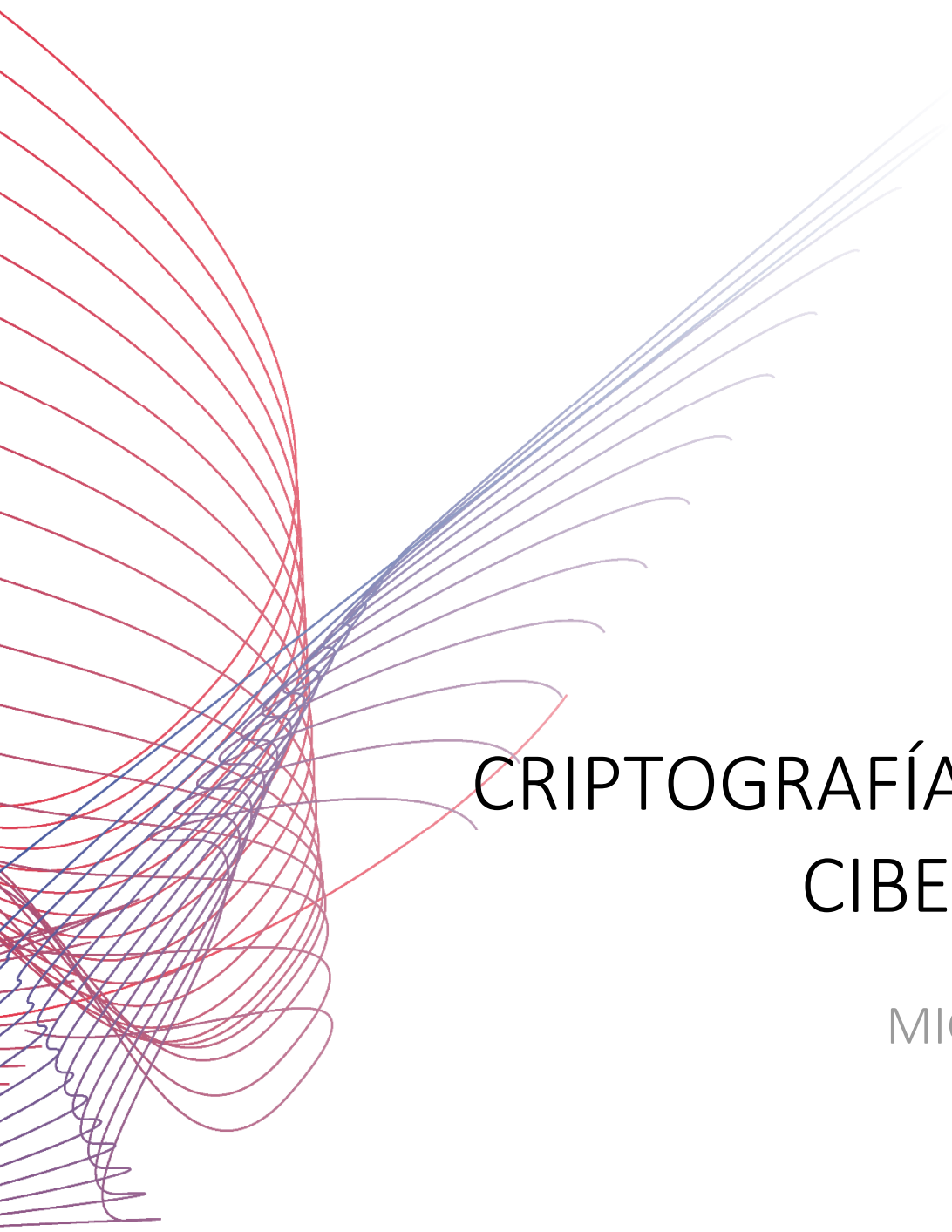
en cs de sk es

TECH pedia



CRIPTOGRAFÍA, DELITOS CIBERNÉTICOS

MIGUEL SORIANO

Título: Criptografía, delitos cibernéticos
Autor: Miguel Soriano
Traducido por: Miquel Soriano
Publicado por: České vysoké učení technické v Praze
Fakulta elektrotechnická
Dirección de contacto: Technická 2, Praha 6, Czech Republic
Número de teléfono: +420 224352084
Print: (only electronic form)
Número de páginas: 40
Edición: Primera edición, 2017

ISBN 978-80-01-06204-3

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea.
Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

NOTAS EXPLICATIVAS

	Definición
	Interesante
	Nota
	Ejemplo
	Resumen
	Ventajas
	Desventajas

ANOTACIÓN

Este módulo contiene información necesaria para la orientación básica de los estudiantes en el campo de la criptografía y los delitos cibernéticos

OBJETIVOS

Este módulo proporciona información básica acerca de la criptografía y los delitos cibernéticos. La primera parte del curso está diseñada para introducir a los estudiantes y ayudarles en el conocimiento de las posibilidades que puede ofrecer la criptografía para la protección de la información. Por lo tanto, el curso incluye una breve descripción de los conceptos fundamentales de la criptografía tanto simétrica como de clave pública, así como de los algoritmos más utilizados. La segunda parte está dedicada a introducir el concepto de delito cibernético e incluye una clasificación de las técnicas de ataque. Por último, se ofrecen algunos consejos básicos de prevención

LITERATURA

[1] Bruce Schneier: Applied Cryptography. John Kiley & Sons, Inc., New York, 1994

[2] William Stallings: Cryptography and Network Security. Principles and Practices. Prentice Hall, New Jersey, 2003

[3] Vesna Hassler: Security Fundamentals for E-Commerce. Artech House, Boston, 2001

[4] Rolf Oppliger: Internet and Intranet Security. Artech House, Boston, 2002

[5] Michael Goodrich, Roberto Tamassia: Introduction to Computer Security, 2010

[6] John R. Vacca: Computer and Information Security Handbook (Morgan Kaufmann Series in Computer Security), 2009

[7] Jason Andress: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Elsevier, 2011

Indice

1 Conceptos básicos de criptografía

La criptografía es una herramienta matemática muy útil para la protección de la información en los sistemas de transmisión de datos. Muchas aplicaciones de seguridad se basan en el uso de la criptografía para el cifrado y descifrado de datos. Gracias a la criptografía, se pueden transmitir datos críticos a través de redes de telecomunicaciones, de forma segura, sin la amenaza que la información sea interceptada y posteriormente, comprometida. El cifrado se puede definir como el proceso de elaboración de información indescifrable e inútil para todos excepto los destinatarios autorizados de dicha información. El descifrado es la conversión de los datos de nuevo a su forma original.

Esta técnica se utiliza en muchas acciones cotidianas, como establecer o recibir una llamada desde un teléfono móvil, pagar con una tarjeta de débito o crédito, retirar dinero de un cajero automático, iniciar una sesión en un ordenador con una contraseña,... La criptografía permite almacenar información crítica o transmitirla a través de redes inseguras (como Internet), de modo que no pueda ser leída por nadie excepto el destinatario. La criptografía se ha convertido en un estándar de la industria para proporcionar seguridad en el almacenamiento de la información, en el control de acceso a los recursos, y en las transacciones electrónicas. Sin embargo, es importante señalar que la criptografía por sí sola no es suficiente para ofrecer protección frente a todas las amenazas a la seguridad de la información.

Un algoritmo criptográfico no es más que un conjunto de secuencias para llevar a cabo tanto el cifrado como el descifrado correspondiente. Es decir, el cifrado de los datos es el resultado de una fórmula matemática diseñada específicamente para ocultar unos datos. Los algoritmos de cifrado más ampliamente extendidos utilizan como parte del proceso operativo con una o varias claves. Un mismo texto claro tiene diferentes cifrados cuando se utilizan diferentes claves. Idealmente, si se desconoce la clave correspondiente, no debería haber ninguna manera de encontrar el texto original a partir del texto cifrado, excepto la fuerza bruta, es decir, probando todas las posibles claves hasta encontrar la clave correcta. La seguridad de los datos cifrados depende totalmente de dos cosas: de la robustez del algoritmo criptográfico y del secreto de la clave.

El número de claves posibles debe ser lo suficientemente grande para que sea computacionalmente imposible llevar a cabo un ataque de fuerza bruta con éxito en un período de tiempo razonable. Muchos algoritmos criptográficos aumentan su protección aumentando la longitud de las claves que utilizan. Sin embargo, cuanto mayor sea la clave, mayor es el tiempo de computación que se requiere para cifrar y descifrar datos. Por ello, es importante elegir un algoritmo de cifrado que tenga un buen equilibrio entre las necesidades de protección y el coste computacional de la protección de los datos.

Los algoritmos criptográficos modernos se pueden clasificar atendiendo a dos criterios distintos: el tipo de clave que se utiliza, y la manera en que operan sobre los datos.

Respecto al tipo de clave utilizada, los algoritmos criptográficos se pueden clasificar en:

a) Algoritmos de clave simétrica, también llamados de clave secreta. La criptografía de clave simétrica se refiere a métodos de cifrado en los que emisor y receptor comparten la misma clave (o, con menor frecuencia, en los que sus claves son diferentes, pero relacionados de una manera fácilmente computable). Un ejemplo de algoritmo simétrico ampliamente utilizado es el "Advanced Encryption Standard (AES)".

b) Algoritmos de clave pública, también llamados de clave asimétrica. Se trata de esquemas que utilizan un par de claves para cada usuario: una clave pública, que puede ser conocido por todo cualquier usuario, y una clave privada, conocida sólo por el usuario correspondiente. Obviamente, las dos claves de un mismo par están vinculadas matemáticamente; sin embargo, es computacionalmente imposible conocer la clave privada a partir de la clave pública. Un usuario o entidad publica su clave pública y mantiene en secreto su clave privada. Cualquier persona que tenga la clave pública de otro usuario puede cifrar información destinada a dicho usuario, pero no puede descifrarla. Sólo la persona que tiene la clave privada correspondiente puede descifrar la información.

La principal ventaja de la criptografía de clave pública es que permite que personas que no tienen ningún acuerdo de seguridad previo puedan intercambiar mensajes de forma segura. El emisor y el receptor no tienen que compartir las claves secretas a través de canales seguros; todas las transmisiones exigen sólo el conocimiento de las claves públicas, y las claves privadas nunca se transmiten ni se comparten.

En cuanto a la manera en que los algoritmos operan con los datos, los sistemas criptográficos se pueden clasificar en,

a) Cifrado en bloque: operan con grupos que tienen un número concreto de bits, llamados bloques, utilizando una transformación invariable que depende de la clave. Se divide el mensaje en bloques y se cifra un bloque cada vez. Si el algoritmo de cifrado en bloque se considera seguro, también se considera protegido el texto cifrado resultante de un único bloque de datos. Sin embargo, el sistema no es seguro cuando se cifran varios mensajes con la misma clave, ya que bloques de mensajes idénticos dan bloque de texto cifrado también idénticos. Por lo tanto, un atacante podría detectar fácilmente repeticiones de bloque en el mensaje; en consecuencia, el uso directo de un cifrado de bloques (sin encadenamientos) es desaconsejable, y por ello se utilizan modos de operación diferentes para evitar este problema.

b) Cifrados de flujo: convierten un símbolo del texto original en un símbolo de texto cifrado. Trabajan mediante la generación de una secuencia pseudoaleatoria que funciona como una cadena de claves criptográficas. Este flujo de claves es básicamente una secuencia de bits que se combina con el texto original para cifrar un símbolo cada vez, generando así el texto cifrado.

Durante el módulo se utilizará la siguiente terminología:

- Texto en claro: es el mensaje original que debe ser transmitido al destinatario.
- Texto cifrado: es la salida que se genera tras cifrar el texto en claro.
- Cifrado: es el proceso de modificar el contenido de un texto en claro, de manera que se oculta el contenido real.
- Descifrado: es el proceso inverso al cifrado; es el proceso de obtener el mensaje de texto en claro a partir del texto cifrado correspondiente.
- Clave: es una palabra, número o secuencia de caracteres que se utiliza para cifrar el texto en claro o para descifrar el texto cifrado.
- Criptoanálisis es la ciencia que estudia como romper algoritmos criptográficos.
- Algoritmo de hash: es un algoritmo unidireccional que convierte una cadena de texto de longitud arbitraria en una cadena de longitud fija.
- Algoritmo criptográfico: una función matemática utilizada para el cifrado y el descifrado.
- Gestión de claves: Proceso por el cual una clave se genera, se almacena, se protege, se transfiere, se usa y se destruye.

2 Criptografía de clave simétrica

El proceso de cifrado y descifrado de información mediante el uso de una única clave se conoce como criptografía de clave simétrica o criptografía de clave secreta. En la criptografía de clave simétrica, las claves utilizadas para cifrar el texto en claro y para descifrar el texto cifrado suelen ser idénticas (situación habitual), o bien cuando se conoce una también se conoce la otra, ya que están vinculadas mediante una transformación muy simple. El principal problema con los algoritmos de clave simétrica es que el remitente y el receptor tienen que ponerse de acuerdo en esa clave común.

Ambas partes deben proteger la clave; la divulgación de la clave por cualquiera de las partes puede comprometer de la información.

El proceso de cifrar mediante criptografía de clave simétrica es el siguiente: El usuario A desea enviar un mensaje al usuario B y quiere tener la certeza que sólo el usuario B es capaz de leer el mensaje. Para proteger la transmisión, el usuario A genera una clave secreta, cifra el mensaje con esta clave, y envía el criptograma al usuario B. El usuario B necesita esa clave para poder descifrar el texto cifrado. El usuario A puede transmitir la clave secreta al usuario B mediante el uso de cualquier medio disponible, siempre que sea una transmisión segura. Cuando el usuario B reciba la clave secreta, ya podrá descifrar el criptograma para recuperar el texto en claro.

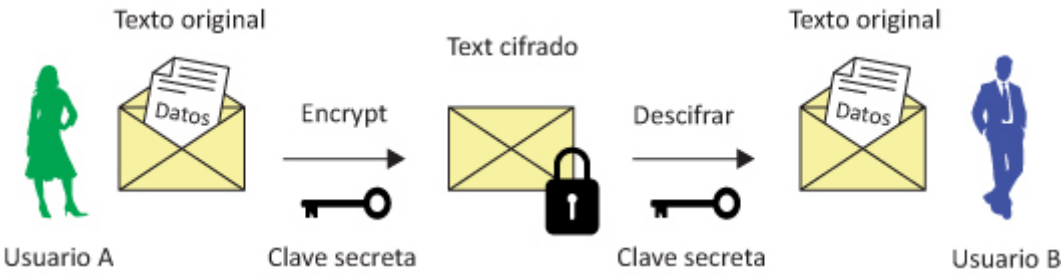


Fig 2.1. Modelo de cifrado con clave simétrica

Las propiedades que un algoritmo de cifrado deben cumplir son las siguientes:

- Difusión: cada bit del texto en claro influye en muchos bits del criptograma y cada bit del criptograma se ve afectado por muchos bits del texto en claro.
- Confusión: es necesario evitar las relaciones estructuradas (especialmente linealidad) entre texto plano y texto cifrado que podrían ser explotadas en los ataques conocidos.
- El criptograma debería tener apariencia aleatoria.
- Simplicidad. No debe ser necesario disponer de un hardware complejo para poder ejecutar el algoritmo

- Eficiencia: muy rápido en hardware y software en una amplia variedad de plataformas.

El principal problema cuando se utiliza criptografía simétrica es que el proceso de transferencia de claves al receptor puede suponer un gran riesgo de seguridad. La transferencia de la clave secreta a través de Internet mediante un mensaje de correo electrónico es insegura. Asimismo, tampoco es seguro transmitir la clave oralmente mediante una llamada telefónica ni enviarla mediante correo convencional.

Los riesgos de seguridad derivados del uso de la criptografía simétrica se han podido solventar en gran medida mediante el uso de la criptografía de clave pública. Un ejemplo de aplicación de criptografía simétrica es el cifrado de datos en los discos duros. En ese caso como la misma persona cifra y descifra los datos no hay ningún problema con la distribución de claves.

Como se indicó en la sección anterior, una distinción importante en los algoritmos de clave secreta entre los algoritmos de cifrado en flujo y en bloque. Hoy en día, los algoritmos de cifrado en bloque son mucho más habituales que los de cifrado en flujo.

2.1 Algoritmos de cifrado en bloque

El cifrado en bloque transforma un grupo de símbolos del texto en claro en un grupo de símbolos de texto cifrado. Así pues, el cifrado se realiza bloque a bloque del texto en claro.

Los símbolos del texto en claro se agrupan en bloques de texto en claro y la transformación criptográfica se aplica a cada uno de esos bloques utilizando la clave criptográfica correspondiente. El resultado del cifrado de un bloque de texto en claro es otro bloque de texto cifrado del mismo tamaño.

Es posible que el tamaño de texto claro no sea exactamente múltiplo de la longitud de bloque; en este caso, generalmente, se aplica un esquema de relleno para completar el último bloque. Sin embargo, dependiendo del modo de operación, este relleno podría no ser necesario. El principio de cifrado y descifrado en el que se basa el sistema de cifrado de bloque se muestra en la siguiente figura.

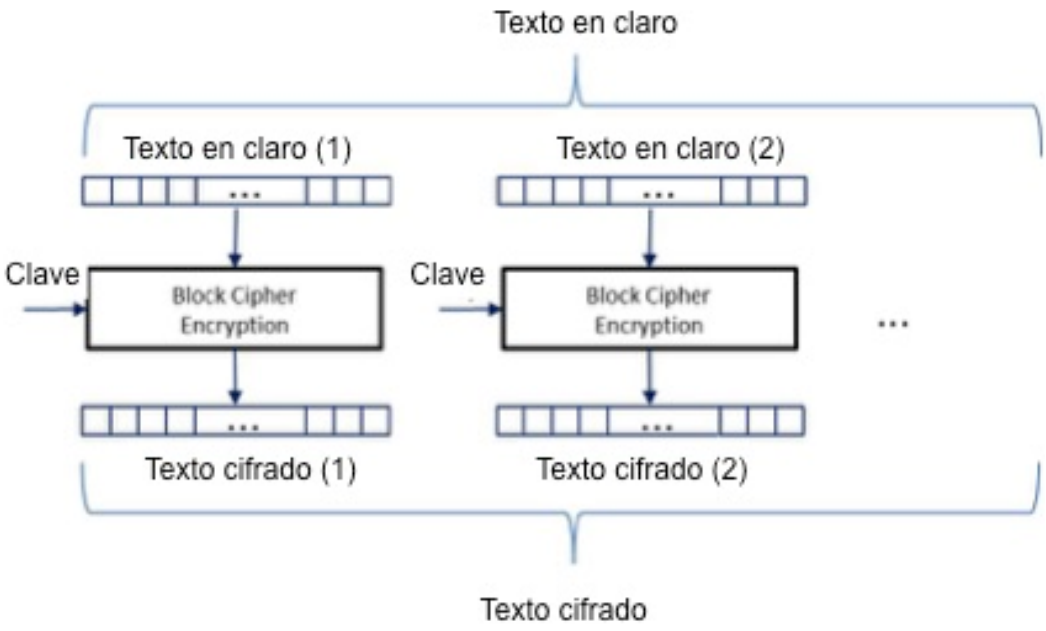


Fig. 2.2. Esquema de cifrado en bloque

La mayoría de los cifrados de bloque se basan en aplicar iterativamente el concepto de cifrado producto. Estos algoritmos realizan el cifrado en múltiples rondas o iteraciones, repitiendo en cada una de ellas una serie de operaciones sobre los datos y utilizando una subclave distinta, que deriva de la clave original. Las operaciones aplicadas en cada ronda normalmente comprenden: sustitución, permutación y mezcla con la clave. Estos algoritmos se conocen como redes de sustitución de permutación (SPN) y cifrados de Feistel. Las operaciones de sustitución constituyen la única operación no lineal en la mayoría de estos sistemas de cifrado; por ello se deben diseñar con mucho cuidado para conseguir protección contra ataques de criptoanálisis.

El descifrado se realiza de la misma manera. Esta transformación se aplica sobre el bloque de texto cifrado utilizando la misma clave k (en el caso de algoritmos de clave simétrica) que se utilizó en el proceso de cifrado. El resultado de este proceso es el bloque de texto en claro.

Típicamente, el tamaño del bloque de texto en claro es 64 o 128 bits y el bloque de texto cifrado es el mismo tamaño.

Las ventajas del cifrado en bloque son:

- Alto nivel de difusión
- Inmunidad a la manipulación: es difícil insertar símbolos sin ser detectado.

Los algoritmos de cifrado en bloque más extendidos son:

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

No se recomienda utilizar la misma clave secreta para cifrar bloques idénticos de texto en claro. Si se utiliza la misma clave para un número de bloques idénticos de texto en claro, el resultado es un número de bloques de texto cifrado idénticos. Hay maneras de encadenar y mezclar bloques de texto claro con bloques de texto cifrado que permiten evitar ataques. Estos métodos se denominan modos de operación en cifrado en bloque.

Modos de operación

El cifrado en bloque se puede utilizar en distintas modalidades, con diferentes propiedades de confidencialidad y de recuperación ante situaciones de error. Estos modos se aplican a casi todos los sistemas de cifrado de bloque existentes actualmente. La elección del modo de cifrado afecta a la velocidad, a la seguridad contra los adversarios y a la propagación de errores.

Modo ECB: Electronic Code Book

Es el modo básico de cifrado en bloque, sin ninguna modificación. El mensaje se divide en bloques, y cada bloque de texto en claro se cifra por separado, independientemente de los otros. Por lo tanto, no hay interdependencia entre bloques. Este modo no se recomienda ya que su uso presenta algunos inconvenientes:

La información estructural del texto en claro queda expuesta

Es susceptible de un ataque de modificación de orden de bloques: los bloques del texto cifrado se pueden reordenar o repetir y ese reordenamiento o repetición de bloques puede cambiar semánticamente el mensaje.

Cualquier texto cifrado, cifrado con la misma clave, se puede utilizar como material de partida para un atacante.

Un ejemplo típico de debilidad del cifrado cuando se utiliza el modo ECB es cuando se cifra una imagen (por ejemplo, un archivo .bmp). Incluso un algoritmo de cifrado robusto, cuando utiliza el modo ECB no puede desdibujar eficientemente su contenido.

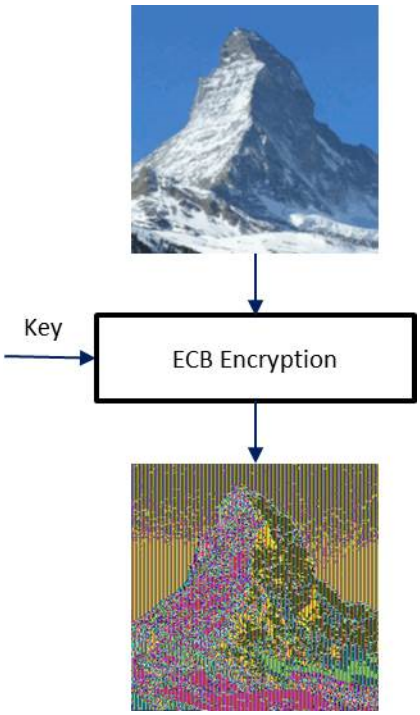


Fig 2.3 Imagen original en formato bmp y su correspondiente criptograma en modo ECB

Modo CBC: Cipher Block Chaining

El modo Cipher Block Chaining (CBC) combina ("encadena") bloques de texto en claro con los bloques de texto cifrado anteriores. Se requiere un vector inicial (IV) para combinar con el primer bloque de texto en claro.

En el proceso de cifrado, se calcula una OR exclusiva (XOR) entre el IV y el primer bloque de texto en claro antes del cifrado. El valor obtenido es cifrado y el resultado obtenido es el primer bloque de texto cifrado. Para los bloques de texto cifrado posteriores, en lugar del IV se utiliza el bloque de texto cifrado anterior. Así pues, como consecuencia de la operación de encadenamiento, el bloque de texto cifrado c_j depende del bloque de texto en claro p_j y del bloque de texto cifrado anterior c_{j-1}. Es fácil ver que esta dependencia equivale a decir que c_j depende del bloque de texto actual y de todos los precedentes.

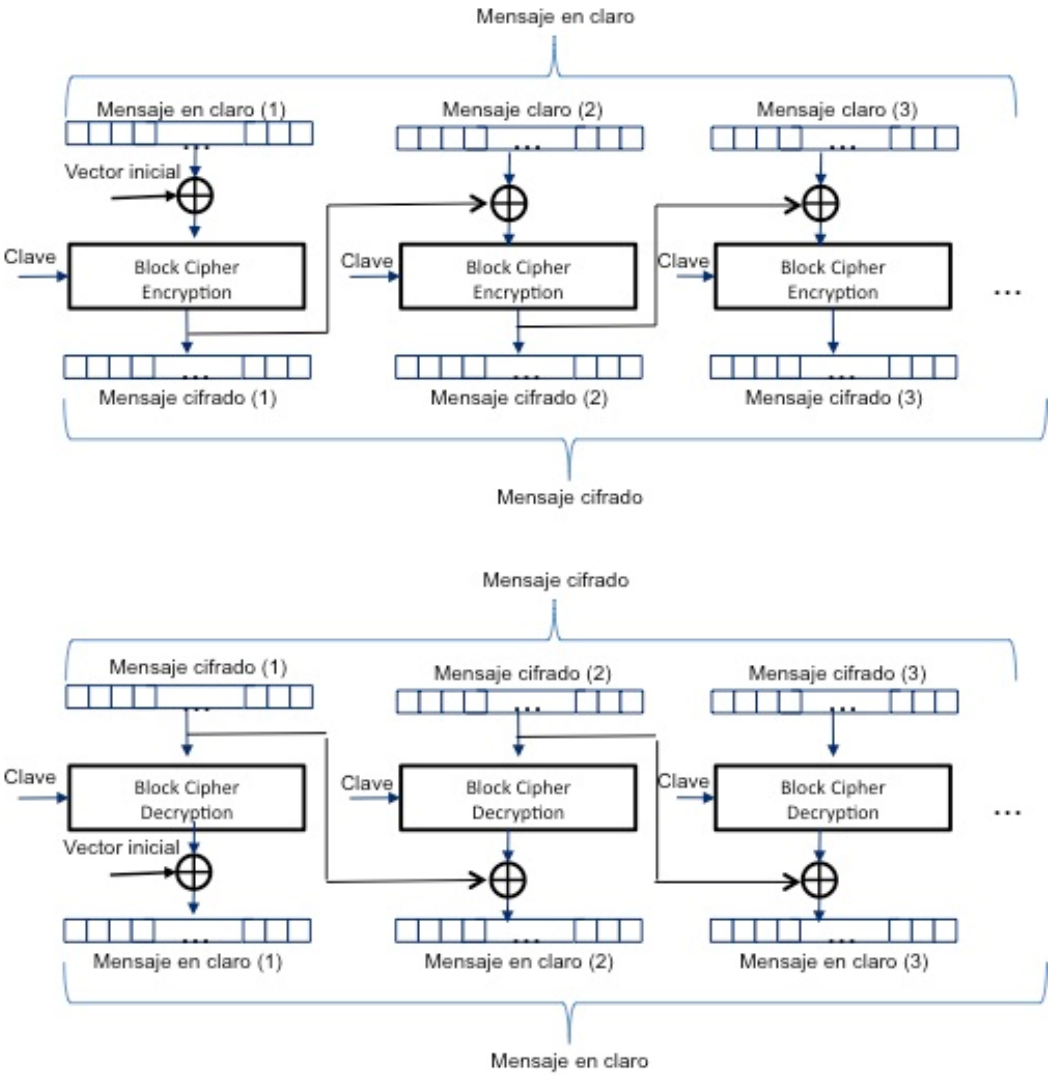


Fig 2.4 CBC: cifrado y descifrado

El uso de CBC resuelve los inconvenientes del modo ECB, pero presenta los siguientes dos inconvenientes

- No es posible paralelizar las operaciones de cifrado paralelo: no se puede cifrar el bloques p_{j+1} antes o durante el cifrado de bloque p_j, ya que se requiere conocer el valor de c_j. Sin embargo, el descifrado es paralelizable; el bloque de texto en claro p_j requiere los bloques de texto cifrado c_j y c_{j-1}.

- Propagación de errores. Un solo bit erróneo durante la transmisión de c_j provocará el descifrado incorrecto del bloque p_j, así como del siguiente bloque p_{j+1}, aunque en este último bloque sólo un bit será incorrecto. Esto se conoce como " propagación de error limitado".

Modo CFB: Cipher Feedback

El modo cipher feedback (CFB) opera de modo que el algoritmo de cifrado en bloque actúa como si fuese una unidad de cifrado en flujo generando secuencias de claves que luego son operadas mediante la función XOR con el texto en claro para

obtener el texto cifrado. Un parámetro importante en este modo de funcionamiento es *s*, un número entero tal que $1 \leq s \leq L$, siendo *L* la longitud de bloque.

El primer bloque de entrada es el IV. Básicamente, el proceso de cifrado en modo CFB toma como entrada los *L-s* bits menos significativos de la entrada anterior y los concatena con los *s* bits del texto cifrado más reciente, cifra esta nueva entrada, y se aplica una función XOR entre los *s* bits más significativos de la salida del algoritmo con los *s* bits correspondientes del texto en claro, y así se va generando el texto cifrado. La siguiente figura ilustra este modo de funcionamiento

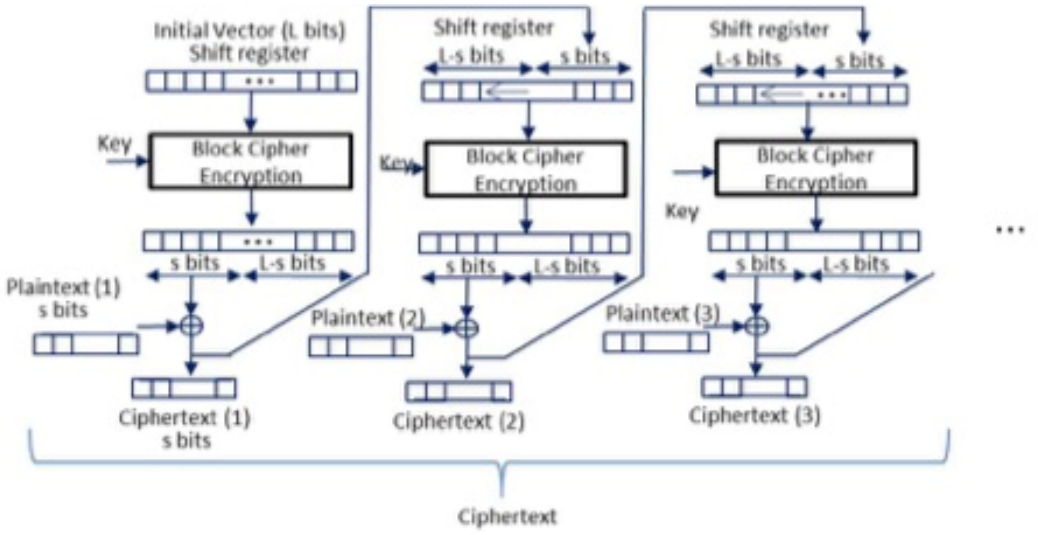


Fig 2.5 Modo de cifrado CFB

En el caso que s=1, CFB convierte el cifrado en bloque en un cifrado en flujo, cifrando bits aislados.

Respecto a la posibilidad de paralelizar este modo de operación, cabe decir que tiene las mismas limitaciones que el modo CBC; es decir, las operaciones de cifrado no se pueden realizar en paralelo, pero sí son aplicables al descifrado.

En cuanto a la propagación del error, un error en un solo bit durante la transmisión de cj afecta al bit correspondiente en p_j, pero modifica de forma significativa p_{j+1}.

Modo OFB: Output Feedback Mode

Igual que ocurre en el modo CFB, OFB utiliza el algoritmo de cifrado en bloque como un generador pseudoaleatorio, cuya salida se combina con el texto en claro mediante una función XOR para dar el texto cifrado. El modo OFB opera de la siguiente manera:

El primer bloque de entrada es el vector inicial (IV). El bloque de entrada correspondiente se cifra y los *s* bits más significativos de la salida de este cifrado se utilizan para dos funciones diferentes. Por un lado constituyen parte de la entrada del siguiente bloque, y por otra parte se combinan con los *s* bits correspondientes del texto en claro mediante una función OR exclusiva (XOR) para generar el texto cifrado. Por lo tanto, los bloques de salida sucesivos se producen a partir de la aplicación del algoritmo criptográfico a los bloques de salida anteriores, y el

resultado se combina con el texto en claro mediante la función XOR para generar el texto cifrado.

La siguiente figura ilustra el proceso

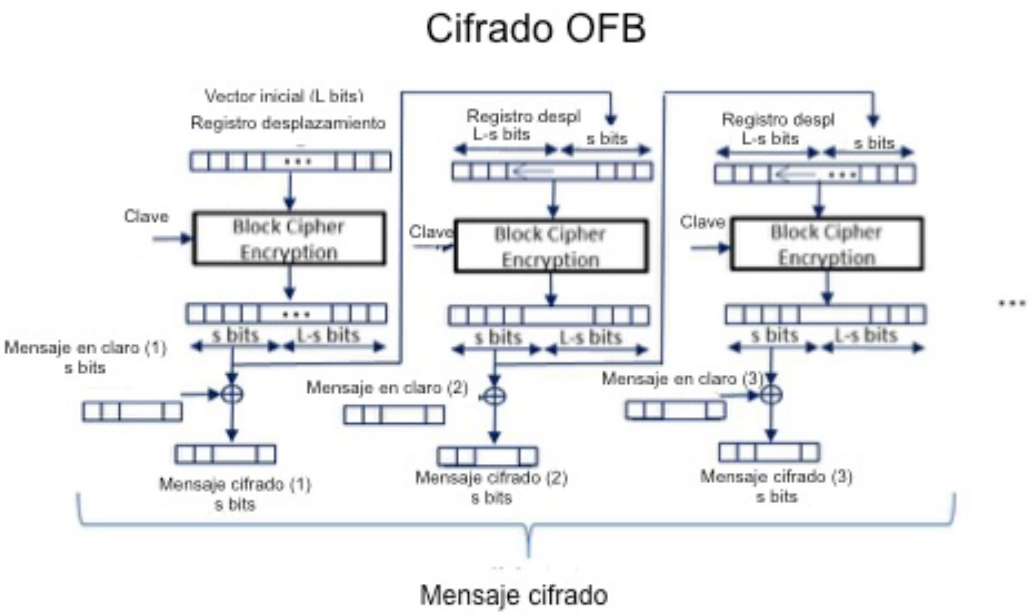


Fig 2.6 Modo de cifrado OFB

Es fácil demostrar que cuando se utiliza este modo de operación, no se propagan los errores, un error simple en la transmisión de c_j sólo afecta al bit correspondiente de p_j.

Respecto CFB, la principal ventaja de OFB es:

Si se conoce el IV, es posible preprocesar los bloques de salida antes de conocer el texto en claro (o datos de texto cifrado durante el descifrado)

Y las desventajas son:

Ni el cifrado ni el descifrado pueden realizarse en paralelo, ya que cada bloque de entrada depende de los resultados de la función de cifrado anterior.

Un atacante activo puede realizar cambios controlados en el texto en claro ya que no hay propagación de errores.

Modo CTR: Counter (contador)

Este modo se basa en el cifrado mediante un algoritmo de cifrado en bloque de un conjunto de bloques de entrada llamado contadores. Se aplica la función XOR a la salida del algoritmo de cifrado y al texto en claro, obteniéndose el texto cifrado y viceversa. En general para un mensaje, dado el bloque inicial de contador, los bloques de contador sucesivos se derivan mediante la aplicación de una función de incremento. Por lo general, el contador se divide en dos secciones: número de

mensajes y el número de bloques dentro del mensaje. Es esencial que contador nunca se repita para una clave dada. El modo CTR se ilustra en la figura siguiente.

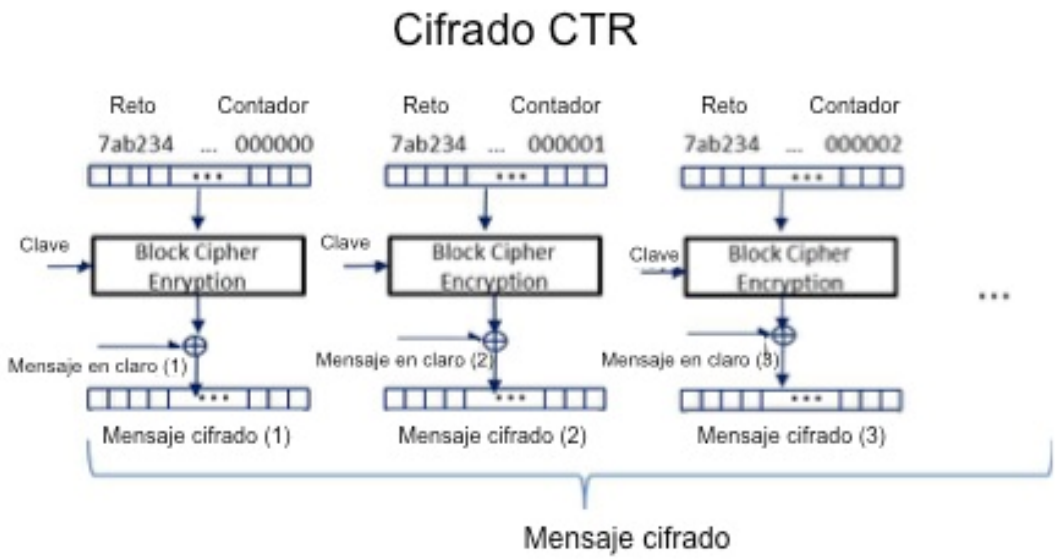


Fig 2.7 Modo de cifrado CTR

Es fácil demostrar que este modo no se propaga errores; si un bloque queda modificado debido a un error de transmisión; sólo ese bloque se descifrará erróneamente.

Las principales ventajas de este modo son:

Tanto el cifrado como el descifrado CTR son altamente paralelizables; no hay vinculación entre etapas

Es posible el preprocesado: las funciones de cifrado se pueden aplicar antes de conocer el texto en claro (o del texto cifrado en el descifrado)

El principal inconveniente es:

Un atacante activo puede hacer cambios controlados sobre el texto cifrado.

Comentarios generales

El modo CBC es el más adecuado para el cifrado en general de ficheros o de paquetes. Cuando hay requisitos importantes de alta velocidad en la operación de cifrado de datos, CTR es la mejor opción. En el caso de que la propagación de errores no sea deseable porque el canal de transmisión introduce muchos errores, OFB es una buena opción. Y, en el caso de riesgo de pérdida de un bit o byte (por problemas de sincronismo entre emisor y receptor), CFB con una $s=8$, o $s=1$ es una buena opción.

2.2 Algoritmos de cifrado en flujo

Un cifrado en flujo es un cifrado simétrico que opera con una transformación variable en el tiempo que aplica a símbolos individuales del texto en claro. Esto se logra mediante la suma lógica de símbolos de texto en claro y de una cadena de claves. La cadena de claves, también llamada clave de funcionamiento, es una secuencia pseudo-aleatoria (una secuencia que aparece como una secuencia aleatoria a un atacante) generada por un autómata de estado finito, cuyo estado inicial está determinado por una clave secreta y un parámetro público.

La seguridad de un cifrado de flujo depende totalmente de la cadena de claves. El flujo de claves debe ser impredecible para prevenir un ataque exitoso.

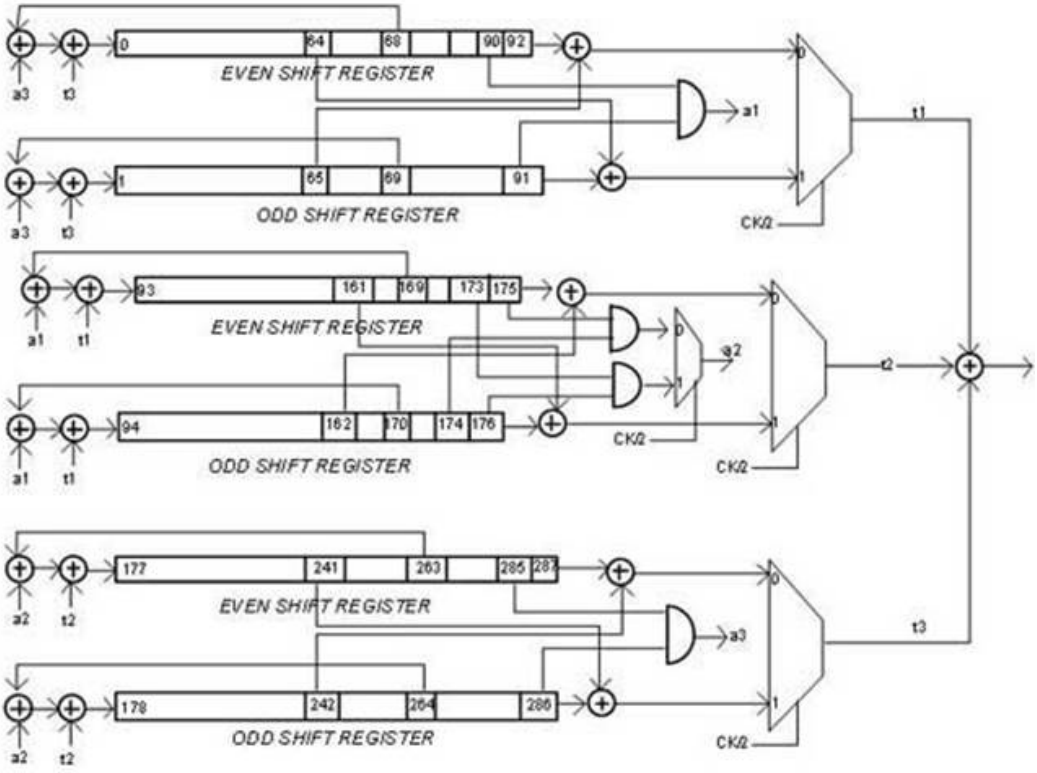


Fig 2.8 Ejemplo de cifrado en flujo: algoritmo Trivium

La implementación de esquemas de cifrado en flujo suele requerir menos recursos que los algoritmos de cifrado en bloque (ya sea en software, por ejemplo, en tamaño de código o en hardware, el área de chip), y son atractivos para su uso en entornos restringidos tales como teléfonos móviles.

En la mayoría de aplicaciones, como la seguridad en Internet, los algoritmos de cifrado en flujo son menos populares que los cifrados de bloque. Hay excepciones, por ejemplo, el algoritmo RC4.

Tipos de algoritmo de cifrado en flujo

Los algoritmos de cifrado en flujo generan elementos sucesivos de la cadena de claves a partir de un estado interno. En un cifrado en flujo síncrono, el mecanismo de actualización de estado es independiente del texto en claro y del texto cifrado. Por el contrario, los cifrados de flujo autosincronizantes actualizan su estado en base a los símbolos anteriores del texto cifrado.

Cifrado en flujo síncrono

La cadena de claves generada por el cifrado en flujo síncrono es independiente del texto en claro y del texto cifrado. Dicha cadena se genera habitualmente mediante un generador pseudoaleatorio, parametrizado con una clave, que es la clave secreta de todo el esquema.

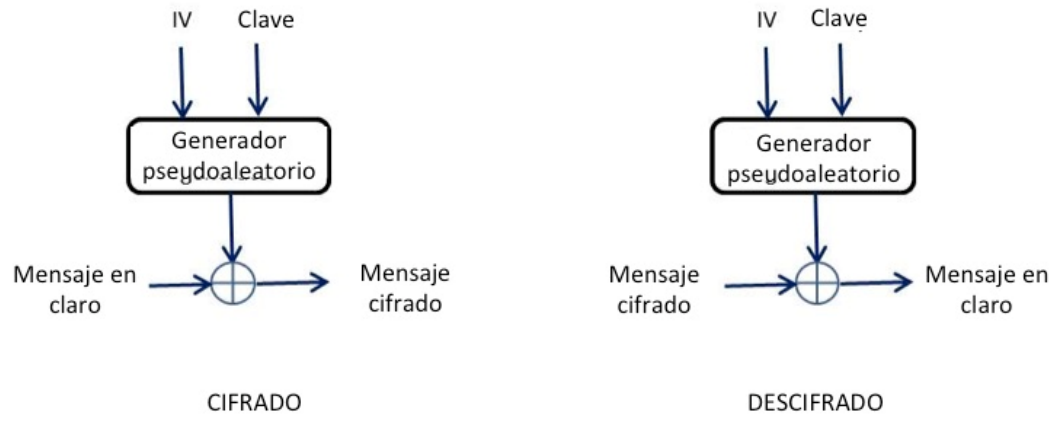


Fig 2.9 Cifrado en flujo síncrono

Algunas propiedades importantes del cifrado en flujo síncrono son:

- No hay propagación de errores: un único error de símbolo en c_j sólo afecta al símbolo p_j correspondiente. Un error de transmisión no afecta a la descodificación de otros símbolos.

- Para poder descifrar correctamente, es necesario que emisor y receptor estén perfectamente sincronizados. Si se inserta o se elimina un símbolo durante la transmisión, el emisor y receptor deberán ser resincronizados, o el resultado será incorrecto a partir de ese símbolo.

Cifrado en flujo autosincronizante

En cifrado en flujo autosincrozante, o asíncrono, el flujo de claves depende de la clave secreta del esquema y de un número fijo de símbolos de texto cifrado (que ya se han generado, o recibido).

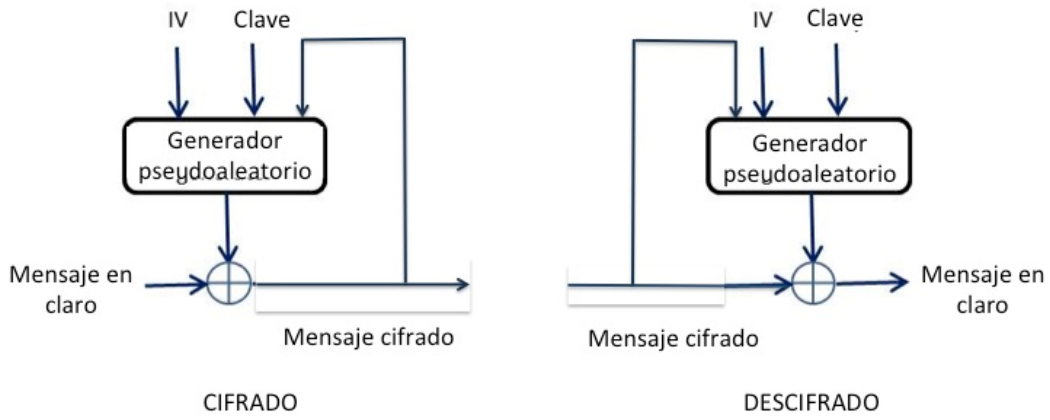


Fig 2.10 Cifrado en flujo autosincronizante

Las principales propiedades de este esquema son las siguientes:

- Auto-sincronización: si se eliminan, insertan o modifican algunos símbolos del texto cifrado, el cifrado es capaz de reanudar automáticamente el descifrado después de algunos símbolos.
- Propagación de errores limitada: el efecto de los errores de un símbolo es limitado, sólo algunos símbolos se descifran erróneamente.

3 Criptografía de clave pública

La criptografía de clave pública apareció para hacer resolver los problemas de seguridad que plantea la criptografía simétrica. Este método resuelve el problema de transmisión de claves que tiene la criptografía de clave secreta mediante el uso de dos claves en vez de una sola, utilizando una de ellas para el cifrado, y la otra para el descifrado.

Este proceso se conoce como criptografía de clave pública o criptografía asimétrica. Las dos claves utilizadas se conocen colectivamente como el par de claves. En la criptografía asimétrica, una de las claves es de libre distribución. Esta clave se denomina clave pública. Por eso, este método de cifrado también se llama el cifrado de clave pública. La segunda clave es la clave privada y como indica su propio nombre no es distribuible. Es importante señalar que las claves públicas y privadas están relacionadas, pero es prácticamente imposible deducir la clave privada si se conoce la clave pública.

Hay una debilidad básica en el cifrado de clave pública: un atacante con tiempo y potencia de cálculo suficiente podrá averiguar la clave privada a partir de una clave pública. Por esta razón el cifrado de clave pública se basa en claves muy grandes; por lo general las claves tienen 1024 o 2048 bits. Mientras más largas son las claves utilizadas (es decir, que tienen más bits), más difícil es el ataque.

Los algoritmos de criptografía de clave pública se basan en problemas matemáticos que actualmente no tienen ninguna solución eficiente. Es computacionalmente fácil para un usuario generar un par de claves (pública y privada) y usarlas para el cifrado y descifrado. Estos problemas matemáticos complejos hacen que sea extremadamente difícil determinar correctamente una clave privada a partir del conocimiento exclusivo de la clave pública. La seguridad de la criptografía de clave pública se garantiza de esta manera; la robustez del algoritmo radica en tal dificultad. Por lo tanto la clave pública puede ser publicada sin comprometer la seguridad. Seguridad depende sólo de mantener el privado clave privada. Los algoritmos de clave pública, a diferencia de los algoritmos de clave simétrica, no requieren un canal seguro para el intercambio inicial de claves entre las partes.

Dos usos comunes de la criptografía de clave pública son la confidencialidad y las firmas digitales de clave pública. La confidencialidad utilizando cifrado de clave pública se consigue cuando un mensaje secreto se cifra usando una clave pública; sólo la persona que posee la clave secreta puede descifrar y leer el mensaje secreto. La firma digital se consigue cifrando con la clave privada del emisor y puede ser verificada por cualquier persona con acceso a la clave pública del remitente. Ambas aplicaciones son ejemplos de confidencialidad y autenticidad de cifrado de clave pública.

Los algoritmos de clave pública son lentos en comparación con los simétricos. A menudo, con el fin de resolver este problema, la clave pública se utiliza para distribuir una clave simétrica. Esta clave simétrica se utiliza para cifrar la información de usuario.

Si bien el uso de criptografía de clave pública simplifica mucho la gestión de claves en comparación con la criptografía simétrica, hay una idea errónea de que la gestión

de claves es trivial con la criptografía de clave pública. Por otra parte, algunos usuarios creen erróneamente que el cifrado de criptografía de clave pública es más seguro que el cifrado simétrico frente a criptoanálisis. De hecho, la seguridad de cualquier sistema depende de la longitud de clave y el trabajo computacional involucrado en romper el cifrado.

El algoritmo de criptografía de clave pública más extendido es ***RSA.***

3.1 ¿Cómo se cifra con criptografía de clave pública?

Uso de cifrado de clave pública para proporcionar confidencialidad

Veamos un ejemplo: el Usuario_B quiere enviar un mensaje al Usuario_A. El Usuario_B cifra el mensaje con la clave pública del Usuario_A, y el Usuario_A descifra el mensaje utilizando su clave privada. Dado que los pares de claves son complementarias, sólo la clave privada del Usuario_A podría descifrar este mensaje. Si otra persona intercepta el texto cifrado, no será capaz de descifrarlo, ya que se necesita la clave privada de Usuario_A para el descifrado. Este método no proporciona autenticación, no se puede demostrar que el mensaje procede del Usuario_B, porque la clave pública de Usuario_A la puede conocer todo el mundo. Sin embargo, sí se ofrece confidencialidad al mensaje, ya que sólo Usuario_A puede descifrar el mensaje.

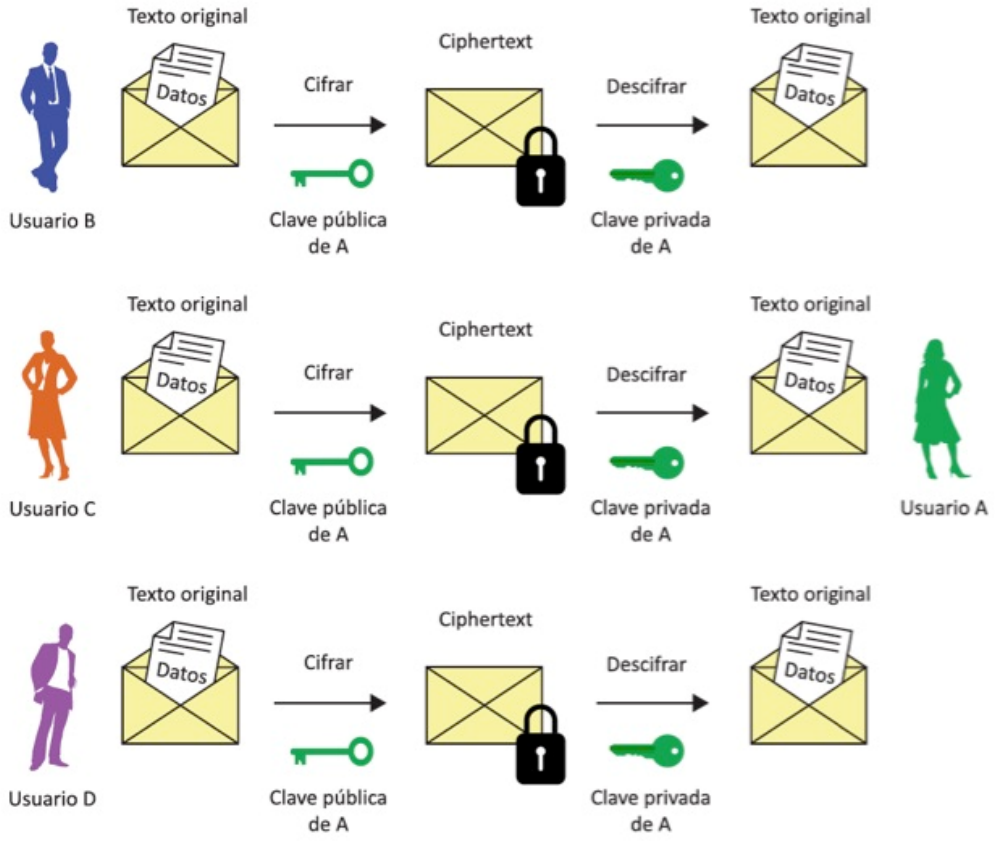


Fig 3.1 Modelo de cifrado con clave pública (para proporcionar confidencialidad)

Este método ofrece confidencialidad ya que el criptograma enviado a un usuario sólo puede ser descifrado con la clave privada del destinatario. El cifrado se realiza mediante la clave pública de dicho destinatario, de forma que desaparece el problema de la distribución de claves, ya que no se requiere la distribución o transmisión de ninguna clave secreta o privada.

Uso de cifrado de clave pública para proporcionar autenticación

Para proporcionar autenticación, el Usuario_A debe cifrar el mensaje con su clave privada y el Usuario_B deberá descifrar el mensaje con la clave pública del Usuario_A. Este método proporciona autenticación, ya que solo Usuario_A puede haber enviado ese mensaje, pero no proporciona confidencialidad ya la clave pública de Usuario_A es conocida por todos. Por lo tanto, cualquier persona que posea la clave pública de Usuario_A podría descifrar el mensaje.

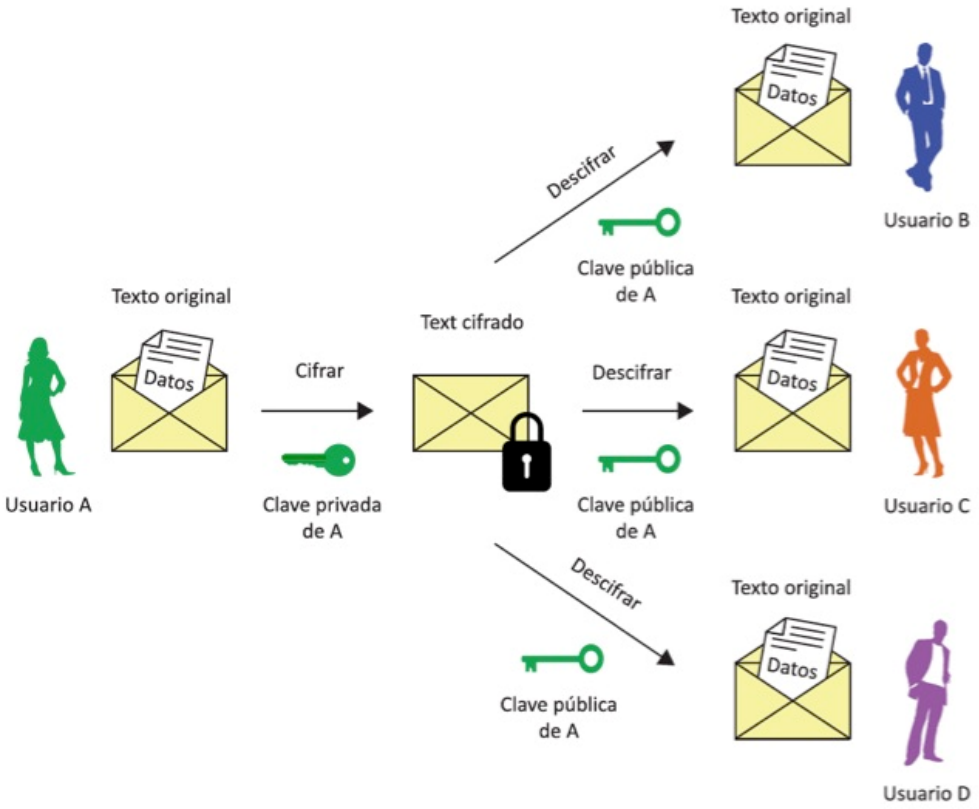


Fig 3.2 Modelo de cifrado con clave pública (para proporcionar autenticación)

Uso de cifrado de clave pública para proporcionar autenticación y confidencialidad

Para proporcionar simultáneamente confidencialidad y autenticación, Usuario_B tendrá que cifrar el texto en claro en primer lugar con su clave privada, lo cual aportará autenticidad. Posteriormente, Usuario_B volverá a cifrar utilizando la clave pública de Usuario_A para proporcionar confidencialidad.

La desventaja del sistema es que es muy lento y complejo ya que se deben realizar dos operaciones de cifrado de clave pública y posteriormente dos operaciones de descifrado. Debe tenerse en cuenta que la longitud de estas claves es grande (1024 bits a 4096 bits)

4 Sistema híbrido: Combinando Criptografía Simétrica y Asimétrica

La desventaja de utilizar cifrado de clave pública es que es un proceso bastante lento, ya que se requieren longitudes de clave grandes (1024 bits a 4096 bits). Cuando se comparan ambos procesos, el cifrado de clave simétrica es mucho más rápido, y emplea longitudes de clave más pequeñas (56 bits a 256 bits). Por otro lado, como se ha mencionado anteriormente, el uso de criptografía simétrica plantea el problema de la transferencia de clave. Ambas técnicas se pueden utilizar conjuntamente para proporcionar un mejor método de cifrado. De esta manera se puede hacer uso de las ventajas combinadas y superar las desventajas.

Específicamente, el sistema híbrido utiliza un algoritmo de clave pública con el fin de compartir de forma segura la clave usada en el sistema de cifrado simétrico. El texto en claro se cifra utilizando una clave simétrica, dando lugar al criptograma. El emisor envía el criptograma al receptor junto con la clave simétrica utilizada cifrada con la clave pública del destinatario. Dado que el método de reparto es seguro, la clave simétrica se renueva cada sesión, por eso a veces a esta clave se denomina clave de sesión. Esto significa que si un atacante es capaz de conocer la clave de sesión, sólo sería capaz de leer el mensaje cifrado con esa clave.

La clave de sesión cifrada utilizando el algoritmo de clave pública, y el criptograma, se combinan automáticamente. El destinatario usa su clave privada para descifrar la clave de sesión y, a continuación utiliza la clave de sesión para descifrar el mensaje. Muchas aplicaciones utilizan este sistema.

Los pasos que sigue una transacción utilizando una técnica combinada son:

1. Se genera una clave aleatoria y se cifra el mensaje con dicha clave utilizando criptografía simétrica, dando lugar al criptograma.

2. Se cifra esta clave aleatoria mediante criptografía de clave pública con la clave pública del destinatario

3. Se envía el criptograma junto con la clave aleatoria cifrada tal como se ha mencionado en el apartado anterior.

Esta técnica de cifrado combinado se utiliza con muchísima frecuencia. Por ejemplo, se utiliza en Secure Shell (SSH) para proteger las comunicaciones entre el cliente y el servidor y en PGP(Pretty Good Privacy) para enviar correos electrónicos. Además, es el mecanismo básico en Transport Layer Security (TLS), que es el protocolo utilizado en la Web para mantener un canal de comunicación seguro.

La siguiente figura ilustra el proceso.

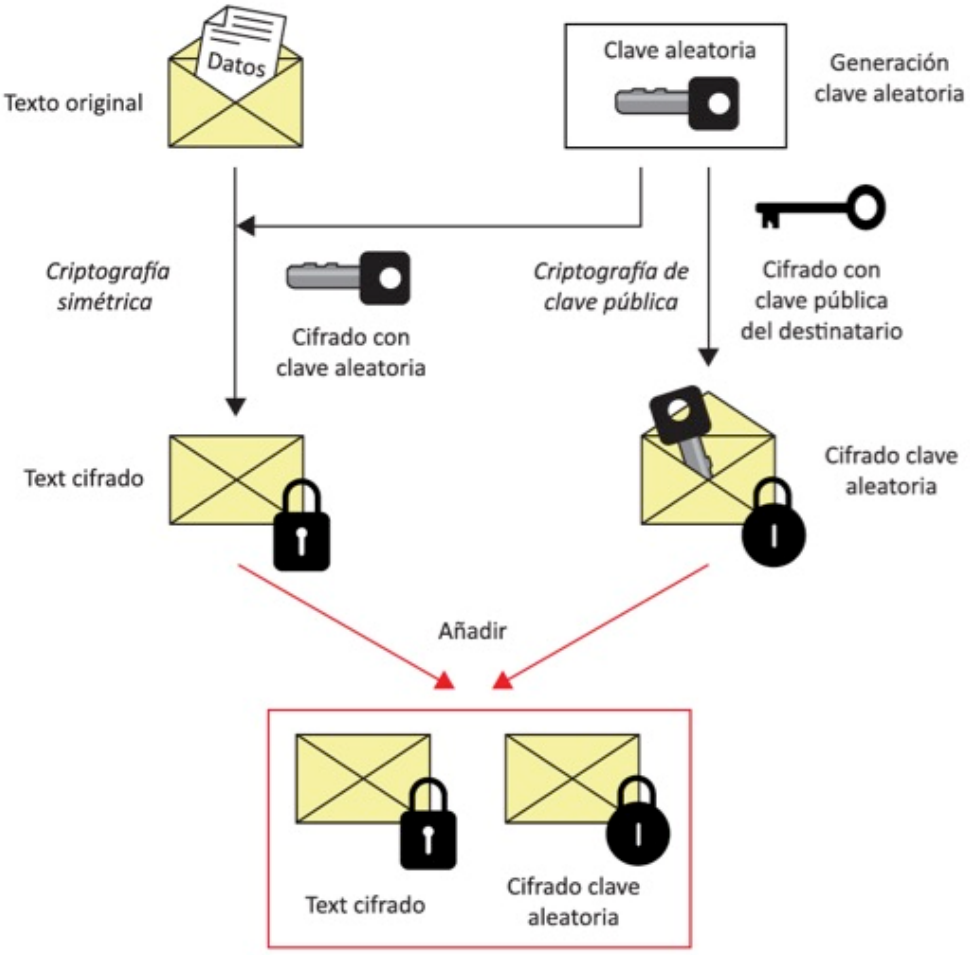


Fig 4.1 Modelo de cifrado híbrido (para proporcionar confidencialidad)

5 Funciones de hash

El término función de hash tiene su origen histórico en la informática, donde representa una función que comprime una cadena de entrada arbitraria en una cadena de longitud fija. Cualquier cambio en los datos de entrada modificará (con muy alta probabilidad) el valor hash. Las funciones hash con esta propiedad tienen una variedad de usos genéricos en computación, pero cuando se emplea en criptografía, deben satisfacer algunas propiedades adicionales. Las funciones de hash criptográficas se pueden utilizar para proporcionar integridad del mensaje, para proteger la autenticidad de la información, para proteger contra la amenaza de repudio y para preservar las contraseñas. A diferencia de los algoritmos de clave secreta y de clave pública, las funciones hash, también llamados resúmenes de mensajes, no utilizan ninguna clave criptográfica.

Los requisitos básicos para una función hash criptográfica son:

- La entrada puede tener cualquier longitud,
- La salida tiene una longitud fija,
- Es fácil calcular el valor hash para cualquier mensaje dado,
- Las funciones hash son unidireccionales, es decir, es computacionalmente imposible generar un mensaje a partir del valor de su hash
- Es computacionalmente imposible modificar un mensaje sin que su hash también se vea alterado
- Libre de colisión, es decir, es computacionalmente imposible encontrar dos mensajes diferentes (x, y), tal que $H(x) = H(y)$.

El valor de hash representa de forma concisa el documento a partir del cual se calcula. Puede pensarse en un resumen del mensaje como “huella digital” de un documento habitualmente más grande.

La principal aplicación de una función hash criptográfica es su uso en la firma digital. Además, un hash puede hacerse público sin revelar el contenido del documento a partir del cual se ha generado dicho hash.

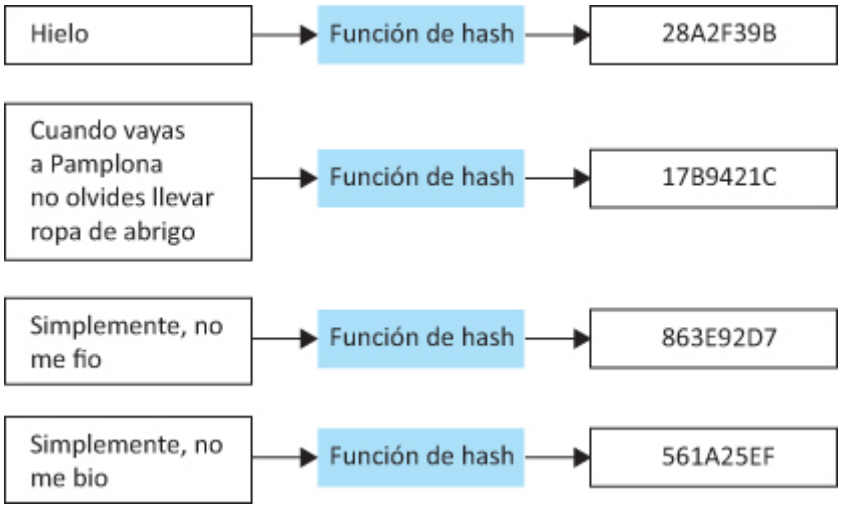


Fig 5.1 Función de hash

6 Firma digital

Las firmas digitales son uno de los desarrollos más importantes relativos al uso de criptografía de clave pública, ya que proporcionan un conjunto de capacidades que serían difíciles de implementar en cualquier otra forma. Una firma digital es una firma electrónica que se puede utilizar para autenticar la identidad del remitente de un mensaje o el firmante de un documento. Asimismo, también garantiza la integridad del mensaje. Las firmas digitales son fácilmente transportables y no pueden ser imitadas por una persona que no sea el remitente real.

Las firmas digitales se basan en las firmas manuscritas. Dichas firmas manuscritas deben satisfacer las siguientes propiedades:

- *La firma es segura* - la firma no debería ser imitada y cualquier posible intento de falsificación de la firma debe ser fácilmente detectado.
- *La firma facilita la autenticación* - la firma identifica de forma única a su autor, que firmó el documento sin ningún tipo de restricciones.
- *La firma no es transferible* - la firma es parte del documento y no puede ser transferido a otro documento.
- *El documento firmado es inalterable* - el documento no puede ser modificado después de la firma
- *La firma es irrenunciable* - el autor de la firma no puede negar posteriormente haber realizado dicha firma

En la práctica, ninguna de estas características se cumplen al cien por cien en las firmas manuscritas. Las firmas digitales también deben satisfacer todos esos requisitos. Sin embargo, aparecen nuevos problemas asociados a aspectos prácticos de la firma digital. Los documentos digitales pueden copiarse fácilmente, parte de un documento se puede transmitir a otro documento y un documento firmado se puede modificar fácilmente. Por lo tanto, se deben formular nuevos requisitos adicionales para una firma digital:

- La firma debe ser un patrón de bits que depende del mensaje firmado.
- La firma deberá utilizar información exclusiva del remitente, para impedir tanto la falsificación como la negación o repudio.
- Firmar digitalmente un documento debe ser relativamente fácil.
- La falsificación de la firma digital, ya sea elaborando un nuevo mensaje para una firma digital existente o generando una firma digital fraudulenta para un mensaje dado debe ser computacionalmente imposible.
- Almacenar una copia de un documento firmado digitalmente debe ser fácil.

Una firma digital se puede utilizar con cualquier tipo de mensaje, ya sea cifrado o no, se trata simplemente que el receptor puede estar seguro de la identidad del remitente y que el mensaje ha llegado intacto (no ha sido modificado).

Hay varios esquemas posibles para firma digital. Uno de los esquemas más aceptados se basa en las funciones hash. En este caso, si un usuario desea firmar digitalmente un documento debe seguir los siguientes pasos:

1. Calcular el hash del documento que debe ser firmado.
2. Usando criptografía de clave pública, se debe cifrar el hash calculado en el paso anterior con la clave privada del remitente para obtener la firma digital.
3. Añadir la firma digital al documento.

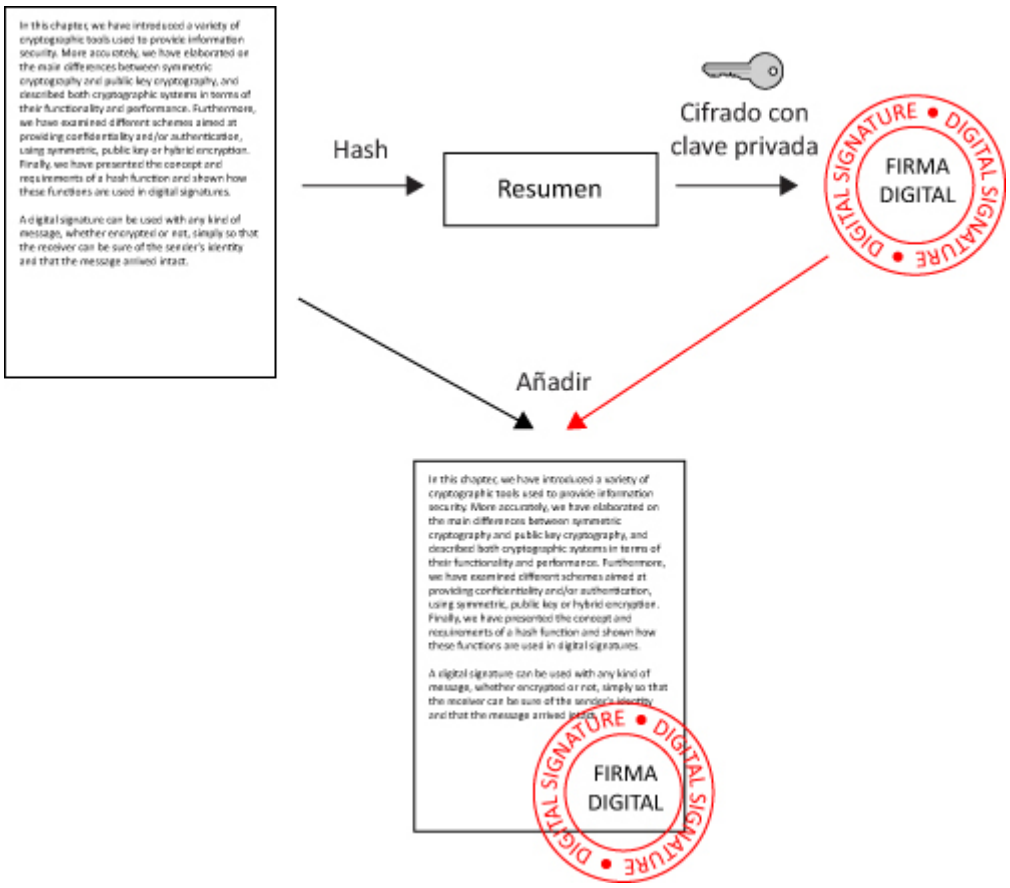


Fig 6.1 Hash based digital signature

El receptor puede verificar la autenticidad de esta firma digital siguiendo los siguientes pasos:

1. Evaluar el hash del documento (excluyendo la parte de firma digital).
2. Usando criptografía de clave pública, descifrar la firma digital con la clave pública del remitente para obtener el hash del mensaje.
3. Comparar los resultados obtenidos en los dos pasos.

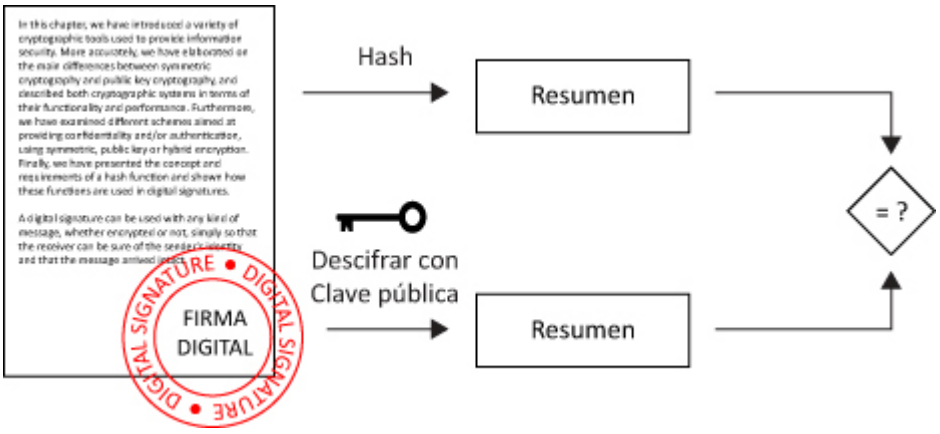


Fig 6.2 Proceso de verificación de una firma digital basada en hash

Si los valores de hash obtenidos en los dos pasos son iguales, el destinatario sabe que los datos firmados no han sido modificados, y por tanto, la firma es correcta.

7 Intercambio de claves. Certificados digitales

Una de las principales aplicaciones de la criptografía de clave pública son las firmas digitales. Una correcta aplicación de firma digital permite al receptor de un documento firmado digitalmente tener la certeza que el mensaje fue enviado por el supuesto remitente. En muchos aspectos, la firma digital es equivalente a la firma manuscrita tradicional, pero una implantación práctica adecuada de la firma digital hace que sea más robusta y difícil de falsificar que la firma manuscrita. Para poder verificar una firma digital es necesario conocer la clave pública del remitente. Por lo tanto, es totalmente necesario un mecanismo de distribución de claves.

El enfoque más aceptado para la distribución de claves se basa en el uso de certificados digitales.

Un certificado digital es un documento electrónico que se utiliza para identificar a un individuo, un servidor, una empresa, o alguna otra entidad y asociar esa identidad con una clave pública. Incorpora una firma digital que vincula la clave pública con una identidad - información tal como el nombre de una persona u organización, dirección, ... El certificado se puede utilizar para verificar que una clave pública pertenece a un individuo. Los certificados ayudan a prevenir el uso de claves públicas falsas para la suplantación. Sólo la clave pública certificada por el certificado se corresponde con la clave privada que posee la entidad identificada por el certificado. Un certificado digital es un documento electrónico que incorpora una firma digital para vincular una clave pública con una identidad - el nombre de una persona o una organización.

Un certificado digital es una estructura de datos que contiene la clave pública de un usuario o entidad (propietario del certificado), así como los datos de identificación del titular del certificado y una marca relacionada con la validez del certificado. Esta estructura se firma con la clave privada de una entidad de confianza denominada autoridad de certificación (CA). Cada usuario es capaz de verificar la autenticidad del contenido del certificado utilizando la clave pública de la autoridad de certificación.

La siguiente figura muestra la estructura de un certificado digital:

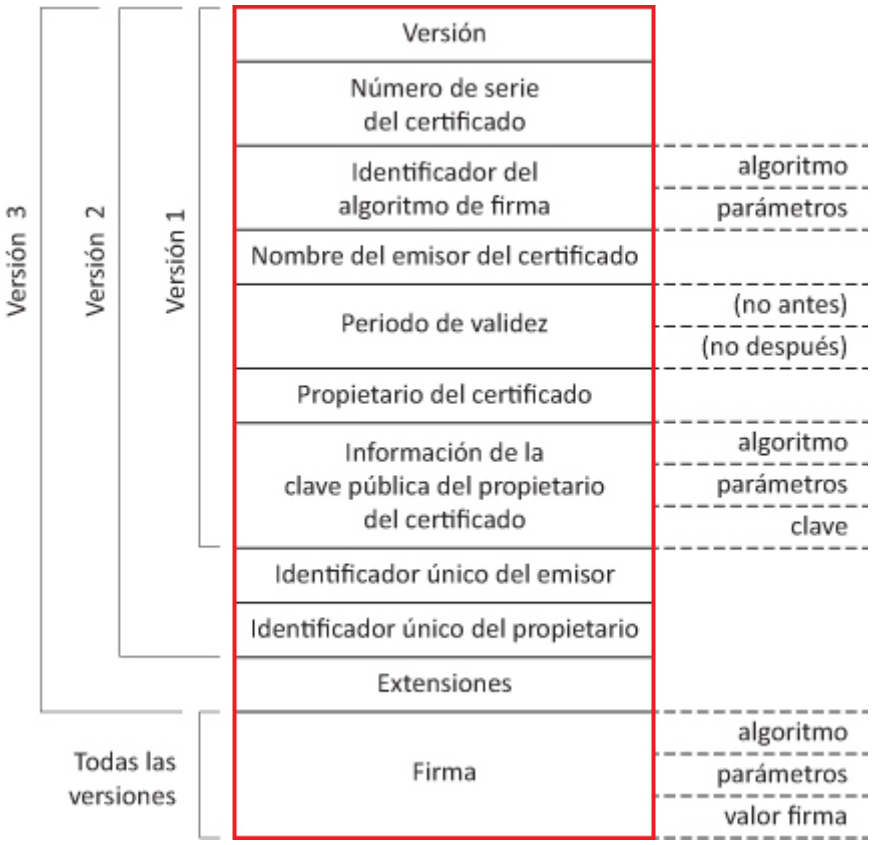


Fig 7.1 Estructura de un certificado digital

8 Ciberdelincuencia: Introducción

La ciberdelincuencia o delito informático es cualquier actividad delictiva que implica el uso de ordenadores y redes de telecomunicación. El rango de actuación va desde los correos electrónicos no solicitados (spam) al fraude. Estos casos de delitos incluyen ataques contra los datos almacenados en ordenadores y equipos de comunicación, robo de identidad, distribución de imágenes de abuso sexual infantil, fraude en Internet, penetración en servicios financieros en línea, así como el despliegue de los virus, botnets, y varias estafas por correo electrónico como el phishing.

Una de las mejores maneras de evitar ser víctima de delitos informáticos y proteger la información sensible es mediante el uso de un sistema unificado de software y hardware para autenticar cualquier información que se envía o se accede a través de Internet.

Los delitos cibernéticos se definen como: "Los delitos que se cometen contra personas o grupos de personas con la intención de dañar la reputación de la víctima o causan daños a la víctima directa o indirectamente usando redes de telecomunicación. Tales delitos pueden poner en peligro la seguridad y la estabilidad económica de una institución. Los temas relacionados con este tipo de delitos se han convertido de alto riesgo, en particular los que rodean el robo de identidad, delitos de derechos de autor, la pornografía infantil, ... También hay problemas de privacidad cuando se distribuye de forma ilegal información confidencial.

Es importante ser consciente de que es casi imposible reconocer todas las actividades de delitos cibernéticos antes que afecten a las entidades objeto de ataque. Por esta razón, es fundamental contar con un enfoque de seguridad cibernética que haga hincapié en los aspectos de la detección y recuperación temprana.

Un procedimiento de respuesta a incidentes eficaz incluye los siguientes pasos:

- Identificación de la amenaza que afecta a la infraestructura.
- Contención de la amenaza, evitando que se propague dentro de la infraestructura objeto de ataque.
- Las investigaciones forenses para identificar los sistemas afectados y la forma en que la amenaza ha penetrado en el sistema informático.
- Remediar/recuperar mediante la restauración de la infraestructura de tecnología de información y su puesta en marcha de nuevo en línea una vez se haya completado la investigación forense.
- Informar y compartir información sobre el impacto con la dirección y distribuir la información de la amenaza y los datos a través de plataformas dedicadas que permiten el intercambio rápido de datos de amenazas con la policía y otras empresas.

Desafortunadamente, el proceso descrito raramente se sigue. Hasta ahora, el proceso de contención y remedio es un proceso manual primario y habitualmente, no demasiado eficiente.

9 Técnicas de ataque

Los ataques a las redes pueden ser definidos como diferentes tipos de actividades sistemáticas dirigidas a disminuir o corromper su seguridad. Desde este punto de vista, un ataque puede ser definido como una amenaza sistemática generada por una entidad de una manera artificial, deliberada e inteligente. Las redes de ordenadores pueden ser vulnerables a muchas amenazas utilizando distintas formas de ataque, entre ellas:

- Ingeniería social, alguien trata de acceder usando medios sociales (haciéndose pasar por un usuario legítimo o el administrador del sistema, engañando a la gente para que le revelen secretos o claves, etc.). Esta forma de ataque suele dar muchos resultados a los atacantes.

- Ataques de denegación de servicio, incluyendo todos los tipos de ataques destinados a saturar a un ordenador o a una red, de tal manera que los usuarios legítimos no puede utilizarla

- Ataques a determinados protocolos, aprovechando debilidades conocidas.

- Ataques a servidores, que aprovechan las vulnerabilidades de ciertos sistemas operativos de los ordenadores o vulnerabilidades en la configuración y administración del sistema.

- Adivinar contraseñas; las contraseñas son secuencias de símbolos, generalmente asociadas a un nombre de usuario, que proporcionan un mecanismo para la identificación y la autenticación de un usuario en particular. En casi todos los servicios son los propios usuarios quienes eligen sus contraseñas, y con frecuencia eligen secuencias que no pueden ser consideradas seguras (por ejemplo, nombre de la pareja , nombre de hijo/hija, fechas de nacimiento, …) Como regla general, las contraseñas que son fáciles de recordar son también fáciles de adivinar.

- Espionaje de todo tipo, incluyendo la captura de mensajes de correo electrónico, archivos, contraseñas y otra información a través de una conexión de red que permite capturar todos los mensajes de un usuario.

Los ataques de seguridad pueden clasificarse en:

- Ataques pasivos.

- Ataques activos.

9.1 Ataques pasivos

Un ataque pasivo es aquél en que el atacante monitoriza el canal de comunicación sin modificar ni añadir datos. Un atacante pasivo sólo pone en peligro la confidencialidad de los datos. El objetivo del atacante es obtener la información que se está transmitiendo.

Los ataques pasivos están relacionados con el contenido del mensaje y con el análisis de tráfico:

- Espionaje. En general, la mayoría de la información que se transmite utilizando una red de comunicaciones se envía de forma no segura (sin cifrar) permitiendo a un atacante "escuchar" o interpretar (leer) los datos intercambiados. Uno de los mayores problemas a los que se enfrenta un administrador de una red deriva de la capacidad de un atacante para monitorizarla. Sin servicios de cifrado (basados en el uso de técnicas criptográficas), los datos pueden ser leídos por otras personas a medida que circulan por la red.

- Análisis de tráfico. Se refiere al proceso de interceptar y examinar los mensajes con el fin de deducir información de patrones en la comunicación. Se puede realizar incluso cuando los mensajes están cifrados. En general, cuanto mayor es el número de mensajes observados, interceptados y almacenados, más se puede inferir del tráfico. El análisis de tráfico permite a un atacante, entre otras cosas, verificar que dos entidades están manteniendo una comunicación en un determinado momento.

9.2 Ataques activos

Un ataque activo intenta alterar los recursos del sistema o afectar a su funcionamiento. En este tipo de ataque el adversario intenta borrar, añadir, o modificar los datos transmitidos. Un atacante activo amenaza la integridad de datos y autenticación, así como la confidencialidad.

Los ataques activos engloban alguna modificación del flujo de datos o la creación de datos falsos. Pueden dividirse en seis categorías:

- Suplantación de identidad. Es un tipo de ataque en el que el atacante suplanta la identidad de otro usuario.

- Repetición. En este tipo de ataque, una transmisión de datos válida es repetida o retardada de forma maliciosa. Este ataque lo puede provocar el mismo emisor de datos originales o bien un atacante que los intercepta y posteriormente los retransmite, posiblemente como parte de un ataque de suplantación de identidad.

- Modificación de mensajes. El atacante elimina un mensaje que atraviesa la red, lo altera, y lo reinserta.

- Hombre en el medio (*Man in the Middle*, **MitM**). En este tipo de ataques, un atacante intercepta las comunicaciones entre dos entidades, por ejemplo entre un usuario y un sitio web. El atacante puede utilizar la información que consigue para luego suplantar la identidad del usuario o realizar cualquier otro tipo de fraude.

- Denegación de Servicio (*Denial of Service* **DoS**) y Denegación de Servicio Distribuida (*Distributed Denial of Service*, **DDoS**). Una denegación de servicio (DoS) es una situación en la que un usuario u organización se ve privado de los servicios o recursos que normalmente debería tener. En denegación de servicio distribuida, un gran número de sistemas comprometidos (a veces llamado botnet) atacan a un solo objetivo.

- Amenazas Avanzadas Persistentes (*Advanced Persistent Threat*, **APT**). Es un ataque a la red en el que un atacante consigue un acceso no autorizado a la red y permanece allí sin ser detectado durante un largo período de tiempo. La principal intención de un ataque APT es robar datos más que causar daños a la red u organización. Algunas organizaciones que pueden ser objetivo de ataques APT son sectores con alto valor informativo, como la defensa nacional, la industria financiera.

10 Consejos de prevención

La prevención del delito cibernético puede ser directa; muchos ataques pueden ser evitados si se dispone de asesoría técnica y sentido común. En general, los atacantes de red tratan de conseguir dinero o los recursos que desean tener, de la forma más rápida y sencilla. Mientras más difícil sea hacer un ataque, mayor es la probabilidad que se busque un objetivo más fácil. Probablemente, la mejor línea de defensa sigue siendo el usuario final. La probabilidad que un usuario sea víctima de un ataque informático crece a medida que aumentan los riesgos asumidos. A continuación se muestran una serie de consejos que proporcionan información básica para prevenir el fraude en la red.

- Mantener el sistema informático actualizado con los últimos parches y actualizaciones. Los vendedores suelen entregar parches para su software cuando se descubre una vulnerabilidad. Una de las mejores maneras de mantener a los atacantes lejos de un equipo es aplicar todos los parches y correcciones de software cuando estén disponibles. La mayoría de productos ofrecen un método para obtener actualizaciones y parches. Algunas aplicaciones comprueban automáticamente si hay actualizaciones disponibles, en caso contrario, es absolutamente necesario comprobar periódicamente si hay actualizaciones. En cualquier caso, mediante la actualización periódica de un ordenador se consigue bloquear aquellos ataques que se aprovechan los fallos de software (vulnerabilidades); de otro modo los atacantes podrían utilizar las vulnerabilidades para entrar en el sistema. Asimismo, debe indicarse que mantener un equipo actualizado no lo protege frente a cualquier tipo de ataque, pero dificulta considerablemente su acceso a atacantes ya que se bloquean totalmente muchos ataques básicos y automatizados, y puede ser suficiente para disuadir a un determinado tipo de atacante que buscará equipos más vulnerables.

- Asegurar que el equipo está configurado de forma segura. La instalación de un sistema tal como se saca de su envoltorio y dejándolo con la configuración por defecto es, probablemente, uno de los errores más comunes cuando se crea una red. Cuando un equipo está instalado, es importante prestar atención no sólo a que ejecute correctamente sus funciones, sino también a que funcione de forma segura. Las configuraciones por defecto a menudo tienen cuentas administrativas predeterminadas y contraseñas que conocen muchísimos atacantes potenciales. Asimismo, es fundamental una correcta configuración de aplicaciones como navegadores de Internet y software de correo electrónico.

- Elegir contraseñas fuertes y mantenerlas protegidas. Las contraseñas son, en algunas ocasiones la única protección utilizada en un sistema. Una identidad de usuario es solamente un nombre y no verifica la identificación; se suele utilizar la contraseña asociada para verificar la identidad del usuario correspondiente. Los firewalls y los sistemas de detección de intrusos no sirven para nada si sus contraseñas están comprometidas. Una contraseña segura es la que no se encuentra en ningún diccionario.

- Proteger el ordenador con software de seguridad. Existen varios tipos de software de seguridad, incluyendo cortafuegos y antivirus que son necesarios para conseguir un nivel básico de seguridad en red. Un cortafuegos es un

software o hardware que filtra la información que entra y sale del equipo para garantizar que se bloquean todos los accesos no autorizados al sistema, proporcionando de esta manera la primera línea de defensa. En muchas ocasiones, la siguiente línea de defensa es el software antivirus, utilizado para analizar los archivos e identificar y eliminar virus informáticos así como otros programas maliciosos (malware). En sentido estricto, un virus es un programa que puede replicarse a sí mismo y está diseñado para propagarse de un ordenador a otro, realizando procesos que el usuario final desconoce y muy posiblemente no desea. El malware es un término más amplio, acrónimo de software malicioso, incluyendo virus, troyanos, keyloggers, gusanos, adware y software espía, entre otros.

- Proteger la información personal. El robo de identidad se ha convertido en un problema importante, por ejemplo para transacciones y servicios bancarios a través de Internet. En este tipo de delito cibernético, un atacante accede a datos relativos a la cuenta bancaria de una persona, tarjetas de crédito, tarjeta de débito y otra información crítica para desviar dinero o para comprar cosas en nombre de la víctima, usando la red. Puede ocasionar importantes pérdidas económicas para la víctima e incluso arruinar su historial de crédito. Por lo tanto, se recomienda precaución al compartir información personal en la red.