Engineer

Cifrado

hacer ilegibles los datos sin la clave

Qué es

El cifrado, que algunas publicaciones del NIST denominan enciphering, transforma datos legibles, el texto en claro, en texto cifrado mediante un algoritmo publicado y un valor secreto llamado clave. El descifrado, con la clave correcta, devuelve el texto en claro byte por byte. El algoritmo es público a propósito: AES, el cifrado al que recurren la mayoría de los sistemas, ganó un concurso abierto del NIST en 2000 y se publica como estándar gratuito. Solo la clave es secreta.

Los cifrados pertenecen a dos familias. Uno simétrico utiliza la misma clave en ambas direcciones. AES, definido en FIPS 197, cifra los datos en bloques de 128 bits con una clave de 128, 192 o 256 bits. ChaCha20, de RFC 8439, es un cifrado de flujo que funciona aproximadamente a tres veces la velocidad de AES en hardware sin instrucciones AES. Los simétricos son suficientemente rápidos para un disco entero, pero ambos extremos necesitan la misma clave y hacerla llegar con seguridad es la parte difícil.

La criptografía de clave pública resuelve eso con un par de claves, una publicada y otra privada. Cada una de las dos partes puede combinar su clave privada con la pública de la otra y obtener el mismo secreto compartido sin enviarlo nunca. Las operaciones de clave pública son lentas, así que los sistemas reales utilizan ambas técnicas: un intercambio de clave pública acuerda una clave simétrica nueva y el cifrado simétrico transporta los datos. TLS, el protocolo detrás de cada dirección `https://`, funciona así.

La idea moderna más importante es la autenticación. Un cifrado sin más oculta el contenido, pero permite modificarlo: en modo contador, cambiar un bit del texto cifrado cambia el mismo bit del texto en claro, y el receptor descifra el mensaje alterado como si fuera auténtico. El cifrado autenticado con datos asociados,

AEAD, añade una etiqueta que el receptor comprueba antes de confiar en un solo byte. AES-GCM y ChaCha20-Poly1305 son los dos habituales. TLS 1.3, publicado como RFC 8446 en 2018, conservó solo cifrados AEAD e hizo que todo intercambio de clave pública tuviera secreto hacia adelante: una clave del servidor robada después no abre ninguna sesión grabada.

Utilice el concepto en una decisión

Aplique «¿Qué es el cifrado?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Cuentas, contraseñas y permisos organizados para que cada persona tenga exactamente el acceso que necesita y lo pierda el mismo día que deja la empresa.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 1.000 reglas RBAC para servidores Linux — 1,000 reglas de acceso escritas para cerrar una brecha de seguridad

1.000 reglas RBAC para servidores Linux Póngase en contacto →

Por qué importa

Los datos rara vez permanecen en hardware controlado por su propietario. Cruzan redes ajenas, residen en el centro de datos de otra entidad y salen del edificio en portátiles. El cifrado permite que pasen por esos lugares con seguridad: un disco robado, un cable intervenido o un bucket filtrado entregan texto cifrado, y sin la clave ese texto es ruido.

Eso traslada el problema, no lo elimina: una vez cifrados los datos, su seguridad depende de la de la clave. La recomendación del NIST sobre gestión de claves, SP 800-57, las compara con la combinación de una caja fuerte: un adversario que la conoce abre incluso la caja fuerte más resistente, y una mala gestión de claves puede comprometer fácilmente un algoritmo sólido. Por tanto, la mayor parte del trabajo real está en las claves: guardarlas separadas de los datos, limitar cuánto protege cada una, sustituirlas según un calendario y proteger la copia de recuperación con el mismo cuidado que la original.

Los reguladores trazan la misma distinción. El RGPD incluye la seudonimización y el cifrado de datos personales entre las medidas de seguridad de su artículo 32. El artículo 34 permite al responsable del tratamiento no avisar individualmente a cada persona afectada por una brecha cuando los datos filtrados eran ininteligibles para cualquiera que no estuviera autorizado a verlos; el cifrado es el ejemplo que ofrece.

El cifrado se aplica en dos lugares. En tránsito, principalmente con TLS, protege los datos durante su transmisión. En reposo, los protege en el almacenamiento. El momento de uso queda fuera de ambos: un servidor que descifra un registro para trabajar con él mantiene a la vez el texto en claro y la clave, de modo que quien controle ese servidor lee lo mismo que él.

Cómo se aplica en la práctica

En tránsito, el trabajo cotidiano consiste en mantener válidos los certificados. Cuando cien aplicaciones Docker necesitaban certificados SSL/TLS, un flujo ACME creó cada certificado, lo renovó antes de que caducara y lo desplegó en hosts Ubuntu con Apache y Nginx. El objetivo era sacar a la persona del circuito, porque es la parte que se olvida: un certificado caducado deja fuera de servicio una aplicación con la misma certeza que un cifrado roto.

En reposo, la pregunta útil es quién tiene la clave. La implementación de copias cifradas fuera del host de la empresa se diseñó para llevar la recuperación más allá de una instantánea del proveedor. Utiliza restic, que cifra lo que almacena con AES-256 en modo contador y lo autentica con Poly1305-AES. Sus scripts permiten enviar instantáneas por SFTP al almacenamiento de otro proveedor. En ese diseño, el proveedor recibe texto cifrado y la empresa conserva la frase de contraseña en un archivo protegido. Eso describe los controles implementados, no su activación operativa: el registro del 2026-10-27 indica que los temporizadores estaban desactivados al no haber un repositorio configurado y no recoge ninguna restauración real completada. El cifrado es una propiedad de la vía de almacenamiento propuesta; demostrar que la copia puede recuperarse exige ejecutar la prueba de restauración separada.

Hasta el recorrido de la frase de contraseña importaba. Se lee desde un archivo porque el supervisor de procesos interpreta los escapes en los valores de entorno; una frase que contuviera una barra inversa habría sido distinta, sin avisar, de la utilizada para crear el repositorio. El flujo mensual de pruebas de restauración implementado está diseñado para restaurar un archivo conocido del repositorio y compararlo con el resultado esperado. Como la prueba necesita la frase de contraseña, una ejecución satisfactoria también verificaría que la clave sigue abriendo los datos.

Cuando la plataforma iba a incorporar un segundo host, el mismo razonamiento decidió cómo se separó cada secreto operativo por host. Una cadena de conexión al repositorio de copias identifica una ubicación. Dos repositorios restic

independientes pueden tener claves maestras distintas aunque utilicen la misma frase de contraseña. Quien obtenga esa frase y pueda leer los datos cifrados y los archivos de claves de ambos repositorios podrá desbloquear los dos, por lo que compartirla vincula su exposición. Cada secreto pasó a ser un mapa indexado por host, con el razonamiento escrito junto a la configuración. SP 800-57 expone el principio general: limitar lo que protege una clave limita el daño cuando se filtra.

Dónde surgen los problemas

La clave solo existe en un lugar. Un cifrado sólido trata a un propietario que olvidó la contraseña exactamente igual que a un atacante. La documentación de restic lo dice claramente: si se pierde la contraseña, también se pierden los datos, sin posibilidad de recuperarlos. Todo almacenamiento cifrado necesita una segunda copia de su clave, guardada donde no pueda llegar lo que destruya la primera.

La clave está junto a los datos. Una base de datos cifrada con la clave en la configuración del mismo servidor, o una copia cuya frase de contraseña vive en el mismo bucket, solo frenan a un ladrón que se lleva la mitad de los archivos. El cifrado de disco es la variante más discreta: protege una unidad extraída de una máquina apagada, mientras que un servidor en marcha ya ha desbloqueado su disco y un atacante presente en él lee texto en claro.

Se confunde secreto con integridad. Un sistema construido con un modo de cifrado sin autenticación oculta el contenido y sigue permitiendo que un atacante lo altere. Utilice una construcción AEAD y descarte cualquier mensaje cuya etiqueta falle antes de actuar sobre uno solo de sus bytes.

Se repite un nonce. AES-GCM y ChaCha20-Poly1305 reciben un nonce, un valor que debe ser único para cada mensaje bajo una misma clave. RFC 8439 lo llama la consideración de seguridad más importante: dos mensajes con el mismo nonce comparten un flujo de claves y una clave de autenticación de un solo uso, lo que revela el XOR de ambos textos en claro. Un contador es una forma segura de crear nonces si hay un único contador para esa clave: dos procesos que comparten clave y cuentan cada uno desde cero producen precisamente la repetición de la que advierte el RFC.

Una contraseña sustituye a una clave. Las personas eligen contraseñas; los cifrados necesitan claves aleatorias de longitud fija. Una frase de contraseña pasa primero por una función de derivación de claves, como hace restic con scrypt,

que RFC 7914 diseña para exigir mucha memoria, de modo que probar contraseñas en masa en hardware especializado siga siendo costoso. Las contraseñas de acceso almacenadas son otro caso: deben almacenarse como hashes producidos por una función así, porque un servidor que pueda descifrarlas también puede filtrarlas.

Los metadatos siguen visibles. El cifrado oculta el contenido, pero el tamaño, los tiempos y las direcciones de ambos extremos siguen a la vista. TLS 1.3 permite al emisor rellenar los registros para ocultar su tamaño, y el relleno es opcional, de modo que la longitud suele revelar más de lo que espera el propietario.

Lecturas adicionales

- Glosario del NIST: cifrado — Todas las definiciones utilizadas por las publicaciones del NIST, cada una con su documento de origen.
- FIPS 197: Advanced Encryption Standard (AES) — La especificación AES, con su tamaño de bloque y sus tres longitudes de clave.
- NIST SP 800-57, parte 1, revisión 5: recomendación para la gestión de claves — Cómo se crean, guardan, utilizan y retiran las claves, y qué ocurre cuando se filtra una.
- RFC 8446: protocolo Transport Layer Security (TLS), versión 1.3 — El protocolo de `https://`, con registros exclusivamente AEAD e intercambio de claves con secreto hacia adelante.
- RFC 8439: ChaCha20 y Poly1305 para los protocolos de IETF — Un cifrado de flujo, un autenticador y su combinación AEAD, con las reglas de los nonces.
- restic: referencias — Cómo una herramienta real de copias deriva claves de una contraseña y después cifra y autentica sus datos.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es el cifrado?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/encryption/