Universidad Nacional Autónoma de México

Facultad de Ingeniería

Semestre 2025-1

Sistemas Operativos

El papel de la criptografía en la protección de la información

Alumno: Gabriela Aquino Lozada

Fecha de entrega:
19/Noviembre/2024

Introducción

Breve Historia de la Criptografía

La criptografía tiene una historia fascinante que se extiende desde la antigüedad hasta la era digital actual. A lo largo de los siglos, la humanidad ha desarrollado métodos para proteger información sensible de forma que solo los destinatarios legítimos puedan entender el mensaje. Las primeras técnicas criptográficas aparecieron en el Antiguo Egipto alrededor del año 1900 a.C., donde se utilizaban jeroglíficos alterados para ocultar mensajes secretos en tumbas y monumentos.

En Grecia y Roma, el uso de la criptografía fue avanzando. Los espartanos empleaban la escítala, una herramienta de cifrado mediante transposición, que consistía en enrollar una tira de cuero alrededor de una vara de un diámetro específico para formar el mensaje oculto. Durante la época romana, el cifrado César (un tipo de cifrado por sustitución) se popularizó. Julio César utilizaba esta técnica para desplazar las letras del alfabeto en sus mensajes secretos, de modo que solo aquellos que conocían el desplazamiento podían descifrarlos.

Durante la Edad Media y el Renacimiento, el cifrado comenzó a hacerse más complejo con la incorporación de métodos basados en polialfabetismo, como el cifrado de Vigenère, que utilizaba varias letras de desplazamiento en un solo mensaje. Este método fue un avance importante, ya que evitaba los patrones repetitivos de los cifrados simples, complicando el trabajo de los criptoanalistas.

La Segunda Guerra Mundial marcó un hito crucial en la historia de la criptografía. La máquina Enigma, desarrollada y utilizada por el ejército nazi, se convirtió en una de las herramientas de cifrado más complejas de su época. Sin embargo, el trabajo de matemáticos y criptoanalistas, como el británico Alan Turing, permitió descifrar el código Enigma, acelerando el fin de la guerra y revolucionando el campo de la criptografía.

Con la llegada de la informática y la teoría de números, la criptografía ingresó a una nueva era. En la década de 1970, se desarrollaron los primeros sistemas de criptografía de clave pública (o criptografía asimétrica), como el sistema RSA, que permitieron realizar transmisiones seguras sin necesidad de compartir una clave común. Estos avances llevaron a la creación de estándares como el Data Encryption Standard (DES) y, más tarde, el Advanced Encryption Standard (AES), que sentaron las bases para la seguridad informática moderna.

Nociones Generales y Características de Criptosistemas

Un criptosistema es un conjunto estructurado de elementos y procedimientos criptográficos diseñados para proteger la información. Un criptosistema generalmente está compuesto por un algoritmo de cifrado y un algoritmo de descifrado, además de una o varias claves criptográficas. Su principal objetivo es mantener la seguridad de la comunicación entre dos o más partes, impidiendo que terceros no autorizados puedan leer, modificar o falsificar los datos.

Principales características de los criptosistemas:

1. **Confidencialidad:** Solo las personas autorizadas pueden acceder y entender la información cifrada. Esto se logra mediante el uso de algoritmos que convierten los datos en un formato ilegible, conocido como “texto cifrado”.

2. **Integridad:** Asegura que el mensaje no ha sido alterado durante su transmisión. Utiliza funciones hash y técnicas de verificación para detectar cualquier cambio en los datos.

3. **Autenticación:** Permite verificar la identidad del emisor y del receptor del mensaje. Esto asegura que ambas partes sean quienes dicen ser, evitando ataques de suplantación de identidad.

4. **No repudio:** Es una garantía de que el remitente de un mensaje no pueda negar haberlo enviado. Esta propiedad es fundamental en aplicaciones legales o transacciones, ya que proporciona evidencia de autenticidad.

Los criptosistemas actuales están diseñados para brindar todos estos atributos, utilizando una combinación de algoritmos matemáticos y claves criptográficas que varían en longitud y complejidad según el nivel de seguridad deseado.

Seguridad y Criptografía

a) **Seguridad:** La seguridad en un contexto amplio se refiere a la implementación de barreras y medidas de control para proteger activos físicos, información o recursos digitales contra posibles amenazas o ataques. En el campo de la criptografía, la seguridad involucra tanto la protección de los datos en tránsito (a través de canales de comunicación) como la protección de los datos en reposo (almacenados). Los sistemas seguros deben ser capaces de detectar, prevenir y mitigar posibles ataques, manteniendo la integridad de la información.

b) **Seguridad de la Información:** La seguridad de la información es una disciplina que se centra en proteger los datos y la información dentro de una organización o sistema. Abarca principios como la confidencialidad (para limitar el acceso solo a los usuarios autorizados), la integridad (para evitar modificaciones no autorizadas) y la disponibilidad (asegurando que la información esté accesible cuando se necesite). Esta seguridad se logra mediante controles de acceso, políticas de cifrado, y prácticas de auditoría y monitoreo.

c) **Seguridad Informática:** Es una subcategoría de la seguridad de la información enfocada en la protección de sistemas, redes y dispositivos de procesamiento de datos. La seguridad informática incluye el uso de antivirus, cortafuegos, cifrado de datos y otros mecanismos para evitar que los sistemas sean vulnerados por software malicioso o usuarios no

autorizados. La criptografía es una de las herramientas esenciales dentro de la seguridad informática, ya que permite cifrar los datos y proteger la integridad de las comunicaciones en entornos digitales.

Criptografía

La criptografía es la ciencia y técnica de transformar la información para ocultar su contenido. Su propósito principal es proteger los datos de accesos no autorizados y garantizar que solo los usuarios legítimos puedan acceder a la información cifrada. La criptografía moderna abarca métodos avanzados que se basan en algoritmos matemáticos y teorías de complejidad computacional.

En un sistema criptográfico, los datos originales (o texto plano) se transforman en un texto cifrado mediante un algoritmo y una clave. Para recuperar los datos originales, el receptor usa un proceso de descifrado aplicando la clave correspondiente. Esta clave puede ser la misma (como en los sistemas simétricos) o diferente (como en los sistemas asimétricos).

Clasificación de la Criptografía

La criptografía se divide en varias categorías, que se pueden clasificar de acuerdo con el tipo de clave y la complejidad del algoritmo utilizado: Criptografía Clásica: Se basa en métodos de sustitución y transposición. Sustitución: Cada letra o símbolo del texto plano es reemplazado por otro símbolo. Un ejemplo es el cifrado César, en el que cada letra es desplazada por un número fijo.

- **Transposición:** Los caracteres del mensaje se reordenan de acuerdo con un patrón preestablecido, lo que da como resultado un texto cifrado en el que la disposición de los caracteres ha cambiado.

- **Criptografía Moderna:** Utiliza algoritmos más avanzados y claves de mayor longitud, y se subdivide en:

    - **Criptografía Simétrica:** En este caso, el mismo conjunto de claves se usa tanto para cifrar como para descifrar los mensajes. Algunos algoritmos simétricos populares incluyen DES (Data Encryption Standard) y AES (Advanced Encryption Standard).

    - **Criptografía Asimétrica:** Utiliza pares de claves: una pública (para cifrar) y otra privada (para descifrar). Ejemplos de este tipo de criptografía son los algoritmos RSA y ECC (Elliptic Curve Cryptography).

Criptografía Clásica

La criptografía clásica abarca los métodos de cifrado y descifrado utilizados desde la antigüedad hasta el advenimiento de la criptografía moderna en el siglo XX. Estos métodos se basan principalmente en técnicas de sustitución y transposición, en las cuales el texto original o texto plano se transforma en texto cifrado aplicando una serie de reglas fijas que pueden realizarse a mano o con herramientas sencillas. A lo largo de la historia, diferentes civilizaciones han desarrollado métodos de criptografía clásica para proteger sus comunicaciones, especialmente en contextos militares, diplomáticos y religiosos.

Cifrado por Sustitución

El cifrado por sustitución implica reemplazar cada letra o símbolo del texto plano con otro carácter según una regla específica. Esto puede incluir un cambio en la posición de las letras, el uso de un alfabeto diferente o la aplicación de un desplazamiento fijo. Existen varios métodos de sustitución, algunos de los cuales se explican a continuación.

- Cifrado César: Este es uno de los métodos de sustitución más antiguos y fue utilizado por Julio César para comunicar mensajes secretos. En el cifrado César, cada letra del alfabeto se desplaza un número fijo de posiciones. Por ejemplo, si se utiliza un desplazamiento de 3, la letra “A” se convierte en “D”, “B” en “E”, y así sucesivamente. Este método es fácil de implementar y descifrar, lo cual es una de sus debilidades, ya que un atacante que conozca el uso de este cifrado solo necesita probar un pequeño número de desplazamientos para recuperar el mensaje original.

- Cifrado Monoalfabético: En este tipo de cifrado, cada letra del texto plano se reemplaza por otra letra según un alfabeto de sustitución fijo. A diferencia del cifrado César, el cifrado monoalfabético no utiliza un desplazamiento uniforme; en su lugar, cada letra del alfabeto se empareja con otra de forma fija. Sin embargo, esta técnica es vulnerable al análisis de frecuencia, un método de criptoanálisis que utiliza las frecuencias con las que aparecen las letras en un idioma para deducir el contenido del mensaje cifrado. Las letras más comunes, como “E” en inglés o “A” en español, tienden a aparecer con mayor frecuencia en el texto cifrado, lo cual facilita el descifrado sin la clave original.

- Cifrado de Vigenère: Este método, inventado en el siglo XVI, fue un avance importante en la criptografía clásica. El cifrado de Vigenère utiliza una clave de texto repetitiva para cifrar el mensaje. Cada letra del mensaje se desplaza según el valor de una letra correspondiente en la clave, lo que da como resultado un cifrado polialfabético. Este cifrado se considera más seguro que los anteriores debido a su resistencia al análisis de frecuencia, aunque es vulnerable a ataques que analicen la longitud de la clave y los patrones en el texto cifrado. El cifrado de

Vigenère se mantuvo como uno de los métodos más seguros hasta que fue descifrado en el siglo XIX por el matemático Charles Babbage.

- Cifrado de Sustitución Homofónica: Para reducir la vulnerabilidad al análisis de frecuencia, algunos métodos de sustitución homofónica asocian múltiples símbolos con las letras más comunes. Por ejemplo, en vez de reemplazar cada letra con una sola, se asignan varios caracteres a una sola letra de modo que las letras más comunes tengan varias representaciones, haciendo el análisis de frecuencia mucho más complicado.

Cifrado por Transposición

El cifrado por transposición no altera las letras o caracteres en el mensaje original; en su lugar, cambia el orden en el que aparecen. Esto genera un texto cifrado en el cual el orden de los caracteres ha sido modificado, lo que dificulta su lectura sin la clave para reorganizar las letras en su orden correcto.

- La Escítala: Este método, utilizado por los espartanos en la Antigua Grecia, consiste en un cilindro o bastón alrededor del cual se enrolla una tira de cuero. El mensaje se escribe a lo largo de la vara y, al desenrollar la tira, el texto se vuelve ilegible a menos que se vuelva a enrollar en una vara del mismo diámetro. Este es un ejemplo de cifrado de transposición, en el que el orden de las letras se reestructura según el diámetro del cilindro utilizado. Esta técnica ofrecía una seguridad relativamente simple y era fácil de utilizar en el campo de batalla.

- Cifrado de Columnas: En este tipo de cifrado, el texto plano se escribe en filas de una tabla y luego se lee columna por columna siguiendo un orden preestablecido. Este orden puede seguir una secuencia numérica determinada por una clave, lo que hace que el mensaje solo sea legible para aquellos que conocen el patrón de lectura. Este método era común en tiempos de guerra, y su simplicidad lo hacía adecuado para ser utilizado con papel y lápiz.

- Cifrado de Ruta: Este método consiste en escribir el texto en una cuadrícula siguiendo un recorrido específico, como una espiral, diagonal o en zigzag, y luego leer el mensaje en otro orden o dirección. Los cifrados de ruta eran populares en Europa y Asia, y aunque eran efectivos para la época, su complejidad aumentaba dependiendo del patrón de ruta elegido, lo que dificultaba el descifrado sin el conocimiento de la clave.

Criptografía Moderna

La criptografía moderna comenzó en el siglo XX, con el surgimiento de tecnologías digitales y la necesidad de métodos de cifrado más seguros y eficientes.

Criptografía Simétrica: En este tipo de cifrado, tanto el remitente como el receptor utilizan la misma clave para cifrar y descifrar el mensaje. Este enfoque es muy rápido y eficiente en términos de procesamiento, lo que lo hace ideal para la protección de grandes volúmenes de datos. Sin embargo, uno de los mayores desafíos de la criptografía simétrica es el problema de la distribución de claves: ambas partes deben tener una copia de la misma clave, lo que presenta un riesgo de seguridad si no se maneja adecuadamente.

Ejemplos de algoritmos de criptografía simétrica:

- **DES (Data Encryption Standard):** Fue el estándar de cifrado en la década de 1970 y utiliza una clave de 56 bits. Sin embargo, fue reemplazado debido a su vulnerabilidad frente a ataques de fuerza bruta.

- **AES (Advanced Encryption Standard):** Actualmente, AES es uno de los estándares más seguros y ampliamente utilizados. Fue adoptado en 2001 y admite claves de 128, 192 y 256 bits, proporcionando un nivel de seguridad muy alto para diversas aplicaciones.

La criptografía clásica y la moderna difieren fundamentalmente en sus métodos, complejidad y nivel de seguridad. La criptografía clásica se basa en técnicas manuales de sustitución y transposición, como los cifrados César y Vigenère, los cuales, aunque útiles en su época, son vulnerables a métodos de criptoanálisis como el análisis de frecuencia. En cambio, la criptografía moderna utiliza algoritmos matemáticos complejos y claves de mayor longitud, como en los cifrados simétricos (AES) y asimétricos (RSA), que brindan una seguridad mucho más robusta contra ataques actuales. A diferencia de los métodos clásicos, los sistemas modernos permiten el cifrado seguro en redes digitales y soportan aplicaciones avanzadas como firmas digitales y autenticación de identidad, ofreciendo una protección integral adecuada para los requisitos de seguridad contemporáneos.

Conclusión

La criptografía, desde sus orígenes en la antigüedad con métodos simples como la escítala y el cifrado César, hasta su evolución en la era moderna con algoritmos avanzados como AES y RSA, ha sido clave para la protección de la información. A lo largo de la historia, ha desarrollado técnicas cada vez más sofisticadas para garantizar la confidencialidad, integridad, autenticación y no repudio de los datos, pasando de métodos vulnerables al análisis de frecuencia a sistemas basados en matemáticas complejas y claves robustas. En la actualidad, la criptografía es una herramienta esencial en la seguridad informática y de la información, permitiendo comunicaciones seguras y aplicaciones críticas como el comercio electrónico y la autenticación digital. Su evolución refleja la constante necesidad de adaptar la seguridad a las demandas de un mundo digital cada vez más complejo y conectado.

Estudiar criptografía es fundamental en ingeniería en computación porque asegura la protección de datos y sistemas en un mundo digital cada vez más dependiente de la tecnología. La criptografía es la base de la seguridad informática, permitiendo proteger comunicaciones, autenticar identidades y garantizar la integridad de la información frente a amenazas como el robo de datos, el espionaje o los ciberataques. Para un ingeniero en computación, comprender y aplicar estas técnicas es crucial para diseñar sistemas seguros, desarrollar software confiable y garantizar la privacidad y confianza en aplicaciones modernas como el comercio electrónico, las redes sociales, la banca en línea y la infraestructura crítica. En un entorno donde la seguridad es un desafío constante, la criptografía no solo es una herramienta, sino un pilar de la innovación tecnológica responsable, es fundamental en los sistemas operativos dado que nos ayuda para asegurar la protección de datos y la integridad de los procesos dentro de un sistema, se emplea para cifrar y proteger las comunicaciones entre dispositivos a través de los procesos como SSL/ TLS. Como ingenieros en computación es vital entender como se emplea esto dado que protegemos la privacidad del usuario y prevenir vulnerabilidades en los sistemas.

Referencias

- Ferguson, N., & Schneier, B. (2003). Practical Cryptography. Wiley Publishing. Consultado el 14 de noviembre de 2024.
- Katz, J., & Lindell, Y. (2008). Introduction to Modern Cryptography: Principles and Protocols. Chapman and Hall/CRC. Consultado el 14 de noviembre de 2024.
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press. Consultado el 14 de noviembre de 2024.
- Paar, C., & Pelzl, J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer. Consultado el 14 de noviembre de 2024.
- Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). John Wiley & Sons. Consultado el 14 de noviembre de 2024.
- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education. Consultado el 14 de noviembre de 2024.
- Stinson, D. R., & Paterson, M. (2018). Cryptography: Theory and Practice (4th ed.). CRC Press. Consultado el 14 de noviembre de 2024.