Universidad Central del Ecuador

Criptografía y Seguridad de la Información

Octavo Semestre

- Arteaga Jhon
- Cacuango Mauricio
- Rivera Cristina
- Salazar Augusto

Documentación de las Técnicas de Cifrado

2024-2025

Contenido

TÉCNICAS DE CIFRADO DE LOS ALGORITMOS CRIPTOGRÁFICOS

Técnicas de cifrado usadas en el algoritmo 1.

El primer algoritmo no es una técnica de cifrado, sino un proceso de generación de permutaciones de una palabra, comúnmente conocidas como "anagramas". Los anagramas, o permutaciones de una palabra, son un problema combinatorio clásico que se aborda mediante algoritmos de permutación [1]. En otras palabras, consiste en la reorganización de las letras de una palabra para formar diversas combinaciones, sin añadir ni eliminar caracteres.

Técnicas de cifrado usadas en el algoritmo 2.

El segundo algoritmo usa un tipo de cifrado conocido como cifrado por transposición, específicamente una transposición de filas y columnas [2]. En esta técnica, el mensaje se organiza en una matriz de tamaño definido por el usuario, con un número de filas y columnas determinado, y se rellena en orden vertical. Posteriormente, el mensaje cifrado se obtiene al leer los caracteres en orden horizontal. Este método reorganiza el texto para enmascarar el mensaje original sin cambiar los caracteres en sí mismos.

Características del Cifrado por Transposición

El cifrado por transposición es una técnica en la que el orden de los caracteres del texto original es alterado según una regla específica, en este caso, el orden de los caracteres en la matriz. A diferencia de los cifrados por sustitución [3], donde los caracteres se reemplazan por otros, en el cifrado por transposición el contenido del mensaje se desordena sin modificar los caracteres individuales. Esto lo hace vulnerable a ciertos tipos de ataques, ya que un adversario podría revertir el proceso con análisis cuidadosos.

Este tipo de cifrado tiene varias variantes, como el cifrado de columnas, en el que los caracteres se colocan en una matriz de columnas y luego se leen en un orden distinto, y el cifrado de filas, que funciona de manera similar, pero con lectura por filas. Los métodos de transposición también pueden combinarse con cifrados por sustitución para aumentar la complejidad, como en el cifrado de doble transposición.

Técnicas de cifrado usadas en el algoritmo 3.

El cifrado por permutación de columnas es un método de cifrado por transposición en el que los caracteres de un mensaje se reorganizan al escribirlos en una matriz de tamaño n x n y luego se leen columna por columna. Este proceso reorganiza los caracteres del texto plano para ocultar el contenido original del mensaje. Una vez que se rellena la matriz, y se completa con un carácter como * si es necesario, el texto cifrado se obtiene leyendo los caracteres de arriba a abajo en cada columna. Según Stallings [4], este tipo de cifrado pertenece a los métodos de transposición, que proporcionan una estructura simple y accesible para encriptar mensajes, pero tienen vulnerabilidades que pueden ser explotadas por métodos de criptoanálisis. Schneier [5] también destaca que, aunque este

método es fácil de implementar, su estructura predecible lo hace susceptible a permutaciones inversas y análisis de patrones.

Técnicas de cifrado usadas en el algoritmo 4.

El cifrado por desplazamiento, también conocido como cifrado César, es una técnica de cifrado simple en la que cada letra en el texto original se sustituye por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Este método es una forma de cifrado de sustitución y se considera uno de los más antiguos y básicos en la criptografía.

Este proceso puede representarse de manera más formal mediante la fórmula:

$$Ci = (Pi + d)$$

donde Ci es la letra cifrada, Pi es la letra origiynal,nal, y d es el desplazamiento. Para descifrar, se utiliza:

$$Pi = (Ci - d)$$

Técnicas de cifrado usadas en el algoritmo 5.

El cifrado de Vigenère es un método de cifrado polialfabético que utiliza una clave para modificar la sustitución de letras en un mensaje. El cifrado se basa en una tabla conocida como tabla de Vigenère, que permite la sustitución de letras. Para cifrar un mensaje, se utiliza una clave que se repite a lo largo del texto. Cada letra del texto claro se combina con la letra correspondiente de la clave mediante una operación de suma modular (mod 26). Por ejemplo, si el mensaje es "TEXTOPLANO" y la clave es "CLAVE", el proceso sería:

1. Repetir la clave hasta que tenga la misma longitud que el mensaje.
2. Sumar las posiciones alfabéticas de cada letra del texto y la clave.
3. Aplicar la operación módulo 26 para obtener la letra cifrada.

Técnicas de cifrado usadas en el algoritmo 6.

El cifrado basado en una tabla de sustitución es una técnica de cifrado por sustitución monoalfabética donde cada carácter del mensaje se reemplaza por un par de caracteres que representan su posición en una matriz predefinida. Esta matriz tiene etiquetas de fila y columna que ayudan a localizar el carácter y determinar sus coordenadas. Si un carácter no se encuentra en la matriz, se reemplaza con un marcador como **. Singh [6] explica que los cifrados de sustitución monoalfabética son una forma básica de ocultar el significado de un texto, pero son susceptibles a ataques de análisis de frecuencia que pueden aprovechar los patrones de letras comunes en un idioma. Katz y Lindell [7] señalan que, aunque este método proporciona un enfoque sencillo para el cifrado, no es suficientemente seguro frente a técnicas modernas de criptoanálisis, debido a la predictibilidad de los patrones de sustitución.

Bibliografía

[1] C. E. L. R. L. R. y. C. S. T. H. Cormen, Introduction to Algorithms, MIT Press: 3a, 2014.

[2] R. Villegas Gómez, Comparativa de seguridad de algoritmos de cifrado asimétrico., D.F.: ESIME, 2009.

[3] S. A. Hannan y A. M. Asif, Analysis of polyalphabetic transposition cipher techniques used for encryption and decryption, Albaha: International Journal of Computer Science and Software Engineering (IJCSSE), 2017.

[4] W. Suallings, Cryptography and Network Security: Principles and Practice, United States: Pearson, 2020.

[5] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, New York: Wiley, 2007.

[6] S. Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, United Kingdom: Fourth States, 1999.

[7] J. Katz y Y. Lindell, Introduction to Modern Cryptography, Florida: CRC Press, 2021.