Cifrado (criptografía)

Ejemplo de cifrado que utiliza el cifrado Vernam.

En criptografía, el **cifrado** es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo. Las claves de cifrado y de descifrado pueden ser iguales (criptografía simétrica), distintas (criptografía asimétrica) o de ambos tipos (criptografía híbrida).

El conjunto de caracteres (alfabeto) usado en el mensaje sin cifrar puede no ser el mismo que el juego de caracteres que se usa en el mensaje cifrado.

A veces el texto cifrado se escribe en bloques de igual longitud. A estos bloques se les denomina *grupos* [*cita requerida*]. Estos grupos proporcionaban una forma de verificación adicional, ya que el texto cifrado obtenido debía tener un número entero de grupos. Si al cifrar el texto plano no se tiene ese número entero de grupos, entonces se suele rellenar al final con ceros o con caracteres sin sentido.

Aunque el cifrado pueda volver secreto el contenido de un documento, es necesario complementarlo con otras técnicas criptográficas para poder comunicarse de manera segura. Puede ser necesario garantizar la integridad la autenticación de las partes, etcétera.

Índice

Terminología
Preprocesado del texto simple
Tipos de cifrado según sus claves
- Cifrado Simétrico
- Cifrado Asimétrico

Tipos de cifrado según sus algoritmos
- La criptografía en el pasado

Tipos de cifrado según sus propiedades
Véase también
Véase también
Referencias
Enlaces externos

Terminología

En el proceso de cifrado/descifrado se establecen una serie de términos y convenios para facilitar referirse a los distintos elementos que intervienen:

- El **texto en claro** o **texto simple** (en inglés, *plain text*) es el mensaje que se cifra.
- El **criptograma** o **texto cifrado** es el mensaje resultante una vez que se ha producido el cifrado, es decir, el mensaje cifrado.
- El **cifrado** es el proceso que consiste en convertir el *texto plano* en un galimatías ilegible (cifrar), el mensaje cifrado.
- El **cifrador** es el sistema que implementa el algoritmo de cifrado.
- El **algoritmo de cifrado** o cifra es el algoritmo que se utiliza para cifrar.
- La **clave** de cifrado se utiliza en el algoritmo de cifrado.
- El **descifrado** es el proceso de convertir el texto cifrado en el texto en claro.
- El **descifrador** es el sistema que implementa el algoritmo de descifrado.
- El **algoritmo de descifrado** o descifra es el algoritmo que se utiliza para descifrar.
- La **clave de descifrado** se utiliza en el algoritmo de descifrado.
- La **gestión de claves** es el proceso de generación, certificación, distribución y cancelación de todas las claves, necesarios para llevar a cabo el cifrado.
- El **criptosistema** es el conjunto estructurado de los protocolos, los algoritmos de cifrado/descifrado, los procesos de gestión de claves y las actuaciones de los usuarios.
- La **descripción de entidades**: cuando se desea describir un algoritmo de cifrado/descifrado que involucra el envío de mensajes secretos, muchos autores usan los nombres genéricos *Alice* y *Bob* en lugar de los crípticos A y B. Si intervienen otras entidades (C, D, F... -la E quedaría reservada-), se les asignan entonces nombres que empiecen con estas iniciales, y los más frecuentes son *Carol* y *Dave*. Cuando un escenario involucra protección frente a atacantes que hacen escuchas, entonces para referirse a ellos se suele usar el nombre *Eve* (del término inglés *eavesdropper*, "fisgón") o bien el nombre *Mallory*, en caso de que el atacante, además de interceptar el mensaje, tenga la habilidad de alterarla.

Con frecuencia a los procesos de cifrado y descifrado se les denomina *encriptado* y *desencriptado*, ambos anglicismos de los términos ingleses *encrypt* y *decrypt*. La Real Academia Española recogió esa acepción en la edición de su diccionario de 2014.[1] Por su parte La Fundación del Español Urgente defiende que *encriptar* es un término válido y que no hay razón para censurar su uso.[2] [3]

Preprocesado del texto simple

En algunas ocasiones, antes de cifrar se realiza un preproceso de adaptación del texto plano. En este proceso se pueden seguir varios pasos que permitan el cifrado o hagan que el cifrado resultante sea más resistente frente a ataques por criptoanálisis. Todos estos cambios se tendrán que tener en cuenta cuando se realice el descifrado para poder obtener el texto plano original. Por ejemplo, son frecuentes las siguientes operaciones:

- **Conversión de alfabeto**. Algunos cifradores usan un alfabeto del texto en claro que no se corresponde con el del mensaje que se quiere cifrar. Por tanto, es necesario adaptar el mensaje a ese alfabeto. Por ejemplo, algunos cifradores usan como alfabeto del texto plano el alfabeto latino. Si se desea cifrar un texto en español, es necesario realizar un proceso como resultado del cual no aparezcan los caracteres H, J, Ñ, K, U, W y Y (por ejemplo, podrían sustituirse la U y la W por la V, la K con la Q, la Ñ por la N, la Y por la I, la J por la G, y eliminar la H). Otro ejemplo clásico es el caso de cifradores que no permiten cifrar minúsculas, en cuyo caso será necesario convertir todo en mayúsculas.
- **Preproceso para dificultar el criptoanálisis**. Para aumentar la calidad del texto cifrado con cierto cifrador, ya sea por su resistencia frente a ataques, extensión o cualquier otra

circunstancia, a veces se preprocesa el texto en claro. Algunos ejemplos de estrategias son:

- Inclusión de fragmentos que son para despistar y que no tienen ningún significado. Habitualmente estos fragmentos son caracteres, y se denominan *caracteres nulos*.
- Eliminación de situaciones del texto claro que pueden ser aprovechadas por ataques de criptoanálisis. Por ejemplo:
  - Los espacios en blanco y signos de puntuación suelen eliminarse para que, además de conseguir una trasmisión más eficiente, se consiga que las palabras no se puedan distinguir por los contornos. Esto puede producir ambigüedades que se tenían que resolver por el contexto.
  - Los casos de secuencias de letras idénticas seguidas (por ejemplo, *RR* o *LL* del idioma español, en ciertos tipos de cifradores pueden ser aprovechadas por atacantes. Para romper estas secuencias de caracteres iguales, suelen aplicarse dos estrategias: eliminar uno de los caracteres o meter un contenido que no se tiene que interpretar (si es un solo carácter, se le llama *carácter nulo*).

- **Usar un código**. A veces, antes de cifrar, se utiliza un código que dificulta llegar al significado de ciertas palabras o frases especialmente importantes o habituales.
- **Conversión a números**. Hay algunos algoritmo de cifrado como el RSA que necesitan convertir los caracteres en números. Se pueden seguir distintas estrategias. Veamos algunos ejemplo:
  - Podríamos usar una tabla de conversión de los caracteres en números usando algún sistema de codificación de caracteres como ASCII o Unicode. Por ejemplo el mensaje "Hello World" usando Unicode-8 quedaría:

    ```
    48 65 6C 6C 6F 20 57 6F 72 6C 64
    ```
    Esta cadena de bytes podríamos convertirla en un número concatenándolos obteniendo:
    `0x48656C6C6F20576F726C64=875216180888825337921158l2`

  - Otra opción podría ser considerar que los caracteres están ordenados según un criterio e interpretar la cadena como un número con base el número de caracteres del alfabeto. Por ejemplo si consideramos que solo hay caracteres en mayúsculas y los ordenamos según el orden alfabético tendríamos por ejemplo:

    $$\texttt{"HIJO"} = 7 \cdot 26^3 + 8 \cdot 26^2 + 9 \cdot 26 + 14 = 128688$$

El cualquier caso el número resultante puede ser demasiado pequeño lo que podría producir un texto cifrado que no sea seguro. Para ello se suele aplicar un esquema de relleno (ejemplo PKCS#1v1.5, el cual está ya roto, o OAEP descrito en PKCS#1v2.0)

Tipos de cifrado según sus claves

Cifrado Simétrico

En esquemas de clave simétrica, las claves de cifrado y descifrado son las mismas. Las partes comunicantes deben tener la misma clave para lograr una comunicación segura. Un ejemplo de una clave simétrica es la máquina Enigma del ejército alemán. Había configuraciones clave para cada día. Cuando los Aliados

descubrieron cómo funcionaba la máquina, pudieron descifrar la información codificada dentro de los mensajes tan pronto como pudieron descubrir la clave de cifrado para las transmisiones de un día determinado.

La criptografía simétrica es la técnica criptográfica más antigua que existe, pero sigue ofreciendo un alto nivel de seguridad. Se basa en la utilización de una única clave secreta que se encargará de cifrar y descifrar la información, ya sea información en tránsito con protocolos como TLS, o información en un dispositivo de almacenamiento extraíble. La criptografía simétrica fue el primer método empleado para el cifrado de la información, se basa en que se utilizará la misma contraseña tanto para el cifrado como el descifrado, por tanto, es fundamental que todos los usuarios que quieran cifrar o descifrar el mensaje, tengan esta clave secreta, de lo contrario, no podrán hacerlo. Gracias a la criptografía simétrica, podremos realizar comunicaciones o almacenar archivos de forma segura.

El cifrado simétrico es una de las más antiguas formas de cifrado de la historia. La cuál utiliza una sola clave para cifrar y la misma clave para descifrar.

Cifrado Asimétrico

En los esquemas de cifrado de clave pública, la clave de cifrado se publica para que cualquiera pueda usar y cifrar mensajes. Sin embargo, solo la parte receptora tiene acceso a la clave de descifrado que permite leer los mensajes.[4] El cifrado de clave pública se describió por primera vez en un documento secreto en 1973;[5] antes de eso, todos los esquemas de cifrado eran de clave simétrica (también llamada clave privada).[6] Aunque se publicó posteriormente, el trabajo de Diffie y Hellman, fue publicado en una revista con un gran número de lectores, y el valor de la metodología se describió explícitamente[7] y el método se conoció como el intercambio de claves Diffie Hellman.Una aplicación de cifrado de clave pública disponible públicamente llamada Pretty Good Privacy (PGP) fue escrita en 1991 por Phil Zimmermann y distribuida gratuitamente con el código fuente. PGP fue comprado por Symantec en 2010 y se actualiza regularmente.[8] A este tipo de cifrado también se le llama **criptografía de clave pública** o **PKE** (del inglés *Public-Key Encryption*). Los métodos más conocidos de este tipo de cifrado son el RSA y ElGamal.

La utilización de un sistema simétrico o asimétrico depende de las tareas a cumplir. La criptografía asimétrica presenta dos ventajas principales: suprime el problema de transmisión segura de la clave y permite la firma electrónica. No reemplaza sin embargo los sistemas simétricos, ya que los tiempos de cálculo son evidentemente más cortos con los sistemas simétricos que con los asimétricos.

Tipos de cifrado según sus algoritmos

Según la forma en la que operan los algoritmos de cifrado o descifrado, es posible distinguir varios tipos:[9]

- Cifrado en flujo: En estos algoritmos el cifrado se realiza bit a bit. Están basados en la utilización de claves muy largas que son utilizadas tanto para cifrar como para descifrar. Estas claves pueden estar predeterminadas (libreta de un solo uso) o generarse usando un generador de claves pseudoaleatorias o RKG (acrónimo del inglés *r*andom *k*ey *g*enerator), que genera una secuencia binaria pseudoaleatoria a partir de una clave de inicialización K. A veces, en el cálculo de la clave pseudoaleatoria también interviene el mensaje cifrado hasta ese momento. Por otra parte, el cifrador propiamente dicho: habitualmente en este tipo de algoritmos hay que mantener en secreto tanto la clave como el cifrador.
- Cifrado por bloques: En este tipo de algoritmos, el cifrado se realiza bloque a bloque. En primera instancia, se descompone el mensaje en bloques de la misma longitud. A continuación, cada bloque se va convirtiendo en un bloque del mensaje cifrado mediante una secuencia de operaciones. Ejemplos típicos de operaciones realizadas para conseguir

cada mensaje cifrado son la sustitución y la permutación (cifrado por transposición) de elementos.

Este tipo de algoritmos pueden ser tanto de clave simétrica como de clave asimétrica. Sin embargo, en la bibliografía suele haber confusión y es frecuente ver casos en que se refieren solo a algoritmos de clave simétrica.

La criptografía en el pasado

En la criptografía clásica los cifrados se basaban en la sustitución (cifrado por sustitución), en la permutación (cifrado por transposición) o en una combinación de ambas técnicas. Habitualmente, las operaciones se aplicaban a bloques aunque otras veces se aplicaban al texto plano completo. Había cifrados por transposición que cambiaban la posición de caracteres a lo largo de la cadena que tenía que cifrarse. Por ejemplo, un cifrado podía consistir en permutar e invertir el orden de los caracteres, dejando el primer carácter en la última posición, el último en la primera posición, el segundo en penúltimo lugar, etcétera.

Tipos de cifrado según sus propiedades

Muchas veces se agrupan los algoritmos de cifrado en función de sus propiedades o características. Algunos ejemplos:

- cifrado seguro hacia adelante
- cifrado con umbral
- cifrado basado en identidad
- cifrado negable
- cifrado con clave aislada
- cifrado maleable

Véase también

- código
- confusión entre cifrados y códigos
- criptografía asimétrica
- criptografía simétrica

Véase también

- Cifrado por transposición

Referencias

1. RAE, [1] (https://twitter.com/RAEinforma/status/611085767943823360)
2. Fundéu BBVA, *encriptar* es ocultar un mensaje con una clave (http://www.fundeu.es/recomendacion/encriptar-es-un-termino-valido/), 3/7/2013.
3. ndéu BBVA en Colombia: "encriptar" es ocultar un mensaje con una clave (http://noticias.lainformacion.com/ciencia-y-tecnologia/ciencias-informaticas/fundeu-bbva-en-colombia-encriptar-es-ocultar-un-mensaje-con-una-clave_GeuK4MhBEcnZqCsdzjqqU/), 3/7/2013

4. Bellare, Mihir. "Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements." Springer Berlin Heidelberg, 2000. Page 1.
5. "Public-Key Encryption - how GCHQ got there first! (https://web.archive.org/web/20100519084635/http://www.gchq.gov.uk/history/pke.html)". gchq.gov.uk. Archived from the original (http://www.gchq.gov.uk/history/pke.html) on May 19, 2010.
6. Goldreich, Oded. Foundations of Cryptography: Volume 2, Basic Applications. Vol. 2. Cambridge university press, 2004.
7. Diffie, Whitfield; Hellman, Martin (1976), *New directions in cryptography*, **22**, IEEE transactions on Information Theory, pp. 644–654
8. "Symantec buys encryption specialist PGP for $300M" (http://www.computerworld.com/s/article/9176121/Symantec_buys_encryption_specialist_PGP_for_300M).
9. José Pastor Franco, Miguel Ángel Sarasa López, José Luis Salazar Riaño (1997). *Criptografía digital: fundamentos y aplicaciones*. Zaragoza: Prenseas Universitarias de Zaragoza.

Enlaces externos

- La primera máquina electrónica Enigma del mundo (en inglés) (http://xoomer.alice.it/www_enigma)
- Video en YouTube (https://www.youtube.com/watch?v=5EUYbI1q1y4)
- Cifrado de los mensajes en línea (http://webcrypt.org/es)
