Universidad Central del Ecuador
Carrera de Computación
Criptografía y Seguridad de la Información

Tema: Tarea03-U1-G05
Documentación de Algoritmos Criptográficos Básicos

Integrantes:
Pineda Marco
Ramírez Leonardo
Vinueza Edlith

Algoritmo 1: Cifrado mediante permutaciones

La exploración del cifrado a través de permutaciones revela un enfoque multifacético para mejorar la seguridad de los datos. Las permutaciones sirven como elemento fundamental en varios esquemas de cifrado, proporcionando un mecanismo para oscurecer los datos de manera efectiva. Esta síntesis de la investigación destaca varios aspectos clave del cifrado basado en permutación.

Esquemas de cifrado basados en permutación

- **Diseño y seguridad**: Varios esquemas de cifrado, como PCBC, POFB, PCFB y PCTR, utilizan permutaciones para mejorar la seguridad contra ataques adaptativos, demostrando su aplicación práctica en escenarios en tiempo real [1].
- **Encriptación de contenido:** En las redes centradas en el contenido, se emplean permutaciones para cifrar objetos de datos, creando manifiestos que facilitan el reensamblaje autorizado del contenido, asegurando así la integridad y confidencialidad de los datos [2].

Técnicas criptográficas

- **Grupos de permutación:** Los sistemas de cifrado que aprovechan los grupos de permutación sintetizan claves simétricas y asimétricas, mejorando la seguridad de los mensajes transmitidos [3].
- **Propiedades Estadísticas:** El uso de isomorfismos y permutaciones tiene como objetivo desarrollar cifrados con propiedades estadísticas robustas, cruciales para resistir el criptoanálisis [4].

Contar permutaciones

- **Fortaleza criptográfica:** La investigación indica que comprender el número de permutaciones que fijan ciertos elementos puede informar el diseño de sistemas criptográficamente fuertes, enfatizando la importancia de la selección de permutaciones en criptografía [5].

Si bien el cifrado basado en permutación ofrece ventajas significativas, es esencial considerar posibles vulnerabilidades, como el riesgo de uso indebido o una administración inadecuada de claves, que pueden socavar la eficacia de estos sistemas.

Algoritmo 2: Cifrado mediante permutación de filas

El concepto de encriptación a través de la permutación de filas, particularmente con N filas como clave, se explora en diversos estudios enfocados en la seguridad y transmisión de datos. Este método implica reorganizar los bloques de datos basados en índices de permutación definidos, mejorando la confidencialidad y la integridad durante el almacenamiento y transmisión de datos. En las siguientes secciones se detallan los mecanismos y aplicaciones de esta técnica de encriptación.

Técnicas de codificación basadas en permutación

- **División de Bloques de Datos: Los** archivos de datos se dividen en bloques de tamaño N, que luego se codifican mediante una función de permutación para generar una clave de datos [6].
- **Claves simétricas y asimétricas:** Los sistemas de cifrado utilizan claves simétricas y asimétricas derivadas de grupos de permutación, lo que permite una transmisión segura de mensajes [2].

Aplicaciones en Privacidad y Seguridad

- **Ocultación de patrones de acceso:** Técnicas como permutar índices de registros de bases de datos pueden oscurecer los patrones de acceso, protegiendo la privacidad del usuario en entornos de nube [7].
- **Resiliencia de errores:** El método de permutación codificada basada en claves (KBCP) mejora el rendimiento de los errores en los canales inalámbricos, asegurando que los datos cifrados permanecen seguros a pesar de los errores de transmisión [8].

Si bien el cifrado basado en permutación ofrece ventajas significativas en la seguridad de los datos, también puede introducir complejidades en la administración de claves y el overhead computacional, lo que podría afectar el performance en entornos con recursos limitados.

Algoritmo 3: cifrado mediante la transposición en columnas

El cifrado mediante la transposición en columnas es un método que reorganiza los caracteres del texto plano para crear texto cifrado, lo que mejora la seguridad de los datos. Esta técnica consiste en organizar el texto plano en una cuadrícula y, a continuación, leerlo por columnas, permutando de manera efectiva el orden de los caracteres. En las siguientes secciones se explican en detalle la mecánica, las variaciones y las aplicaciones de este método de cifrado.

Mecánica de la transposición columnar

- El texto plano está escrito en una cuadrícula rectangular, rellenada fila por fila.
- El texto cifrado se genera leyendo la cuadrícula columna por columna, lo que crea una permutación del mensaje original [11].
- El número de columnas (C) y la longitud del mensaje (L) determinan las dimensiones de la cuadrícula e influyen en la complejidad del cifrado [11].

Variaciones y mejoras

- Técnicas como la transposición diagonal y el uso de un generador criptográfico de números pseudoaleatorios (CPRNG) pueden mejorar la seguridad al introducir aleatoriedad en el proceso de transposición [9] [10].
- Las implementaciones pueden incluir transposiciones simples, dobles o triples, y combinar varios métodos para aumentar la eficacia del cifrado [12].

Aplicaciones y rendimiento

- La transposición en columnas se puede integrar con otros métodos de cifrado para formar sistemas híbridos, lo que mejora la resistencia contra los ataques [9].
- El uso de la transposición matricial en el álgebra lineal aumenta aún más la complejidad y la confidencialidad del proceso de cifrado [13].

Si bien la transposición por columnas ofrece un método sólido para cifrar datos, es fundamental tener en cuenta las posibles vulnerabilidades, como los patrones que pueden surgir del uso repetido o de estructuras clave predecibles. Por lo tanto, se recomienda combinarlo con otras técnicas para mejorar la seguridad.

Algoritmo 4: Método de sustitución Monoalfabético de desplazamiento n caracteres a la derecha.

El método de sustitución monoalfabética, a menudo ejemplificado por el cifrado César, implica cambiar los caracteres del alfabeto en un número fijo de posiciones. Esta técnica crea un mapeo uno a uno entre caracteres de texto plano y texto cifrado, lo que lo convierte en un método de cifrado

sencillo pero eficaz. En las siguientes secciones se explican con más detalle su mecánica, sus aplicaciones y su criptoanálisis.

Mecanismo de sustitución monoalfabética

- Cada letra del texto plano se sustituye por una letra situada en un número fijo de posiciones en el alfabeto.
- Por ejemplo, en un turno de 3, A se convierte en D, B se convierte en E, y así sucesivamente, hasta el final del alfabeto [16].
- Este método se puede generalizar a cualquier cambio de 1 a 25, lo que permite múltiples variaciones del cifrado [16].

Aplicaciones y criptoanálisis

- El cifrado de sustitución monoalfabético se usa ampliamente en tareas de cifrado sencillas debido a su facilidad de implementación [14].
- Las técnicas de criptoanálisis, como el análisis de frecuencias, pueden descifrar estos cifrados de forma eficaz mediante el análisis de la frecuencia de las letras del texto cifrado [15], [17].

Limitaciones

- A pesar de su simplicidad, el cifrado de sustitución monoalfabético es vulnerable al análisis de frecuencias, lo que lo hace menos seguro para la información confidencial [18].
- Se han desarrollado sistemas de cifrado más complejos, como el de Vigenère, para mejorar la seguridad mediante la combinación de varios métodos de sustitución [18].

Si bien el método de sustitución monoalfabética es fundamental en criptografía, su susceptibilidad al análisis pone de manifiesto la necesidad de utilizar técnicas de cifrado más sofisticadas en las aplicaciones modernas.

Algoritmo 5: Cifrado de Vigenere.

Es un metdo para cirfrar texto alfabetico. Utiliza sustitucion polialfabetica mediante la tabla de Vigenere. [19]

La tabla de vigenere consta de 26 alfabetos escritos en filas, cada uno desplazado con 1 posicion a la derecha del anterior. [19]

Para cifrar se utiliza el texto plano y la llave, se forman pares elemento por elemento y se usan como coordenadas en la tabla para encontrar la letra correspondiente. [19]

Bibliografía

1. K. Zheng and P. Wang, "Encryption Schemes based on a Single Permutation: PCBC, POFB, PCFB and PCTR," 2017. doi: 10.5220/0006713804520460.
2. C. A. Wood, "Permutation-based content encryption with manifests in a content centric network," 2016.
3. S. W. Ahn, "Encryption systems and method using permutation group based cryptographic techniques," 2020.
4. B. S. Sattar, "A Proposed Cipher System Using Isomorphism and Permutations," 2018. doi: 10.1109/ICETS.2018.8724627.

5. R. M. Campello de Souza, A. N. Kauffman, and R. C. C. de Lima, "Sobre a Escolha de Permutações para Fins Criptográficos," Journal of Communication and Information Systems, 1997. doi: 10.14209/JCIS.1998.11.
6. J. G. De Froe, "Permutation-based coding for data storage and data transmission," 2021.
7. D. Choi, S. Kim, and Y. Lee, "Address Permutation for Privacy-Preserving Searchable Symmetric Encryption," ETRI Journal, 2012. doi: 10.4218/ETRIJ.12.0111.0243.
8. W. Y. Zibideh and M. M. Matalgah, "Key-Based Coded Permutation ciphers with improved error performance and security in wireless channels," 2014. doi: 10.1109/ICC.2014.6883449.
9. J. Jones, "A Columnar Transposition Cipher in a Contemporary Setting," *IACR Cryptology ePrint Archive*, 2015.
10. U. Thirupalu and E. K. Reddy, "A New Cryptosystem for Ciphers using Transposition Techniques," *International Journal of Engineering Research and Technology*, 2019.
11. B. Bjorkman and R. Talbert, "Fixed Points of Columnar Transpositions," *Journal of Discrete Mathematical Sciences and Cryptography*, 2015, doi: 10.1080/09720529.2014.986910.
12. M. B. Pramanik, "Implementation of Cryptography Technique using Columnar Transposition," 2014.
13. M. A. Shareef and N. Hasani, "Develop a Method for Cryptography by Using Matrix Transpose in Linear Algebra," *Nucleation and Atmospheric Aerosols*, 2022, doi: 10.1063/5.0120611.
14. S. Hubalovsky and M. Musilek, "Algorithm for Automatic Deciphering of Mono-Alphabetical Substituted Cipher Realized in MS Excel Spreadsheet," *Applied Mechanics and Materials*, 2014, doi: 10.4028/www.scientific.net/AMM.513-517.624.
15. J. Luthra and S. K. Pal, "A Hybrid Firefly Algorithm Using Genetic Operators for the Cryptanalysis of a Monoalphabetic Substitution Cipher," 2011, doi: 10.1109/WICT.2011.6141244.
16. R. F. Churchhouse, *Codes and Ciphers: From Julius Caesar to Simple Substitution*, 2001, doi: 10.1017/cbo9780511542978.003.
17. A. Sinkov, *Elementary Cryptanalysis: A Mathematical Approach*, 1998.
18. S. Agustini, W. M. Rahmawati, and M. Kurniawan, "Modified Vigenère Cipher to Enhance Data Security Using Monoalphabetic Cipher," *International Journal of Artificial Intelligence Research*, vol. 1, no. 1, 2019, doi: 10.25139/IJAIR.V1I1.2029.
19. A. Khanduri, “Vigenère Cipher - GeeksforGeeks,” GeeksforGeeks, Oct. 07, 2016. https://www.geeksforgeeks.org/vigenere-cipher/