TECNOLÓGICA DEL ORIENTE
INSTITUCIÓN DE EDUCACIÓN SUPERIOR

SEGURIDAD EN SOFTWARE

CIFRADO SIMÉTRICO Y ASIMÉTRICO

COMPARACIÓN ENTRE CIFRADO SIMÉTRICO Y ASIMÉTRICO:
FUNDAMENTOS, USOS Y HERRAMIENTAS

El cifrado es un pilar esencial de la seguridad informática, ya que permite resguardar la confidencialidad de la información en entornos digitales. Existen dos enfoques principales: el cifrado simétrico y el asimétrico. Aunque ambos buscan proteger los datos, presentan diferencias clave en su estructura, velocidad, seguridad y aplicaciones. Conocer sus características y usos prácticos permite tomar decisiones acertadas al implementar medidas de protección en sistemas informáticos. Este módulo explora sus principales diferencias, su integración en protocolos de seguridad, la gestión adecuada de claves, y algunas de las herramientas más relevantes utilizadas actualmente.

Comparativa entre cifrado simétrico y asimétrico

1. Introducción

El cifrado es una técnica fundamental en la seguridad informática para proteger la confidencialidad de la información (Hernández Encinas, 2016). Existen dos métodos principales: el cifrado simétrico y el cifrado asimétrico. Aunque ambos buscan asegurar datos, difieren significativamente en su funcionamiento, aplicaciones y características. Entender sus diferencias es crucial para elegir el método adecuado según el contexto de seguridad.

2. Claves utilizadas

- **Cifrado simétrico:** Utiliza la misma clave secreta para cifrar y descifrar la información. Esto significa que tanto el emisor como el receptor deben compartir la misma clave y mantenerla confidencial.
- **Cifrado asimétrico:** Emplea un par de claves, una pública y una privada. La clave pública se usa para cifrar, y la clave privada para descifrar, permitiendo que la clave privada se mantenga en secreto mientras la pública puede ser compartida libremente (Hernández Encinas, 2016).

3. Velocidad y eficiencia

- **Cifrado simétrico:** Es mucho más rápido y eficiente en términos de procesamiento, por lo que es ideal para cifrar grandes volúmenes de datos o para comunicaciones en tiempo real.
- **Cifrado asimétrico:** Es más lento debido a la complejidad matemática detrás del uso de dos claves diferentes, por lo que suele emplearse para cifrar pequeñas cantidades de datos, como claves de sesión o autenticación.

4. Seguridad y gestión de claves

- **Cifrado simétrico:** La principal vulnerabilidad radica en el intercambio seguro de la clave secreta. Si esta clave es interceptada, toda la comunicación queda comprometida (Hernández Encinas, 2016).
- **Cifrado asimétrico:** Permite un intercambio seguro de información sin necesidad de compartir la clave privada. Esto reduce los riesgos en la distribución de claves, haciendo que el sistema sea más seguro en entornos abiertos.

5. Ejemplos prácticos

- **Cifrado simétrico:** Un ejemplo común es el uso del algoritmo AES (Advanced Encryption Standard) para proteger archivos o discos duros completos donde el usuario y el sistema usan la misma clave secreta para cifrar y descifrar la información.
- **Cifrado asimétrico:** Es utilizado en los protocolos HTTPS que aseguran las páginas web. Cuando un usuario accede a un sitio web seguro, se usa el cifrado asimétrico para intercambiar una clave de sesión que luego se usa para cifrado simétrico durante la sesión.

6. Aplicaciones combinadas

En la práctica, muchos sistemas de seguridad combinan ambos métodos para aprovechar sus ventajas. Por ejemplo, en una sesión HTTPS, primero se usa cifrado asimétrico para intercambiar de forma segura una clave simétrica, y luego el cifrado simétrico para la transmisión de datos, optimizando seguridad y rendimiento.

7. Resumen comparativo

Característica	Cifrado Simétrico	Cifrado Asimétrico
Claves	Una misma clave para cifrar y descifrar	Par de claves: pública y privada
Velocidad	Alta velocidad y eficiencia	Más lento y complejo
Seguridad en intercambio de claves	Riesgo en compartir la clave secreta	Intercambio seguro sin compartir clave privada
Uso típico	Cifrado de grandes volúmenes de datos	Autenticación, intercambio de claves, firma digital
Ejemplo común	AES, DES	RSA, ECC

Gestión y distribución de claves

En los sistemas de seguridad informática, el uso de cifrado y autenticación es fundamental para proteger la confidencialidad e integridad de la información (Ortega Candel, 2018). No obstante, estos mecanismos dependen en gran medida de las claves criptográficas, las cuales actúan como el corazón del proceso. Por esta razón, la gestión y distribución de claves se convierte en una tarea crítica dentro de cualquier estrategia de ciberseguridad.

¿Qué es la gestión de claves?

La gestión de claves hace referencia al conjunto de procesos, políticas y tecnologías utilizados para generar, almacenar, proteger, distribuir, revocar y destruir claves criptográficas durante su ciclo de vida. Su objetivo es garantizar que las claves estén disponibles y sean seguras en todo momento, tanto para los usuarios legítimos como para los sistemas que las requieren.

Etapas del ciclo de vida de una clave

1. **Generación:** Se crea una clave con características de aleatoriedad y longitud apropiadas para el tipo de algoritmo usado (por ejemplo, AES o RSA).
2. **Distribución:** La clave se entrega a las partes autorizadas de forma segura.
3. **Almacenamiento:** La clave debe ser guardada en un entorno seguro, como un módulo de seguridad hardware (HSM) o un sistema de gestión de claves (KMS).
4. **Uso:** La clave se emplea para cifrar, descifrar, firmar o autenticar datos.
5. **Rotación o renovación:** Se reemplaza la clave por una nueva, según políticas internas o ante sospechas de compromiso.
6. **Revocación:** Se invalida una clave antes de su vencimiento si se detecta que ha sido comprometida.
7. **Destrucción:** La clave es eliminada de forma segura cuando ya no se necesita, para evitar su recuperación por terceros.

¿Qué es la distribución de claves?

La distribución de claves es el proceso mediante el cual dos o más entidades obtienen claves compartidas para poder comunicarse de manera cifrada (Ortega Candel, 2018). Este proceso debe ser seguro, de lo contrario, toda la protección que ofrece el cifrado se ve comprometida.

Ejemplo 1: Clave simétrica compartida

- Imaginemos que dos empresas, A y B, desean intercambiar archivos cifrados utilizando el algoritmo AES (que es simétrico, es decir, usa la misma clave para cifrar y descifrar). El desafío principal es cómo A puede entregar la clave a B sin que un atacante la intercepte.

Una solución tradicional es usar un canal seguro, como una conexión VPN o entregar la clave en mano usando una memoria USB. Sin embargo, esto no siempre es práctico, especialmente a gran escala.

Ejemplo 2: Distribución de claves usando criptografía asimétrica

- Para resolver este problema, se puede usar criptografía asimétrica. Por ejemplo, la empresa B genera un par de claves (una pública y una privada). Luego:

1. A cifra la clave simétrica con la clave pública de B.

2. B recibe el mensaje cifrado y lo descifra con su clave privada.
3. Ahora ambas entidades comparten una clave simétrica sin que esta haya sido expuesta en texto plano.

Este es el principio básico del intercambio de claves híbrido, utilizado en protocolos como TLS (Transport Layer Security), que protege la mayoría de las comunicaciones en Internet.

Modelos de distribución de claves

Existen varios modelos para distribuir claves, dependiendo del entorno y del nivel de seguridad requerido:

1. **Distribución manual:** Apta para redes pequeñas, pero no escalables. Por ejemplo, ingresar una clave Wi-Fi de forma manual en cada dispositivo.
2. **Centro de distribución de claves (KDC):** Utilizado en entornos corporativos, como en Kerberos, donde un servidor central gestiona y entrega las claves de sesión.
3. **Infraestructura de clave pública (PKI):** Permite distribuir claves públicas a través de certificados digitales, firmados por una Autoridad Certificadora (CA).
4. **Protocolos de intercambio de claves:** Como Diffie-Hellman, que permite a dos partes generar una clave común sin necesidad de transmitirla directamente.

Importancia de una gestión eficaz

Una mala gestión de claves puede provocar fugas de información, suplantación de identidad o la imposibilidad de acceder a datos cifrados. Por ello, organizaciones de todo tipo implementan soluciones de Gestión Centralizada de Claves (EKMS o Enterprise Key Management Systems), que automatizan la rotación, expiración y acceso de claves según políticas de seguridad.

Ejemplo 3: Caso real de compromiso por mala gestión

- En 2013, Adobe sufrió una violación de seguridad que expuso millones de contraseñas cifradas. El problema no solo fue el cifrado débil, sino también la gestión inadecuada de claves, que permitió a los atacantes acceder a información que debía estar protegida.

Aplicaciones prácticas y herramientas de cifrado

Protección de comunicaciones

Uno de los usos más extendidos del cifrado es en la protección de la información que viaja a través de redes, especialmente en Internet (Ortega Candel, 2018).

- **Ejemplo:** Al acceder a una página web con el protocolo HTTPS, el navegador y el servidor establecen una conexión segura mediante TLS (Transport Layer Security). Esto asegura que datos como contraseñas, tarjetas de crédito o correos no puedan ser interceptados por terceros.

Almacenamiento seguro de datos

El cifrado también se aplica al almacenamiento local o en la nube para evitar el acceso no autorizado.

- **Ejemplo:** Un dispositivo móvil moderno (como un teléfono Android o un iPhone) cifra todo el contenido del almacenamiento interno. De esta manera, si el dispositivo es robado, el atacante no puede acceder a los datos sin la clave de desbloqueo.

Cifrado de correos electrónicos

Los correos electrónicos contienen información sensible que puede ser vulnerada si no se protegen adecuadamente. Herramientas como PGP (Pretty Good Privacy) permiten cifrar el contenido del mensaje y garantizar su autenticidad mediante firma digital.

- **Ejemplo:** Una periodista que intercambia información con una fuente confidencial puede usar PGP para asegurarse de que sólo el destinatario previsto pueda leer su mensaje.

Firmas digitales y autenticación

El cifrado asimétrico permite no solo proteger datos, sino verificar la identidad de un emisor mediante firmas digitales. Esto es fundamental para garantizar la integridad y autoría de documentos (Hernández Encinas, 2016).

- **Ejemplo:** Al firmar un contrato digital con certificado digital emitido por una Autoridad Certificadora (CA), se garantiza que el documento no ha sido alterado y que proviene de la persona o entidad firmante.

Respaldo y recuperación segura de datos

Los sistemas de respaldo modernos aplican cifrado para asegurar que incluso si el respaldo cae en manos equivocadas, los datos no sean accesibles sin la clave.

- **Ejemplo:** Servicios de respaldo en la nube como Backblaze o Acronis ofrecen la opción de cifrar los archivos antes de subirlos, protegiéndose con claves definidas por el usuario.

Herramientas de cifrado más utilizadas

Existen diversas herramientas que implementan algoritmos de cifrado y están disponibles para distintos entornos y necesidades (Hernández Encinas, 2016). A continuación, se presentan algunas de las más representativas.

VeraCrypt

- **Tipo:** Software de código abierto para cifrado de discos.
- **Uso:** Permite crear volúmenes cifrados o cifrar particiones completas.
- **Ejemplo práctico:** Un investigador que trabaja con datos confidenciales puede crear un volumen oculto cifrado en su disco duro, al que solo accede mediante una contraseña compleja.

GnuPG (GPG)

- **Tipo:** Herramienta de cifrado y firma digital basada en PGP.
- **Uso:** Cifrado y descifrado de archivos y correos, firma de documentos, gestión de claves públicas/privadas.
- **Ejemplo práctico:** Un equipo de desarrollo en software libre puede distribuir actualizaciones firmadas con GPG para que los usuarios verifiquen su autenticidad.

OpenSSL

- **Tipo:** Biblioteca de cifrado de código abierto.
- **Uso:** Implementa protocolos como TLS/SSL; se usa en servidores web, aplicaciones y dispositivos de red.
- **Ejemplo práctico:** Un administrador de sistemas puede generar certificados autofirmados para pruebas internas en una intranet.

BitLocker (Windows) y FileVault (macOS)

- **Tipo:** Sistemas de cifrado de disco completos integrados en sistemas operativos.
- **Uso:** Protección automática de los datos del disco duro.
- **Ejemplo práctico:** Un trabajador remoto cuya laptop contiene información de clientes puede activar BitLocker para que, en caso de pérdida del equipo, la información siga siendo inaccesible para terceros.

Signal

- **Tipo:** Aplicación de mensajería segura.
- **Uso:** Cifrado de extremo a extremo de mensajes, llamadas y archivos.
- **Ejemplo práctico:** Activistas de derechos humanos la utilizan para comunicarse de manera segura, incluso en regiones con censura o vigilancia gubernamental.

KeePassXC

- **Tipo:** Gestor de contraseñas cifrado.
- **Uso:** Guarda contraseñas en una base de datos cifrada con AES.
- **Ejemplo práctico:** Un analista de seguridad utiliza KeePassXC para mantener contraseñas complejas y únicas para cada sistema que administra.

Consideraciones pedagógicas y de implementación

- Se recomienda enseñar estas herramientas de forma práctica, mediante talleres paso a paso, capturas de pantalla, y simulaciones.

- Las actividades pueden incluir: cifrado y descifrado de mensajes, creación de volúmenes seguros, instalación de certificados SSL en servidores locales, entre otros.
- Un enfoque por proyectos puede consistir en que cada estudiante diseñe una política de cifrado para una pequeña empresa ficticia, seleccionando las herramientas más adecuadas según el caso.

El cifrado no es solo una función matemática compleja, sino una solución concreta para los desafíos actuales de la seguridad digital. Sus aplicaciones se extienden desde la navegación por internet hasta la protección de dispositivos personales y la gestión de infraestructuras críticas. A través del dominio de herramientas específicas, los usuarios pueden proteger activamente su información y contribuir a entornos más seguros y confiables (Hernández Encinas, 2016).

BIBLIOGRAFÍA

- Hernández Encinas, L. (2016). La criptografía. Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro.net/es/lc/tecnologicadeloriente/titulos/41843
- Ortega Candel, J. M. (2018). Seguridad en aplicaciones Web Java. RA-MA Editorial. https://elibro.net/es/lc/tecnologicadeloriente/titulos/106511