Universidad Siglo 21

Trabajo Final de Grado. Trabajo de Investigación en Tecnologías Informáticas.

Carrera: Ingeniería en Software

Investigación documental sobre el uso de Criptografía en el Desarrollo Seguro de Software.

Autor: Juan Cruz Maurino

Legajo: SOF01618

Tutor: Jorge Humberto Cassi

Córdoba, Junio del 2024.

Índice

Resumen

La presente investigación aborda el análisis documental del uso de la criptografía en el ámbito del desarrollo de software, con un enfoque particular en las técnicas y metodologías que garantizan la seguridad y la privacidad de la información. El objetivo principal fue investigar la aplicación, los mecanismos tecnológicos y las limitaciones en la implementación de estas tecnologías criptográficas. Se examinaron en detalle las dos principales categorías de criptografía: la criptografía simétrica, que utiliza la misma clave para el cifrado y descifrado, y la criptografía asimétrica, que emplea un par de claves pública y privada.

Se describieron aplicaciones específicas de estas tecnologías, como la encriptación de redes de comunicación y bases de datos, así como el uso de algoritmos como AES para cifrado simétrico y RSA para cifrado asimétrico. Los resultados revelaron que estas tecnologías han mejorado significativamente la confidencialidad y protección de datos, proporcionando seguridad en los canales de comunicación y redes. Asimismo, se destacó el papel de la criptografía en la autenticación y en la integridad de la información, factores cruciales en el desarrollo de software seguro.

Además de los beneficios, se abordaron los desafíos tecnológicos y las limitaciones de la implementación de la criptografía en el desarrollo de software. Entre estos desafíos se encuentran la precisión en la implementación, la sincronización de las claves, el costo asociado a la implementación de tecnologías avanzadas y la necesidad de una validación continua de los sistemas criptográficos. Se enfatizó la necesidad de adaptar estas tecnologías a las necesidades específicas de cada aplicación y de mejorar la calidad del software a través de un desarrollo robusto y seguro.

Finalmente, se concluyó subrayando la relevancia de la criptografía en el desarrollo de software, tanto para proteger la información sensible contra accesos no autorizados como para asegurar la integridad y autenticidad de las comunicaciones en diversas aplicaciones. La criptografía se presenta no solo como una herramienta esencial para la seguridad informática, sino también como un componente crítico en el diseño de software seguro y confiable.

Palabras clave: Criptografía, Criptografía Simétrica, Criptografía Asimétrica, Desarrollo de Software, Seguridad Informática, Protección de Datos, Tecnologías Criptográficas.

Abstract

This research addresses the documentary analysis of the use of cryptography in the field of software development, with a particular focus on the techniques and methodologies that ensure the security and privacy of information. The main objective was to investigate the application, technological mechanisms, and limitations in the implementation of cryptographic technologies. The study examined in detail the two main categories of cryptography: symmetric cryptography, which uses the same key for encryption and decryption, and asymmetric cryptography, which employs a pair of public and private keys.

Specific applications of these technologies were described, such as the encryption of communication networks and databases, as well as the use of algorithms like AES for symmetric encryption and RSA for asymmetric encryption. The results revealed that these technologies have significantly improved data confidentiality and protection, providing security in communication channels and networks. The role of cryptography in authentication and information integrity, which are crucial factors in secure software development, was also highlighted.

In addition to the benefits, the technological challenges and implementation impediments of cryptography in software development were addressed. These challenges include the precision of implementation, key synchronization, the cost associated with implementing advanced technologies, and the need for continuous validation of cryptographic systems. The necessity to adapt these technologies to the specific needs of each application and to improve software quality through robust and secure development was emphasized.

Finally, the conclusion underscored the relevance of cryptography in software development, both for protecting sensitive information against unauthorized access and for ensuring the integrity and authenticity of communications in various applications. Cryptography is presented not only as an essential tool for information security but also as a critical component in the design of secure and reliable software.

Keywords: Cryptography, Symmetric Cryptography, Asymmetric Cryptography, Software Development, Information Security, Data Protection, Cryptographic Technologies.

Introducción

La criptografía es esencial en el desarrollo de software para garantizar la seguridad y privacidad de la información. Mediante técnicas de cifrado y autenticación, protege datos sensibles contra accesos no autorizados y asegura la integridad de las comunicaciones en diversas aplicaciones.

Según Lawrence Lessig (1999):

> Las tecnologías de encriptación constituyen el avance tecnológico más importante de los últimos mil años. Ningún otro descubrimiento tecnológico –desde las armas nucleares (espero) hasta Internet– tendrá un impacto más significativo en la vida social y política de la humanidad. La criptografía va a cambiar absolutamente todo (pp. 35-36).

Según la Oficina de Ciencia y Tecnología de la Casa Blanca (Marrero Travieso, 2003):

> Las pérdidas anuales estimadas en Estados Unidos, debido al espionaje económico ascienden a 100 mil millones de dólares. En Internet, las principales amenazas para la protección de la información provienen de:
>
> • Anexos a mensajes enviados por correo electrónico infectados con virus.
>
> • El intercambio de códigos de virus.
>
> • Firewalls o cortafuegos mal configurados.

• Ataques a la disponibilidad de los recursos de información existentes en la red (bancos de datos o software disponibles para descargar por los usuarios).

• La alteración de las páginas web.

• El "repudio" y las estafas asociadas al comercio electrónico.

• Las vulnerabilidades de los sistemas operativos y la desactualización de los "parches" concernientes a su seguridad.

• La rotura de contraseñas.

• La suplantación de identidades.

• El acceso a páginas pornográficas, terroristas, etc.

• El robo y la destrucción de información.

• Pérdida de tiempo durante el acceso a sitios ajenos a la razón social de la entidad.

• El hecho de que herramientas de hacking y cracking se ofrezcan como freeware.

Por estas y otras razones, el tratamiento de los temas relacionados con la seguridad informática ha tomado un gran auge. Los problemas relacionados con la confidencialidad, integridad y autenticidad en un documento electrónico se resuelven mediante la tecnología llamada Criptografía.

De Acuerdo con la definición descrita en *Amazon Web Services (2024):*

La criptografía es una práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas. La

información puede estar en reposo (como un archivo ubicado en un disco duro), en tránsito (una comunicación electrónica intercambiada entre dos o más partes) o en uso (mientras se ejecutan operaciones de computación con los datos). La criptografía tiene cuatro objetivos principales:

- Confidencialidad: poner la información únicamente a disposición de usuarios autorizados.
- Integridad: asegurar que la información no se ha manipulado.
- Autenticación: confirmar la autenticidad de la información o de la identidad de un usuario.
- No repudio: evitar que un usuario deniegue compromisos o acciones previas.

La criptografía utiliza varios algoritmos criptográficos de bajo nivel para lograr uno o más de dichos objetivos de seguridad de la información. Estas herramientas incluyen algoritmos de cifrado, algoritmos de firma digital, algoritmos de hash y otras funciones.

Según *Amazon Web Services*:

La criptografía tiene sus raíces en el envío de información sensible entre militares y políticos. Los mensajes podían encriptarse para que parecieran texto aleatorio a cualquiera que no fuera el destinatario.

Hoy en día, las técnicas originales de encriptación no funcionan. Tanto es así que solo se encuentran en las secciones de enigmas de algunos periódicos. Afortunadamente, el campo ha hecho grandes avances en

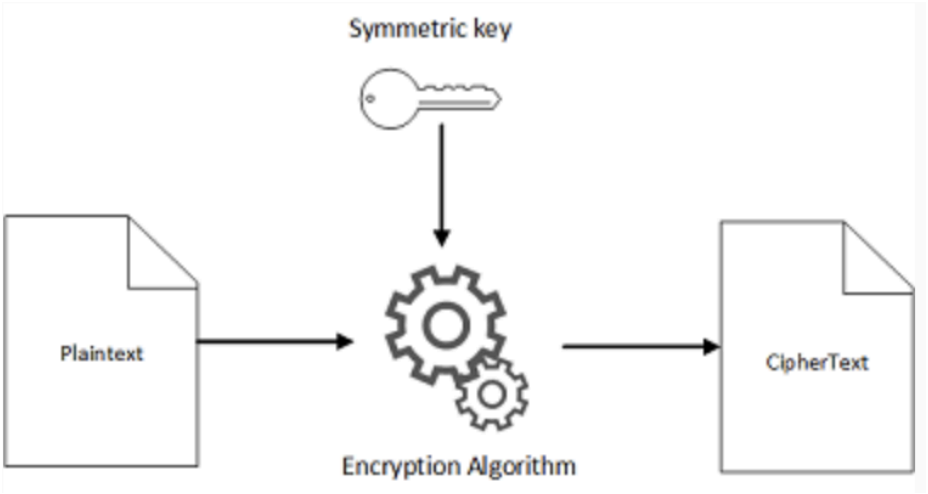
> materia de seguridad, y los algoritmos que se utilizan hoy en día se basan en un análisis riguroso y en las matemáticas para su seguridad.
>
> A medida que la seguridad avanza, el campo de la criptografía se amplía para incluir una gama más amplia de objetivos de seguridad. Entre ellos se encuentran la autenticación de mensajes, integridad de los datos, cálculo seguro, etc.
>
> La criptografía está en la base de la sociedad moderna. Es la base de innumerables aplicaciones de Internet a través del protocolo seguro de transferencia de hipertexto (HTTPS), de la comunicación segura de texto y voz, e incluso de las monedas digitales.

La criptografía se clasifica en dos categorías principales: criptografía de clave privada o simétrica y criptografía de clave pública o asimétrica. Siguiendo con las definiciones proporcionadas por *Amazon Web Services:*

> Los algoritmos criptográficos de clave simétrica utilizan las mismas claves criptográficas tanto para el cifrado del texto plano como para el descifrado del texto cifrado. El cifrado simétrico requiere que todos los destinatarios del mensaje tengan acceso a una clave compartida.

La siguiente ilustración muestra cómo funciona el cifrado y descifrado con claves y algoritmos simétricos, partiendo de la base de que todas las partes comparten la misma clave.

Se utiliza una clave simétrica y un algoritmo para convertir un mensaje de texto plano en texto cifrado.



(Figura 1: Claves simétricas. Fuente: *Amazon Web Services*)

Los cifrados por bloques más populares son el estándar de cifrado avanzado (AES). Este cifrado en bloque admite claves de 128, 192 o 256 bits. AES se combina a menudo con Galois/Counter Mode (GCM) y se conoce como AES-GCM para hacer un algoritmo de cifrado autenticado.

AES es el estándar del sector para el cifrado efectuado en todo el mundo. Su seguridad es muy conocida y existen despliegues eficientes de software y hardware.

La criptografía asimétrica (o de clave pública) consiste en un amplio conjunto de algoritmos. Estos se basan en problemas matemáticos que son relativamente fáciles de hacer en una dirección, pero que no se pueden invertir fácilmente.

Un ejemplo famoso de este tipo de problema es el de la factorización: para números primos cuidadosamente elegidos p y q, podemos calcular el producto N=p*q rápidamente. Sin embargo, si solo se da N, es muy difícil recuperar p y q.

Un algoritmo criptográfico de clave pública común basado en el problema de la factorización es la función Rivest-Shamir-Adleman (RSA). Si se combina con un esquema de relleno adecuado, RSA puede utilizarse para múltiples propósitos, incluido el cifrado asimétrico.

Un esquema de cifrado se denomina asimétrico si utiliza una clave (la clave pública) para cifrar los datos, y una clave diferente pero matemáticamente relacionada (la clave privada) para descifrarlos.

Determinar la clave privada debe ser inviable desde el punto de vista informático si lo único que se conoce es la clave pública. Por ello, la clave pública puede distribuirse ampliamente mientras que la clave privada se mantiene secreta y segura. El conjunto de las claves se denomina par de claves.

> Un esquema de cifrado asimétrico popular es RSA-OAEP, que es una combinación de la función RSA con el esquema de relleno Optimal Asymmetric Encryption Padding (OAEP). RSA-OAEP se suele utilizar solo para cifrar pequeñas cantidades de datos, ya que es un esquema lento y los textos cifrados son mucho más grandes que el texto plano.

Desde el punto de vista informático nos surgen los siguientes interrogantes: ¿Cómo se aplica la Criptografía al Desarrollo seguro del Software? ¿Cuáles son las ventajas y desventajas de la clave simétrica y asimétrica en el desarrollo de software? ¿Qué limitaciones tecnológicas nos encontramos a la hora de implementar las mismas?

Se establece como objetivo indagar el uso de la Criptografía en el Desarrollo Seguro de Software, analizando su aplicación, ventajas y desventajas de la Criptografía Simétrica y Asimétrica y limitaciones tecnológicas.

Los objetivos específicos comprenden:

- Recopilar información sobre el uso de la Criptografía en el Desarrollo de Software.
- Analizar los mecanismos tecnológicos de aplicación de la clave simétrica y asimétrica en el desarrollo de software, identificando sus principales ventajas y desventajas.
- Identificar y analizar las limitaciones tecnológicas que se presentan para la implementación de Criptografía en el Desarrollo de Software.

Métodos

Diseño

En la presente investigación se llevó a cabo un análisis de alcance descriptivo con el objetivo de examinar la literatura existente relacionada con el uso de la Criptografía en el Desarrollo de Software.

Se llevó a cabo una revisión selectiva del tema en estudio. La consulta se realizó en dos niveles: inicialmente, desde la perspectiva de la seguridad informática en general, y posteriormente, con un enfoque específico en la criptografía. Así, se recopilaron numerosos documentos tanto generales como específicos, lo que facilitó una mejor comprensión y contextualización del objeto de estudio particular: la criptografía en el contexto de la seguridad informática.

Participantes

La población objetivo de esta investigación se compone de libros académicos, artículos científicos, revistas especializadas, informes técnicos y sitios web confiables, relacionada con la aplicación de Criptografía en el Desarrollo de Software. Para abordar esta población, se realizó un muestreo no probabilístico intencional por conveniencia, en el que se revisaron varias fuentes documentales.

Se consideró no probabilístico dado que la elección de las fuentes documentales ha sido por causas relacionadas con las características de la investigación seleccionando la muestra según se consideró representativa para la misma (Grasso, 1999).

La muestra está compuesta por los siguientes documentos que fueron elegidos por su importancia dentro de la bibliografía más conocida respecto al ámbito de la Criptografía en el desarrollo de software:

- *Ferguson, Niels, Schneier, Bruce, & Kohno, Tadayoshi. (2014). Cryptography Engineering: Design Principles and Modern Applications (2da ed.). John Wiley & Sons.*
- *Maiorano, Ariel (2019). Criptografía. Técnicas de Desarrollo para Profesionales (2da ed.). Alfaomega Grupo Editor.*
- *Bruce Schneier. (1993). Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition.*

Instrumento

El instrumento de la presente investigación se basó en la recopilación y análisis de datos a partir de la lectura de fuentes y publicaciones literarias, con el fin de comprender y examinar el uso, la aplicación y las limitaciones de la implementación de la Criptografía en el Desarrollo de Software.

Según se detalla a continuación:

- Selección de material: implicó la recolección de fuentes que incluyen libros académicos, artículos científicos, revistas especializadas, informes técnicos y sitios web confiables. La elección de estas fuentes se basó en su pertinencia y utilidad para los objetivos de investigación.
- Revisión de la información: luego de la elección del material, se procedió a una revisión exhaustiva de la información contenida en cada fuente. Este

paso permitió identificar y descartar datos irrelevantes o duplicados para trabajar sobre los aspectos más significativos para la investigación.

- Organización de la información: la organización se basó en la relevancia de los datos y la temática abordada.

Análisis de datos

El análisis de datos se llevó a cabo mediante un enfoque de análisis de contenido, donde se examinaron las fuentes recopiladas para categorizar los datos relevantes con el fin de identificar temas, conceptos, términos clave y relaciones entre estos.

Este proceso se desarrolló a través de una serie de etapas:

- Síntesis y categorización: los hallazgos se sintetizaron y organizaron en categorías temáticas y conceptuales, lo que permitió comprender la información recopilada.
- Identificación de patrones y tendencias: se llevó a cabo una búsqueda para identificar patrones recurrentes o tendencias significativas presentes en las fuentes documentales analizadas.

Para analizar las problemáticas planteadas se establecieron las siguientes variables:

Aplicación: esta variable midió el uso de la Criptografía, teniendo en cuenta las siguientes características:

- Dispositivos: investigar los dispositivos tecnológicos que se emplean para el uso de Criptografía.

- Ventajas y desventajas: identificar cuáles son las ventajas y desventajas de las dos ramas dentro de la Criptografía.

Limitaciones: la variable hace referencia a los obstáculos, las restricciones y las limitaciones que pueden afectar en la aplicación de la Criptografía en el Desarrollo de Software.

- Aspectos técnicos: identificar las restricciones tecnológicas mencionadas en los textos, tales como limitaciones de *hardware*, *software* o conectividad que podrían influir en la eficacia e implementación de la Criptografía en el desarrollo de Software.
- Barreras de implementación: explorar los obstáculos que se plantean al implementar la Criptografía simétrica y asimétrica que incluyen posibles desafíos organizativos, financieros o de integración con sistemas existentes.

Resultados

A partir del instrumento diseñado y la documentación seleccionada, se derivaron los siguientes resultados que proporcionaron respuestas a los interrogantes planteados.

En cuanto a la variable de **aplicación** de la Criptografía en el Desarrollo de Software, se pudo distinguir el uso de los dispositivos de la siguiente forma según los autores:

Empezando con Maiorano (pp. 151-160) enfatiza la importancia fundamental de la confidencialidad en las comunicaciones digitales y destaca el uso de la criptografía para cifrar datos en tránsito, asegurando que solo los usuarios autorizados puedan acceder a la información. Menciona ejemplos como HTTPS y VPN. Además, profundiza en la implementación de algoritmos de cifrado simétrico y asimétrico, detallando cómo AES y RSA son utilizados para proteger datos sensibles. Discutió también sobre la gestión de claves y la importancia de un intercambio seguro de claves para mantener la confidencialidad. Él resalta la necesidad de verificar la identidad de los usuarios y entidades en los sistemas informáticos. Describe los principios básicos de la autenticación y menciona ejemplos de protocolos basados en claves compartidas, como PAP (Password Authentication Protocol) y CHAP (Challenge-Handshake Authentication Protocol), detallando su funcionamiento y sus limitaciones en términos de seguridad. También aborda el uso de certificados digitales y su papel en protocolos como SSL/TLS para establecer conexiones seguras y autenticadas en internet. Además, se discute la gestión y revocación de certificados, así como la infraestructura de clave pública (PKI) que sustenta estos mecanismos (pp. 240-255).

Continuando con Maiorano (pp. 169-176) subraya la importancia de proteger los datos almacenados en bases de datos de accesos no autorizados. Describe los diferentes métodos de cifrado de bases de datos, incluyendo cifrado de disco completo, cifrado de tablas y cifrado de columnas. Detalla cómo el cifrado de columnas permite una protección más granular de datos sensibles, permitiendo cifrar sólo la información crítica sin afectar el rendimiento global de la base de datos. También se mencionan las técnicas de gestión de claves, esenciales para la seguridad del cifrado de bases de datos, y la importancia de utilizar hardware seguro (HSM) para el almacenamiento y gestión de claves criptográficas.

Ferguson et al. (pp. 224-239) explican los principios de diseño de sistemas criptográficos seguros, abarcando temas como la resistencia a ataques criptográficos y la importancia de un diseño robusto. Se centran en técnicas avanzadas, como el uso de cifrados de flujo y bloque, y la implementación de protocolos seguros que previenen vulnerabilidades comunes. También destacan la importancia de las buenas prácticas de ingeniería en criptografía, como la validación de entradas y la actualización regular de algoritmos para contrarrestar nuevos tipos de amenazas.

Además, mencionan el papel de las auditorías de seguridad y las pruebas de penetración en la evaluación continua de la eficacia de las soluciones criptográficas implementadas. Los autores analizan en profundidad los diferentes mecanismos de autenticación, incluyendo contraseñas, tokens de seguridad y biometría. Discuten las ventajas y desventajas de cada método y las consideraciones de seguridad en su implementación. Enfatizan la importancia de la autenticación multifactor (MFA) como una medida adicional de seguridad para proteger contra el acceso no autorizado.

Explican cómo la combinación de varios factores, como algo que el usuario sabe (contraseña), algo que el usuario tiene (token de seguridad), y algo que el usuario es (biometría), puede fortalecer significativamente la seguridad de los sistemas (pp. 240-255).

En la misma línea, Ferguson et al. (pp. 256-271) consideran en profundidad los diferentes métodos de cifrado de bases de datos, incluyendo cifrado de disco completo, cifrado de tablas y cifrado de columnas. Discuten las ventajas y desventajas de cada método y las consideraciones de rendimiento y seguridad en su implementación. Además, analizan cómo el cifrado de bases de datos puede integrarse con otras medidas de seguridad, como el control de acceso basado en roles (RBAC) y la auditoría de acceso a datos. También explican las implicaciones de la encriptación en el rendimiento de las consultas y transacciones, destacando la importancia de optimizar las bases de datos para mantener un equilibrio entre seguridad y eficiencia operativa.

Según Schneier brinda una perspectiva práctica sobre la implementación de cifrado de comunicaciones en redes y aplicaciones web. Destaca la importancia de elegir algoritmos y protocolos adecuados, así como de configurar correctamente las herramientas de cifrado para garantizar la seguridad de las comunicaciones (pp. 224-239). A su vez, profundiza en los aspectos técnicos de la implementación del cifrado, proporcionando orientación sobre cómo configurar correctamente las herramientas y bibliotecas de cifrado disponibles para garantizar la seguridad de las comunicaciones. Esto incluye consideraciones sobre la longitud y la fortaleza de las claves criptográficas, así como la gestión segura de claves para evitar posibles vulnerabilidades.

El autor se enfoca en la autenticación en entornos web y aplicaciones distribuidas. Describe protocolos como SAML y OAuth y discute los desafíos de la gestión de identidades y acceso en sistemas complejos (pp. 559-577). Schneier aborda la importancia crucial de establecer mecanismos confiables de autenticación para verificar la identidad de los usuarios y garantizar la seguridad de los sistemas en línea. Describe en profundidad protocolos ampliamente utilizados como SAML (Security Assertion Markup Language) y OAuth, que desempeñan un papel fundamental en la gestión de identidades y el acceso en entornos distribuidos. Schneier explora cómo estos protocolos permiten a los usuarios autenticarse de manera segura en diversos servicios y aplicaciones sin necesidad de compartir sus credenciales de inicio de sesión en cada interacción. Además, discute las ventajas y limitaciones de cada protocolo, así como las consideraciones de seguridad asociadas con su implementación.

También se consideraron las ventajas y desventajas de la Criptografía Simétrica y Asimétrica según los autores:

Criptografía Simétrica:

Ventajas:

Maiorano destaca la rapidez de los algoritmos simétricos para cifrar y descifrar grandes cantidades de datos, haciéndolos ideales para aplicaciones con alto volumen de información (pp. 102-115). Además, enfatiza la facilidad de implementación y comprensión de los algoritmos simétricos, lo que los hace accesibles para desarrolladores con diversos niveles de experiencia en criptografía (pp. 116-122). A su vez, menciona el bajo consumo de recursos computacionales de los algoritmos simétricos, haciéndolos adecuados para dispositivos con recursos limitados, como

dispositivos móviles o embebidos (pp. 123-128). El autor también discute ejemplos específicos de algoritmos simétricos ampliamente utilizados, como AES y DES, detallando sus características y casos de uso prácticos. Además, menciona la importancia de la gestión segura de claves para mantener la integridad y la confidencialidad de los datos cifrados.

Ferguson et al. (pp. 162-175) se enfocan en la eficiencia de la criptografía simétrica, mencionando que su rendimiento computacional es superior al de la criptografía asimétrica, especialmente en escenarios que requieren cifrar y descifrar grandes volúmenes de datos. También resaltan la simplicidad conceptual de la criptografía simétrica en comparación con la asimétrica, lo que facilita su integración en sistemas y aplicaciones (pp. 176-191). Además, Ferguson et al. discuten la implementación de algoritmos simétricos en diferentes contextos, incluyendo su uso en cifrados de flujo y de bloque, y la importancia de seleccionar modos de operación seguros, como CBC y GCM, para mitigar posibles vulnerabilidades. Luego destacan la relevancia de la criptografía simétrica en la construcción de protocolos seguros y en la protección de la información en tránsito y en reposo.

Schneier añade que la velocidad de los algoritmos simétricos los hace particularmente adecuados para aplicaciones en tiempo real, donde la latencia es un factor crítico (pp. 289-302). Luego señala que el bajo consumo de recursos de los algoritmos simétricos los hace particularmente adecuados para aplicaciones que funcionan en entornos con baterías limitadas, como dispositivos móviles o sensores inalámbricos (pp. 521-534). En su bibliografía explica que la integración de

mecanismos de autenticación en la criptografía simétrica requiere un análisis cuidadoso de los requisitos de seguridad y la usabilidad del sistema (pp. 535-542).

Desventajas:

Ferguson et al. explican el desafío que presenta la distribución segura de claves en la criptografía simétrica, mencionando que la complejidad aumenta en entornos con muchos participantes y canales de comunicación diversos (pp. 162-175). Comentan que otra desventaja es la susceptibilidad de la criptografía simétrica a ataques de fuerza bruta, especialmente con claves cortas o cuando la potencia de cómputo del atacante es superior a la del defensor (pp. 192-207). Además, Ferguson et al. discuten estrategias para mitigar estos riesgos, como el uso de protocolos de intercambio de claves asimétricas para establecer una clave de sesión segura antes de iniciar la comunicación con criptografía simétrica. También resaltan la importancia de utilizar claves largas y robustas, así como algoritmos resistentes a ataques de fuerza bruta, como AES con longitudes de clave de 128 bits o superiores.

Mariorano enfatiza la dificultad de compartir de forma segura una clave secreta entre las partes que se comunican, especialmente en entornos distribuidos donde la confianza entre las partes no es inmediata (pp. 129-134). Destaca la vulnerabilidad de la criptografía simétrica a ataques de fuerza bruta, donde un atacante intenta descifrar la clave probando todas las combinaciones posibles (pp. 135-144). Además, discute sobre técnicas específicas para el intercambio seguro de claves, como el uso de protocolos de establecimiento de claves basados en autenticación mutua, donde las partes intercambian información para verificar su identidad antes de compartir la clave secreta. También menciona la importancia de la gestión de claves a largo plazo, incluyendo la

renovación periódica de claves y la revocación de claves comprometidas para mantener la seguridad de la comunicación cifrada.

Schneier comenta que la distribución segura de claves requiere mecanismos robustos de autenticación y gestión de claves, lo que puede incrementar la complejidad y el costo de implementación (pp. 578-584). Por otro lado, señala que la longitud de la clave es un factor determinante en la resistencia a ataques de fuerza bruta en la criptografía simétrica. Cuanto más larga sea la clave, mayor será el tiempo y la potencia de cómputo necesarios para descifrarla. Sin embargo, claves más largas también pueden impactar el rendimiento y la complejidad de la implementación (pp. 303-318).

Criptografía Asimétrica:

Ventajas:

Ferguson et al. destacan que las claves asimétricas se pueden compartir públicamente, mientras que las claves privadas permanecen secretas. Esto simplifica la distribución de claves en entornos distribuidos, eliminando la necesidad de canales de comunicación seguros para el intercambio de claves simétricas (pp. 176-191).

Maiorano menciona que la criptografía asimétrica permite la autenticación de la identidad de las partes que se comunican mediante firmas digitales. Estas firmas permiten verificar que un mensaje ha sido enviado por un remitente específico y que no ha sido alterado durante la transmisión (pp. 145-155).

Schneier enfatiza la robustez de la criptografía asimétrica frente a ataques de fuerza bruta, destacando la diferencia fundamental en la longitud de las claves en comparación con la criptografía simétrica (pp. 303-318). Las claves asimétricas, utilizadas en algoritmos como RSA o ECC, suelen ser significativamente más largas

que las claves simétricas utilizadas en algoritmos como AES o DES. Esta longitud adicional de las claves asimétricas hace que sea computacionalmente inviable para un atacante descifrarlas mediante ataques de fuerza bruta en un tiempo razonable.

Desventajas:

Maiorano indica que los algoritmos asimétricos son generalmente más lentos que los simétricos, lo que los hace menos adecuados para cifrar y descifrar grandes cantidades de datos. Esto se debe a la complejidad de las operaciones matemáticas involucradas en la criptografía asimétrica (pp. 135-144). También menciona que los algoritmos asimétricos consumen más recursos computacionales que los simétricos, lo que los hace menos adecuados para dispositivos con recursos limitados. Esto se debe a la mayor complejidad de las operaciones matemáticas involucradas (pp. 156-161).

Ferguson et al. señalan que los algoritmos asimétricos son más complejos que los simétricos, lo que los hace más difíciles de implementar y comprender. Esta complejidad puede generar desafíos en la integración de la criptografía asimétrica en sistemas y aplicaciones (pp. 192-207).

Con relación a las **limitaciones,** se exploraron las restricciones tecnológicas y las barreras que presenta la Criptografía en el Desarrollo de Software, según las documentaciones seleccionadas.

Maiorano destaca la complejidad de la implementación de algoritmos criptográficos, especialmente para desarrolladores sin experiencia en el área, subrayando los desafíos técnicos y de seguridad que pueden surgir durante este proceso

(pp. 56-62). Además, enfatiza la importancia de contar con personal capacitado en criptografía para garantizar la correcta implementación y uso de estas técnicas.

Aborda también la necesidad de realizar pruebas exhaustivas y auditorías de seguridad durante el proceso de implementación para identificar posibles vulnerabilidades y asegurar la robustez del sistema criptográfico. Explica que la gestión segura de claves criptográficas, incluyendo su generación, almacenamiento, distribución y destrucción, es un desafío complejo (pp. 231-244). Maiorano señala que el uso de la criptografía puede generar preocupaciones sobre la privacidad, especialmente si se utiliza para cifrar datos personales o comunicaciones (pp. 312-327).

Ferguson et al. abordan la falta de estandarización en algunos aspectos de la criptografía, lo que dificulta la interoperabilidad entre diferentes sistemas y plataformas (pp. 104-112). Resaltan que esta falta de estandarización puede llevar a problemas de compatibilidad y dificultades en la comunicación segura entre sistemas heterogéneos. Además, destacan la necesidad de estándares y protocolos abiertos en criptografía para facilitar la adopción y el uso generalizado de estas técnicas de seguridad en diferentes aplicaciones y entornos.

Argumentan que los estándares abiertos promueven la transparencia, la colaboración y la innovación en el campo de la criptografía, permitiendo el desarrollo de soluciones interoperables y seguras que benefician a la comunidad en su conjunto. Resaltan que la implementación de la criptografía puede afectar la usabilidad de las aplicaciones, especialmente si se requiere que los usuarios interactúen con claves o certificados (pp. 362-377). Ferguson et al. sostienen que la exportación de tecnología

criptográfica puede estar sujeta a restricciones legales y regulaciones gubernamentales (pp. 556-561).

Schneier examina críticamente la falta de estandarización en ciertos aspectos de la criptografía, lo que presenta desafíos significativos para la interoperabilidad entre diferentes sistemas y plataformas (pp. 104-112). La falta de estándares comunes puede dificultar la comunicación segura entre dispositivos y aplicaciones, ya que cada uno puede implementar sus propios protocolos y algoritmos, lo que dificulta la compatibilidad y la coherencia en el intercambio de datos cifrados. También subraya la importancia de establecer estándares y protocolos abiertos en el campo de la criptografía para facilitar la adopción y el uso generalizado de estas técnicas de seguridad (pp. 104-112).

Los estándares abiertos promueven la transparencia, la interoperabilidad y la innovación al permitir que diferentes sistemas y aplicaciones se comuniquen de manera segura utilizando protocolos comunes y ampliamente aceptados. Schneier implica que la implementación y mantenimiento de soluciones criptográficas robustas puede ser costoso, especialmente para organizaciones con recursos limitados (pp. 578-584). Schneier indica que la criptografía puede dificultar el acceso a la evidencia digital en investigaciones criminales o legales (pp. 642-657).

Discusión

La presente investigación tuvo como objetivo general explorar el uso de la Criptografía en el Desarrollo Seguro de Software. El mismo se logró al identificar y describir diversos dispositivos y tecnologías empleados en la práctica, así como sus usos en campo de la tecnología definiendo sus aplicaciones, ventajas, desventajas y las limitaciones que hay en sus implementaciones. Se destaca que los resultados obtenidos proporcionaron respuesta a los interrogantes planteados según se detalla a continuación.

En relación con los objetivos específicos abordados, se identificaron los mecanismos tecnológicos de aplicación y las limitaciones que presenta su implementación.

Cuando se estudió la variable aplicación**,** los hallazgos obtenidos permitieron identificar y describir diferentes técnicas de cifrado, tales como el cifrado de comunicaciones en redes y aplicaciones web, mecanismos de autenticación, certificados digitales y cifrado de bases de datos. Los mismos permiten garantizar la seguridad de las comunicaciones, que solo usuarios autorizados puedan acceder a la información y protección de los datos almacenados en la base de datos. Además, se destacan las principales ventajas y desventajas de las Claves Simétricas y Claves Asimétricas. Para profundizar en este tema, es útil explorar los pensamientos y teorías de diferentes autores en el campo de la criptografía.

Respecto al antecedente de Amazon Web Service, en el que introduce varios ejemplos de aplicación como autenticación de mensajes, integridad de datos, cálculos seguros, entre otros, se encuentra concordancia con los siguientes autores:

Maiorano enfatiza la importancia fundamental de la confidencialidad en las comunicaciones digitales, destacando el uso de criptografía para cifrar datos en tránsito y en reposo. En sus escritos, aborda ejemplos concretos como HTTPS y VPN para proteger las comunicaciones en línea, así como el cifrado de bases de datos mediante técnicas como el cifrado de disco completo, tablas y columnas. Este autor profundiza en la implementación de algoritmos de cifrado simétrico (AES) y asimétrico (RSA), explicando cómo se utilizan para proteger datos sensibles.

Además, Maiorano discute la gestión de claves criptográficas y la necesidad de un intercambio seguro de claves para mantener la confidencialidad. En términos de autenticación, describe los principios básicos y menciona protocolos basados en claves compartidas como PAP y CHAP, además del uso de certificados digitales en protocolos SSL/TLS para conexiones seguras.

Por otro lado, Ferguson et al. abordan el diseño de sistemas criptográficos seguros, centrándose en la resistencia a ataques criptográficos y la robustez del diseño. Estos autores destacan el uso de cifrados de flujo y bloque, y subrayan la importancia de buenas prácticas de ingeniería en criptografía, como la validación de entradas y la actualización regular de algoritmos para contrarrestar nuevas amenazas. A diferencia de Maiorano, Ferguson et al. también discuten en profundidad los métodos de autenticación, incluyendo contraseñas, tokens de seguridad y biometría, y promueven la autenticación multifactor (MFA) como una medida adicional de seguridad. Además, estos autores analizan los métodos de cifrado de bases de datos, considerando sus ventajas y desventajas, así como las implicaciones de rendimiento y seguridad. Resaltan la integración del cifrado de bases de datos con otras medidas de seguridad como el control de acceso basado en roles (RBAC) y la auditoría de acceso a datos.

En contraste con las perspectivas de Maiorano y Ferguson et al., Schneier ofrece una visión práctica sobre la implementación de cifrado en redes y aplicaciones web. Destaca la importancia de elegir algoritmos y protocolos adecuados y de configurar correctamente las herramientas de cifrado para garantizar la seguridad de las comunicaciones. Este autor profundiza en los aspectos técnicos de la implementación del cifrado, proporcionando orientación sobre la configuración de herramientas y bibliotecas de cifrado, y enfatizando la gestión segura de claves para evitar posibles vulnerabilidades. Además, Schneier se enfoca en la autenticación en entornos web y aplicaciones distribuidas, describiendo protocolos como SAML y OAuth, y discutiendo los desafíos de la gestión de identidades y acceso en sistemas complejos. Schneier explora cómo estos protocolos permiten la autenticación segura sin necesidad de compartir credenciales de inicio de sesión en cada interacción y aborda las ventajas y limitaciones de cada protocolo.

A pesar de las diferencias en sus enfoques y profundidades, todos los autores coinciden en la importancia de la confidencialidad y el cifrado, la gestión de claves criptográficas y la autenticación de usuarios para la seguridad de los sistemas informáticos.

Maiorano proporciona ejemplos concretos y aplicaciones prácticas, mientras que Ferguson et al. Se enfocan en el diseño robusto y las mejores prácticas de ingeniería. Schneier, por su parte, ofrece una guía práctica y técnica para la implementación de cifrado y autenticación en entornos web, subrayando la necesidad de configuraciones adecuadas y seguras. Esta convergencia y divergencia en sus perspectivas enriquecen el

entendimiento global de la criptografía y la seguridad informática, proporcionando una visión amplia y detallada de las múltiples facetas de la protección de datos y sistemas.

La criptografía simétrica y asimétrica representan dos enfoques distintos en la protección de datos, cada uno con sus ventajas y desventajas. En el ámbito de la criptografía simétrica, Maiorano enfatiza su capacidad para cifrar y descifrar grandes volúmenes de datos de forma rápida y eficiente, convirtiéndola en una opción ideal para aplicaciones con alta demanda de procesamiento de información. Además, resalta su facilidad de implementación y bajo consumo de recursos computacionales, lo que la hace accesible incluso para desarrolladores menos experimentados en el campo de la criptografía.

Por otro lado, Ferguson et al. subrayan la eficiencia computacional de la criptografía simétrica, especialmente en comparación con la asimétrica, siendo preferible en escenarios que requieren el cifrado y descifrado de grandes volúmenes de datos. También hacen hincapié en su simplicidad conceptual y su fácil integración en sistemas y aplicaciones. Sin embargo, reconocen desafíos en la distribución segura de claves y la vulnerabilidad a ataques de fuerza bruta, proponiendo estrategias como el uso de protocolos de intercambio de claves asimétricas para mitigar estos riesgos.

Schneier, por su parte, complementa estas perspectivas al destacar la idoneidad de la criptografía simétrica para aplicaciones en tiempo real y entornos con recursos limitados. Además, enfatiza la importancia de una gestión segura de claves y la integración de mecanismos de autenticación para garantizar la seguridad de la comunicación cifrada.

En contraste, la criptografía asimétrica presenta sus propias fortalezas y debilidades. Ferguson et al. y Maiorano coinciden en que la distribución de claves es más sencilla, ya que las claves públicas pueden compartirse abiertamente, eliminando la necesidad de canales seguros. También resaltan su robustez frente a ataques de fuerza bruta debido a la mayor longitud de las claves utilizadas en algoritmos como RSA y ECC.

Sin embargo, Maiorano señala que los algoritmos asimétricos son generalmente más lentos y consumen más recursos computacionales que los simétricos, debido a la complejidad de las operaciones matemáticas involucradas. Ferguson et al. profundizan en la dificultad de implementación y comprensión de la criptografía asimétrica, lo que puede representar un desafío en la integración con sistemas y aplicaciones.

Con respecto al análisis de las **limitaciones** que puede presentar en la implementación de la Criptografía en el Desarrollo de software, los resultados de esta investigación concuerdan con los antecedentes y los amplían.

Maiorano enfatiza la complejidad técnica y los desafíos de seguridad inherentes a la implementación de algoritmos criptográficos, destacando la importancia de contar con personal capacitado y realizar pruebas exhaustivas para garantizar la robustez del sistema. Esta preocupación por la seguridad y la competencia técnica también es compartida por Ferguson et al., quienes resaltan la necesidad de estándares abiertos para promover la interoperabilidad y la innovación en el campo de la criptografía.

Sin embargo, Ferguson et al. amplían su enfoque hacia la falta de estandarización y sus implicaciones en la interoperabilidad entre sistemas y plataformas,

mientras que Schneier se suma a esta preocupación, pero agrega un aspecto económico: el costo asociado con la implementación y mantenimiento de soluciones criptográficas. Esta perspectiva económica resalta cómo la criptografía puede no solo ser técnica y operativamente desafiante, sino también financieramente demandante, especialmente para organizaciones con recursos limitados.

Por otro lado, Schneier introduce una dimensión adicional al debate al señalar cómo la criptografía puede complicar el acceso a la evidencia digital en investigaciones criminales o legales. Esta preocupación por los aspectos legales y forenses de la criptografía añade una capa de complejidad al argumento, evidenciando que sus implicaciones van más allá del ámbito técnico y financiero.

Se considera que la investigación encuentra correlación con los antecedentes y los hallazgos obtenidos, dado que han destacado las aplicaciones de la Criptografía en el Desarrollo de Software, como sus ventajas y desventajas a la hora de implementar y también las limitaciones que surgen.

Cabe destacar que el método de selección de las fuentes documentales presenta, por un lado, limitaciones al basarse en un muestreo no probabilístico intencional y por conveniencia, lo que puede introducir un sesgo en la recopilación de datos al no garantizar la representatividad de todas las perspectivas relevantes en el campo de estudio. Por otro lado, se pueden distinguir fortalezas debido a que la documentación corresponde a libros de autores reconocidos en el ámbito de la criptografía, lo que supone ser fuentes confiables y respaldadas por investigaciones formales, rigurosas y verificadas, en cuanto implican un proceso de revisión por pares y rigurosidad de la metodología científica utilizada. Así como también, se ha dado prioridad a la utilización

de los documentos más actualizados de cada tema para garantizar que la investigación esté basada en la información más reciente y relevante en el campo de estudio.

Por lo expuesto se concluye que los objetivos de la investigación fueron alcanzados en su totalidad. Se destaca que la Criptografía en el Desarrollo de Software es de vital importancia ya que nos permite tener conexiones seguras y protección a datos sensibles, al ofrecer aplicaciones innovadoras y beneficios significativos. Se recomienda continuar investigando sobre tecnologías que aborden y contribuyan a mejorar las limitaciones identificadas, como la precisión de la superposición y la latencia en la visualización.

A nivel profesional, esta investigación ha proporcionado una comprensión más detallada de la Criptografía en el Desarrollo de Software y cómo se aplican estas misma para que nuestras aplicaciones, comunicaciones y programas sean seguros.

Como estudiante de la carrera de Ingeniería en Software, este trabajo ha sido una oportunidad para explorar y aprender sobre un campo disciplinar no abordado anteriormente.

Referencias

- Amazon Web Services. (n.d.). What is cryptography?. https://aws.amazon.com/es/what-is/cryptography/
- Ferguson, N., Schneier, B., & Kohno, T. (2014). Cryptography engineering: Design principles and modern applications (2nd ed.). John Wiley & Sons.
- Lessig, L. (1999). Code and other laws of cyberspace. Basic Books.
- Maiorano, A. (2019). Criptografía. Técnicas de desarrollo para profesionales (2nd ed.). Alfaomega Grupo Editor.
- Marrero Travieso, Yran. (2003). La Criptografía como elemento de la seguridad informática. ACIMED, 11(6) Recuperado en 29 de junio de 2024, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012&lng=es&tlng=es.
- Miller, M. (2013). Applied cryptography: Protocols, algorithms, and source code in Python (2nd ed.). Peachpit Press.