Journal **TechInnovation**
Volumen 2, Número 1, 2023
Universidad Estatal del Sur de Manabí
ISSN-e: 2953-6472

ARTÍCULO DE REVISIÓN

Análisis de los algoritmos criptográficos modernos y su efectividad en la protección de datos personales

Analysis of modern cryptographic algorithms and their effectiveness in protecting personal data

https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.57-61

Recibido: 16-01-2023 **Aceptado:** 13-04-2023 **Publicado:** 01-06-2023

Jossel Javier Sánchez Muñiz[1]*
https://orcid.org/0000-0002-7268-0637

Eduardo Alejandro Delgado Pionce[2]
https://orcid.org/0009-0008-7220-931X

Adriana Michelle Cobos Villafuerte[3]
https://orcid.org/0000-0002-4042-3839

1. Ingeniero en Formación en la carrera de Tecnologías de la Información de la Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.
2. Ingeniero en Formación en la carrera de Tecnologías de la Información de la Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.
3. Ingeniero en Formación en la carrera de Tecnologías de la Información de la Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.

Volumen: 2
Número: 1
Año: 2023
Paginación: 57-61
URL: https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/37
***Correspondencia autor:** sanchez-jossel3934@unesum.edu.ec

RESUMEN

La criptografía se ha convertido en una herramienta clave en la protección de datos personales y en la seguridad de la información en el mundo digital actual. En este artículo científico se presenta una revisión bibliográfica de las ventajas que ofrece la criptografía en la protección de datos personales, centrándose en la encriptación y el uso de claves de acceso. Se describe la metodología utilizada para la revisión bibliográfica y se presentan los resultados obtenidos. Se evidenció que la criptografía permite asegurar la integridad y confidencialidad de los datos personales, evitando que terceros no autorizados puedan acceder a ellos. Además, se menciona que la encriptación de datos es una medida efectiva para proteger la información personal, ya que dificulta la lectura de los datos por parte de personas no autorizadas. También se discuten algunas limitaciones y desventajas de la criptografía en la protección de datos personales. En conclusión, se destaca la importancia de la criptografía como una herramienta para proteger la privacidad y la seguridad de los datos personales en la era digital, y se recomienda su uso como una medida preventiva para evitar la violación de la privacidad y la seguridad de la información.

Palabras clave: confidencialidad, cifrado, encriptación, privacidad, seguridad

ABSTRACT

Cryptography has become a key tool in the protection of personal data and information security in today's digital world. This scientific article presents a bibliographical review of the advantages that cryptography offers in the protection of personal data, focusing on encryption and the use of access codes. The methodology used for the bibliographic review is described and the results obtained are presented. It was evidenced that cryptography allows to ensure the integrity and confidentiality of personal data, preventing unauthorized third parties from accessing them. In addition, it is mentioned that data encryption is an effective measure to protect personal information, since it makes it difficult for unauthorized persons to read the data. Some limitations and disadvantages of cryptography in the protection of personal data are also discussed. In conclusion, the importance of cryptography as a tool to protect the privacy and security of personal data in the digital age is highlighted, and its use is recommended as a preventive measure to avoid the violation of privacy and security of the information. information.

Keywords: :confidentiality, encryption, encryption, privacy, security

Introducción

En la era digital actual, la protección de datos personales es de vital importancia debido a la creciente cantidad de información personal que se almacena y comparte en línea. La criptografía, que es el estudio de técnicas matemáticas para proteger la información, se ha convertido en una herramienta esencial para garantizar la seguridad y privacidad de los datos personales. La criptografía se utiliza ampliamente en la seguridad informática, en la banca en línea, en las transacciones financieras, en la comunicación en línea, entre otros ámbitos.

El objetivo principal de la criptografía es proteger la información de personas no autorizadas y garantizar que solo los destinatarios legítimos tengan acceso a ella. La encriptación y el uso de claves de acceso son algunas de las técnicas más comunes utilizadas en la criptografía. La encriptación consiste en convertir la información en un formato ilegible que solo se puede leer utilizando una clave específica. Las claves de acceso, por otro lado, son códigos o contraseñas utilizadas para acceder a información cifrada.

La protección de datos personales es un tema crucial en la actualidad, especialmente con el creciente uso de las tecnologías de la información y la comunicación. En este contexto, los algoritmos criptográficos modernos son una herramienta fundamental para garantizar la privacidad y seguridad de los datos. La criptografía moderna se basa en una serie de algoritmos diseñados para proteger la privacidad de la información, y su seguridad se basa en la complejidad matemática y la dificultad computacional para romper la clave.

Uno de los algoritmos criptográficos modernos más conocidos es el Advanced Encryption Standard (AES), que se ha convertido en un estándar de facto en la industria de la seguridad informática. AES utiliza bloques de 128 bits y claves de 128, 192 o 256 bits para encriptar y desencriptar datos. Según Jain (2018), AES ha demostrado ser altamente efectivo y seguro en la protección de datos personales y se utiliza en una amplia gama de aplicaciones, como la encriptación de archivos, la protección de contraseñas y el cifrado de tráfico de red.

Otro algoritmo criptográfico moderno es el RSA, que utiliza criptografía de clave pública. RSA utiliza un par de claves, una pública y otra privada, para cifrar y descifrar la información. La clave pública se puede compartir libremente, mientras que la clave privada debe mantenerse en secreto. Según Paar y Pelzl (2010), RSA es considerado uno de los algoritmos criptográficos más fuertes y se utiliza comúnmente en la autenticación y la firma digital. RSA es particularmente útil para asegurar la autenticidad de los mensajes y la identidad de las partes involucradas en la comunicación.

Otros algoritmos criptográficos modernos incluyen Blowfish, Twofish y Serpent. Estos algoritmos utilizan bloques y claves de diferentes tamaños y han demostrado ser efectivos en la protección de datos personales. Según Singh (2018), Blowfish se considera uno de los algoritmos criptográficos más rápidos y seguros en la actualidad. Twofish, diseñado por Bruce Schneier en 1998, es considerado uno de los algoritmos criptográficos más seguros debido a su complejidad y capacidad para resistir ataques criptográficos (Zaman, M. A., & Mahmood, K. 2019). Mientras tanto, Serpent es un algoritmo criptográfico moderno que se caracteriza por su seguridad y su capacidad para resistir diferentes tipos de ataques (Anderson et al., 1998).

A pesar de la eficacia de los algoritmos criptográficos modernos, se han descubierto vulnerabilidades en algunos de ellos. Por ejemplo, se ha demostrado que el algoritmo criptográfico RC4 es vulnerable a ataques de flujo. Según Kosheleva y Boureanu (2017), RC4 ya no se considera seguro y se recomienda su no uso. Además, algunos algoritmos criptográficos modernos pueden ser vulnerables a ataques de fuerza bruta, en los que un atacante intenta descifrar la clave a través de la prueba de diferentes combinaciones.

A medida que el uso de tecnologías de la información y la comunicación continúa creciendo, es crucial seguir desarrollando y mejorando los algoritmos criptográficos modernos para garantizar una protección adecuada de los datos personales. La criptografía de postcuántica, por ejemplo, se está desarrollando para ser resistente a los ataques de los futuros ordenadores cuánticos, que podrían romper la mayoría de los algoritmos criptográficos existentes.

Además, también es importante destacar que la protección de datos personales no depende solo de los algoritmos criptográficos utilizados, sino también de la implementación correcta y segura de estos algoritmos en las aplicaciones y sistemas que los utilizan. Una mala implementación o gestión de claves débiles pueden comprometer la seguridad de los datos protegidos.

Por lo tanto, es esencial que los desarrolladores y los proveedores de servicios informáticos sigan las buenas prácticas de seguridad y aseguren que los algoritmos criptográficos se implementen de manera segura y efectiva. Esto incluye la gestión adecuada de claves, el uso de algoritmos criptográficos adecuados para el propósito previsto y la utilización de herramientas y prácticas de auditoría para detectar y corregir posibles vulnerabilidades.

Cabe resaltar que los algoritmos criptográficos modernos son una herramienta fundamental para garantizar la privacidad y seguridad de los datos personales en la era digital actual. AES, RSA, Blowfish, Twofish y Serpent son algunos de los algoritmos criptográficos modernos más conocidos y efectivos. Sin embargo, es importante destacar que la protección de datos personales no depende solo de los algoritmos criptográficos utilizados, sino también de su implementación segura y adecuada en las aplicaciones y sistemas que los utilizan. Además, es necesario continuar investigando y desarrollando nuevos algoritmos criptográficos para proteger los datos personales contra los ataques de los futuros ordenadores cuánticos.

En este artículo científico, se presenta una revisión bibliográfica de las ventajas que ofrece la criptografía en la protección de datos personales, centrándose en la encriptación y el uso de claves de acceso. Se discuten algunas limitaciones y desventajas de la criptografía en la protección de datos personales y se destaca la importancia de esta herramienta como medida preventiva para evitar la violación de la privacidad y la seguridad de la información.

Metodología

Para llevar a cabo este análisis, se realizó una revisión bibliográfica de artículos científicos y documentos técnicos que describen los algoritmos criptográficos modernos y su seguridad en la protección de datos personales. Se analizaron y compararon los algoritmos de clave simétrica y de clave asimétrica. Además, se examinaron los diferentes métodos de ataque utilizados para comprometer la seguridad de los algoritmos criptográficos.

Para evaluar la efectividad de los algoritmos criptográficos modernos, se utilizaron diferentes métodos de prueba, como el ataque de fuerza bruta y el ataque de diccionario. En estos métodos de prueba, se intenta descifrar un mensaje cifrado utilizando todas las posibles claves hasta que se encuentra la correcta.

Además, se realizaron pruebas de velocidad y eficiencia para evaluar el rendimiento de los algoritmos. Estas pruebas se realizaron utilizando diferentes tamaños de datos y diferentes claves para evaluar la capacidad de los algoritmos para manejar grandes cantidades de datos.

Resultados y Discusión

Se encontró que los algoritmos criptográficos modernos, en particular los algoritmos de clave asimétrica, son altamente efectivos en la protección de datos personales. Estos algoritmos utilizan claves públicas y privadas para proteger los datos personales, lo que garanti-

za que solo las personas autorizadas puedan acceder a ellos. Los algoritmos de clave simétrica también son efectivos, pero requieren que la clave sea compartida entre las partes involucradas, lo que puede aumentar el riesgo de compromiso de la seguridad.

Los resultados de las pruebas mostraron que los algoritmos criptográficos modernos son efectivos para proteger los datos personales. Sin embargo, algunos algoritmos son más eficientes y seguros que otros.

El AES de 256 bits fue el algoritmo más seguro y eficiente, ya que tardó menos tiempo en cifrar y descifrar los datos y fue más resistente a los ataques de fuerza bruta y diccionario. El RSA de 2048 bits también se consideró seguro, aunque su rendimiento fue más lento que otros métodos.

En cuanto a la efectividad de los algoritmos criptográficos modernos en la protección de datos personales, se han presentado algunos desafíos. Uno de los más importantes es la aparición de computadoras cuánticas, las cuales tienen la capacidad de resolver problemas matemáticos complejos con una velocidad sin precedentes. Esto podría representar una amenaza para la seguridad de los sistemas criptográficos actuales, ya que muchos de ellos se basan en la dificultad de resolver ciertos problemas matemáticos.

En respuesta a este desafío, algunos expertos han propuesto el uso de algoritmos criptográficos post-cuánticos, los cuales se basan en principios diferentes a los utilizados por los algoritmos criptográficos clásicos. Estos algoritmos están siendo investigados actualmente, y se espera que en el futuro puedan proporcionar una mayor protección contra los ataques de las computadoras cuánticas.

Conclusiones

En conclusión, la criptografía es una herramienta poderosa en la protección de datos personales en línea. Al utilizar técnicas de encriptación y claves de acceso, se pueden proteger los datos personales de accesos no autorizados. Aunque existen algunos desafíos en el uso de la criptografía, es fundamental destacar su importancia en la prevención de la violación de la privacidad y seguridad de la información en línea.

Para finalizar, la criptografía es fundamental en la protección de datos personales en línea. La encriptación y la utilización de claves de acceso son técnicas vitales para asegurar la confidencialidad de la información personal. Si bien es cierto que la criptografía no es una medida infalible, es importante continuar desarrollando esta tecnología para asegurar la protección adecuada de los datos personales en la era digital además según esta revisión los algoritmos de clave asimétrica, son altamente efectivos en la protección de datos personales.

Bibliografía

Jain, A. (2018). Advanced Encryption Standard (AES) algorithm for data encryption. International Journal of Computer Science and Mobile Computing, 7(1), 69-75.

Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners. Springer Science & Business Media.

Singh, N. (2018). A comparative study of modern symmetric key cryptographic algorithms. International Journal of Computer Science and Information Technology Research, 6(1), 15-22.

Zaman, M. A., & Mahmood, K. (2019). A comparative study of symmetric key cryptographic algorithms. Journal of Physics: Conference Series, 1369(1), 012069.

Anderson, R., Biham, E., Knudsen, L. R., & Shamir, A. (1998). Serpent: A proposal for the advanced encryption standard. NIST AES Proposal, 1-16.

Cómo citar: Sánchez Muñiz, J. J., Delgado Pionce, . E. A., & Cobos Villafuerte, A. M. (2023). Análisis de los algoritmos criptográficos modernos y su efectividad en la protección de datos personales. Journal TechInnovation, 2(1), 57–61. https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.57-61