esto significa que, dado suficiente texto cifrado, un criptoanalista puede identificar las letras más comunes y deducir el alfabeto de sustitución, especialmente en lenguajes como el inglés donde ciertas letras (como 'E' y 'T') son mucho más frecuentes **[8]**.

Variantes de Sustitución Mono alfabética

- **Cifrado César:** El desplazamiento es constante, por ejemplo, siempre tres posiciones hacia la derecha.
- **Cifrado Atbash:** Donde se invierte el alfabeto (A → Z, B → Y, etc.).

5) Cifrado de Mensajes Vigenére

El cifrado de Vigenère es un tipo de cifrado por sustitución poli alfabética que utiliza una clave para aplicar desplazamientos a cada letra del mensaje. Cada letra en la clave determina el desplazamiento para la correspondiente letra del mensaje. **[9]**

Parámetros:

Mensaje: El mensaje que se desea cifrar. Este mensaje puede contener caracteres que no están en el alfabeto especificado y que se conservarán sin modificar.

Clave: La clave utilizada para cifrar el mensaje. La clave debe estar en el mismo alfabeto que el mensaje.

Retorno: El mensaje cifrado utilizando el cifrado de Vigenère, donde cada letra ha sido desplazada de acuerdo con la clave.

Detalles de Implementación:

1. Se define el alfabeto de letras en español, incluyendo la letra "ñ".
2. Tanto el mensaje como la clave se convierten a minúsculas para una comparación uniforme.
3. La clave se repite o se trunca para que coincida en longitud con el mensaje original.
4. Para cada letra en el mensaje:
5. Si la letra está en el alfabeto, se calcula su nueva posición en base a la clave.
6. Si la letra no está en el alfabeto (como un espacio o puntuación), se agrega sin cambios **[10]**.

6) cifrado de una cadena de caracteres utilizando la siguiente tabla de cifrado

El cifrado mediante una tabla de sustitución implica reemplazar cada carácter de un texto con otro, siguiendo una tabla predefinida. Esta técnica pertenece a la categoría de cifrados de sustitución y es una de las más antiguas y simples. El método tiene aplicaciones en criptografía elemental y puede ser implementado en sistemas donde no se necesita un cifrado extremadamente robusto **[11]**.

2. Definición de la Tabla de Cifrado

Una tabla de cifrado es un mapeo de caracteres donde cada carácter del alfabeto original se reemplaza con un carácter distinto. La tabla puede ser simple o aleatoria, pero debe ser conocida tanto por el remitente como por el receptor para descifrar el mensaje.

Ejemplo de una Tabla de Cifrado

Supongamos una tabla de cifrado en la que cada letra del alfabeto se sustituye por una letra fija:

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

Con esta tabla, el carácter "A" se convierte en "Q", "B" en "W", "C" en "E", y así sucesivamente.

3. Algoritmo de Cifrado

El algoritmo de cifrado recorre cada carácter de la cadena original y lo sustituye utilizando la tabla de cifrado. Este proceso transforma el mensaje original en un mensaje cifrado ilegible sin la tabla.

Pasos del Algoritmo

1. Crear un diccionario a partir de la tabla de cifrado que mapee cada carácter original a su correspondiente carácter cifrado.
2. Inicializar una cadena vacía para almacenar el mensaje cifrado.
3. Recorrer cada carácter del mensaje original:
    - Si el carácter está en la tabla, sustituirlo por el carácter correspondiente.
    - Si el carácter no está en la tabla (por ejemplo, espacios o signos de puntuación), dejarlo sin cambios.
4. Concatenar cada carácter cifrado en el mensaje cifrado final.
5. Devolver la cadena cifrada **[12]**.

Ejemplo de Uso

Dado el mensaje "HELLO", el cifrado sería:

- "H" → "I"
- "E" → "T"
- "L" → "S"
- "L" → "S"
- "O" → "G"

Mensaje cifrado: **"ITSSG"**

4. Desempeño y Seguridad

Este método es simple y eficiente en términos de tiempo de ejecución, con una complejidad de O(n)O(n)O(n), donde nnn es la longitud del mensaje. Sin embargo, no es un cifrado seguro contra ataques de fuerza bruta o análisis de frecuencia, ya que la estructura de cada carácter es predecible. Para mejorar su seguridad, este método puede combinarse con técnicas como rotaciones o múltiples niveles de sustitución **[13], [14]**.

5. Referencias

[1] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. John Wiley & Sons, 1996.

[2] T. H. Cormen, C. E. Leiserson, R. L. Rivest y C. Stein, Introduction to Algorithms, 3rd ed. MIT Press, 2009.

[3] J. Katz y Y. Lindell, Introduction to Modern Cryptography: Principles and Protocols, 2nd ed. CRC Press, 2014.

[4] R. A. Mollin, An Introduction to Cryptography, Chapman and Hall/CRC, 2000.

[5] W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall, 2006. Este libro presenta una visión general de los cifrados de sustitución y transposición, abordando el cifrado monoalfabético en el contexto de los sistemas de seguridad clásicos.

[6] R. A. Mollin, "An Introduction to Cryptography", CRC Press, 2006. Este libro proporciona una base sólida en técnicas de cifrado, incluyendo el uso de transposiciones y permutaciones en criptografía.

[7] Menezes, P. van Oorschot y S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996. Este manual abarca múltiples técnicas criptográficas, con una explicación de la transposición como método clásico de cifrado y sus limitaciones.

[8] *VPN Unlimited*, "Transposition Cipher," Disponible en: https://www.vpnunlimited.com/es/help/cybersecurity/transposition-cipher

[9] J. Rodríguez y A. Giménez, "*Introducción a la Criptografía*", Universidad de Granada, España, 2011. Disponible en: https://www.ugr.es/~anillos/textos/pdf/2011/EXPO-1.Criptografia/02a11.htm

[10] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. John Wiley & Sons, 1996.
[11] D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, 1996.
[12] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2016.
[13] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
[14] J. Katz and Y. Lindell, *Introduction to Modern Cryptography: Principles and Protocols*, 2nd ed. CRC Press, 2014.