SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

4.1.3.MF0489_3. Capítulo 1
Parte 3
Criptografía

JOSÉ PABLO HERNÁNDEZ

8. ALGORITMOS CRIPTOGRÁFICOS MÁS FRECUENTEMENTE UTILIZADOS

Criptografía de clave privada

- **DES**
- **Triple DES**
- **AES**
- **IDEA**
- **Blowfish**

Criptografía de clave pública:

- **RSA**
- **El Gamal**

8.1. ALGORITMOS DE CRIPTOGRAFÍA DE CLAVE SECRETA

Data Encryption Standard (DES)

Este algoritmo es uno de los más utilizados.

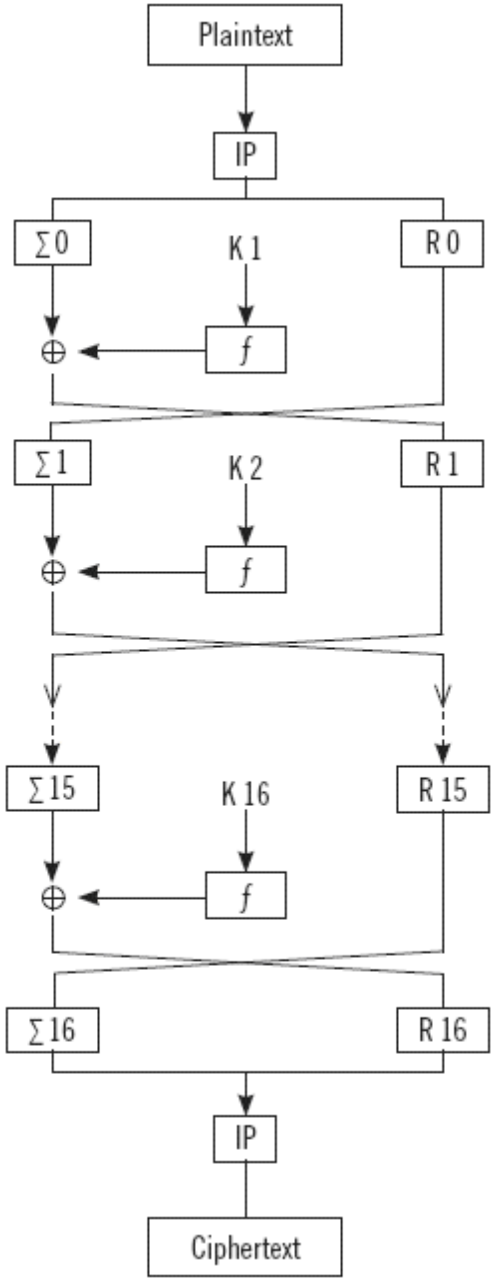
Fue adoptado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) en 1977.

En 1998 DES fue atacado en 56 horas en un primer momento y en 22 horas posteriormente (DES cracker), surgiendo la necesidad de crear un algoritmo más robusto.

En 2001 este algoritmo es sustituido por AES.

8.1. ALGORITMOS DE CRIPTOGRAFÍA DE CLAVE SECRETA

Data Encryption Standard (DES)



8.1. ALGORITMOS DE CRIPTOGRAFÍA DE CLAVE SECRETA

Triple DES

En 1999 se crea Triple DES, que consiste en el encadenamiento de tres funciones DES.

Particularmente, su forma más común está basada en el uso de dos claves, de forma que se cifra con la primera, el resultado se descifra con la segunda y a su vez el resultado se cifra con la primera.

8.1. ALGORITMOS DE CRIPTOGRAFÍA DE CLAVE SECRETA

International Data Encryption Algorithm (IDEA)

IDEA, creado en 1991, tenía como objetivo reemplazar al algoritmo DES.

Es un cifrador de bloque que opera sobre bloques de 64 bits, claves de 128 bits y un total de 8 rondas.

8.1. ALGORITMOS DE CRIPTOGRAFÍA DE CLAVE SECRETA

Blowfish

Se desarrolló en 1993 con el objetivo de reemplazar al algoritmo DES o IDEA, pero no llegó a convertirse en estándar.

Actualmente Blowfish es un algoritmo público que está a disposición de los usuarios.

Blowfish es un cifrador de bloque que opera sobre bloques de 64 bits con unos tamaños de claves desde 32 a 448 bits.

8.1. ALGORITMOS DE CRIPTOGRAFÍA DE CLAVE SECRETA

Advanced Encryption Standard (AES)

Como mejora de DES y Triple DES se propone AES, basado en el algoritmo Rijndael.

Este algoritmo fue escogido en 2001 por el NIST como el nuevo estándar para comunicaciones gubernamentales, transferencias de fondos bancarios, comunicaciones por satélite y software libre.

8.1. ALGORITMOS DE CRIPTOGRAFÍA DE CLAVE SECRETA

Advanced Encryption Standard (AES)

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

8.2. ALGORITMOS DE CRIPTOGRAFÍA DE CLAVE PÚBLICA

RSA

Este algoritmo fue creado en 1978 por Rivest, Shamir y Adleman, de donde proviene el nombre RSA, y destaca por ser el primer algoritmo efectivo de clave pública.

RSA utiliza el mismo algoritmo tanto para el cifrado como para la firma electrónica.

En ambos casos, el proceso utiliza la clave pública para una operación (envío de mensajes cifrados / verificación de la firma) y la privada para la contraria (descifrado de mensajes / realización de una firma).

8.2. ALGORITMOS DE CRIPTOGRAFÍA DE CLAVE PÚBLICA

RSA

Suponiendo que A quiere mandar un mensaje cifrado a B, el proceso de ejecución es el siguiente:

- A escoge dos números primos muy grandes y no públicos, p y q, de modo que obtiene $n=p \cdot q$.

  A escoge un número entero e que sea primo relativo con ø(n).

  A escoge un número d tal que $e \cdot d = 1 \bmod(ø(n))$

  La clave pública de A es (e, n), mientras que la clave privada es (d, n). A distribuye su clave pública utilizando cualquiera de los mecanismos de distribución de claves públicas.
- B envía un mensaje cifrado (que llamaremos M) a A, C = M^e mod(n). Recuérdese que esta operación se realiza, primero, multiplicando el mensaje por sí mismo tantas veces como indique "e" y, posteriormente, se obtiene el resto de dividir el resultado por el número "n". Es importante resaltar que el mensaje M tiene que ser numérico, por lo que si fuese un texto será necesario representarlo como número.
- A descifra el mensaje haciendo uso de la clave privada, M = C^d mod(n)

8.2. ALGORITMOS DE CRIPTOGRAFÍA DE CLAVE PÚBLICA

El Gamal

Es un algoritmo basado en el protocolo de intercambio de claves Diffie-Hellman.

Fue creado en 1984.

El Gamal se basa en el problema del logaritmo discreto y puede utilizarse tanto para cifrar como para firmar, aunque los algoritmos son distintos.

La principal diferencia frente a RSA radica en que en El Gamal cada operación de cifrado sobre el mismo dato produce un resultado distinto, lo que complica el criptoanálisis.

8.3. ALGORITMOS HÍBRIDOS

Estos algoritmos están basados en la aplicación de un algoritmo de clave pública y otro de clave privada.

Asumiendo que se desea enviar un mensaje desde A a B, el proceso de ejecución consiste en los siguientes pasos:

- A cifra un mensaje utilizando un algoritmo de cifrado de clave privada, como por ejemplo DES.
- La clave utilizada en el paso anterior (representada por Ks) se cifra utilizando un algoritmo de clave pública (como RSA) usando la clave pública de B.
- A envía el resultado de ambas operaciones a B.
- B descifra primero la clave simétrica Ks haciendo uso de su clave privada. Posteriormente, utiliza Ks para descifrar el mensaje.

8.4. ROBUSTEZ Y EFICIENCIA PRÁCTICA DE LOS ALGORITMOS

Vulnerabilidades del software

No es extraño encontrar boletines de seguridad que describan la existencia de un error de programación o de configuración que da lugar a la creación de un procedimiento que pone en riesgo la seguridad del algoritmo.

Cuando esto sucede, se dice que esa implementación es vulnerable a uno o varios ataques, con lo que la seguridad efectiva que ofrece es inferior a la que teóricamente proporciona la especificación.

Para dar un nombre uniforme a los errores con independencia de quien lo descubra y permitir que se sepa si están o no resueltos, existen listas que les otorgan un código único. Entre ellas, una de las más conocidas es la Common Vulnerability Exposure (CVE), mantenida por la organización MITRE.

8.4. ROBUSTEZ Y EFICIENCIA PRÁCTICA DE LOS ALGORITMOS

Gestión de claves

Otra de las cuestiones que suelen provocar incidentes es la inadecuada gestión de las claves.

Algunos algoritmos de cifrado simétrico no utilizan la clave proporcionada por el usuario. En su lugar, utilizan el resultado de aplicar sobre dicha clave algún proceso, que habitualmente es una función resumen (HASH).

Otros programas que hacen uso de cifrado incorporan la clave en su interior. De este modo, es posible que un atacante suficientemente preparado pueda extraer dicha clave del código del programa.

8.4. ROBUSTEZ Y EFICIENCIA PRÁCTICA DE LOS ALGORITMOS

Relevancia de la auditoría y certificación

Con el fin de garantizar que un determinado programa hace lo que debe hacer, en los últimos tiempos se está generalizando la realización de auditorías sobre el código del programa.

Dado que una parte significativa de algoritmos criptográficos están descritos en sus respectivas normas (e.g. estándares ISO, FIPS, etc.) permite que se pueda realizar una verificación objetiva del funcionamiento.

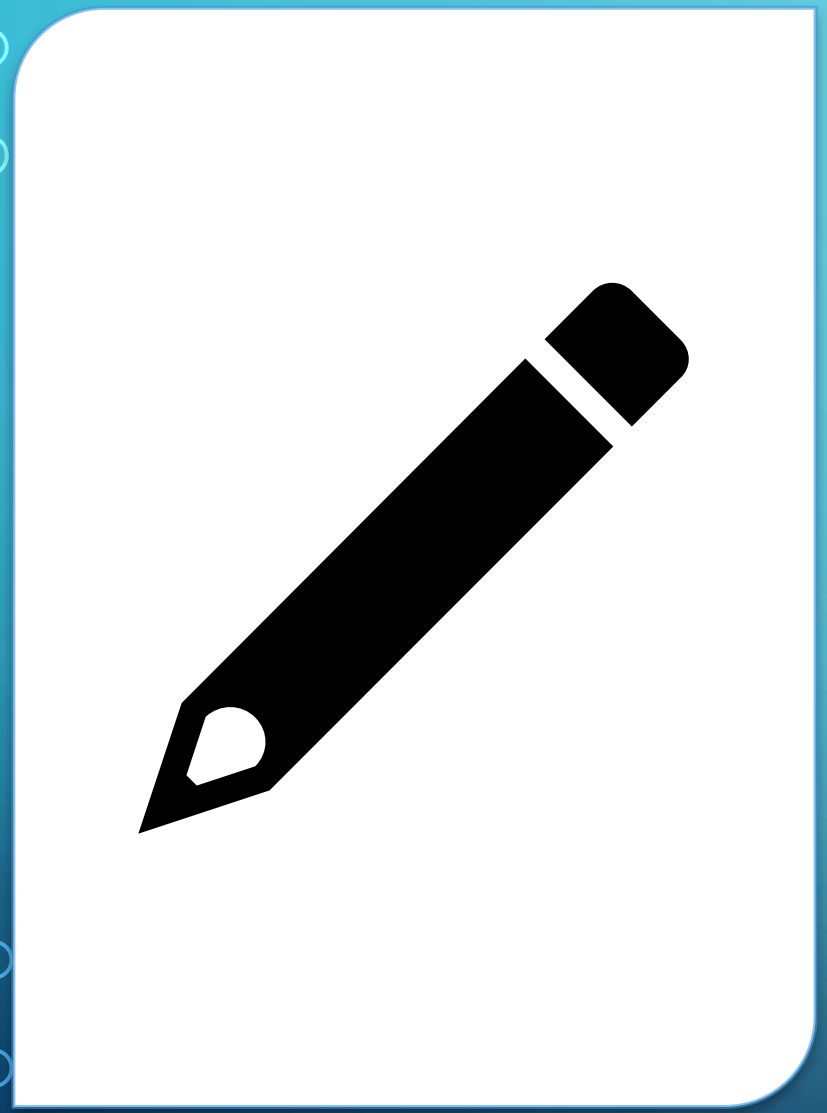
8.4. ROBUSTEZ Y EFICIENCIA PRÁCTICA DE LOS ALGORITMOS

Eficiencia práctica

La utilización práctica de estos algoritmos está sujeta en buena medida a su eficiencia computacional.

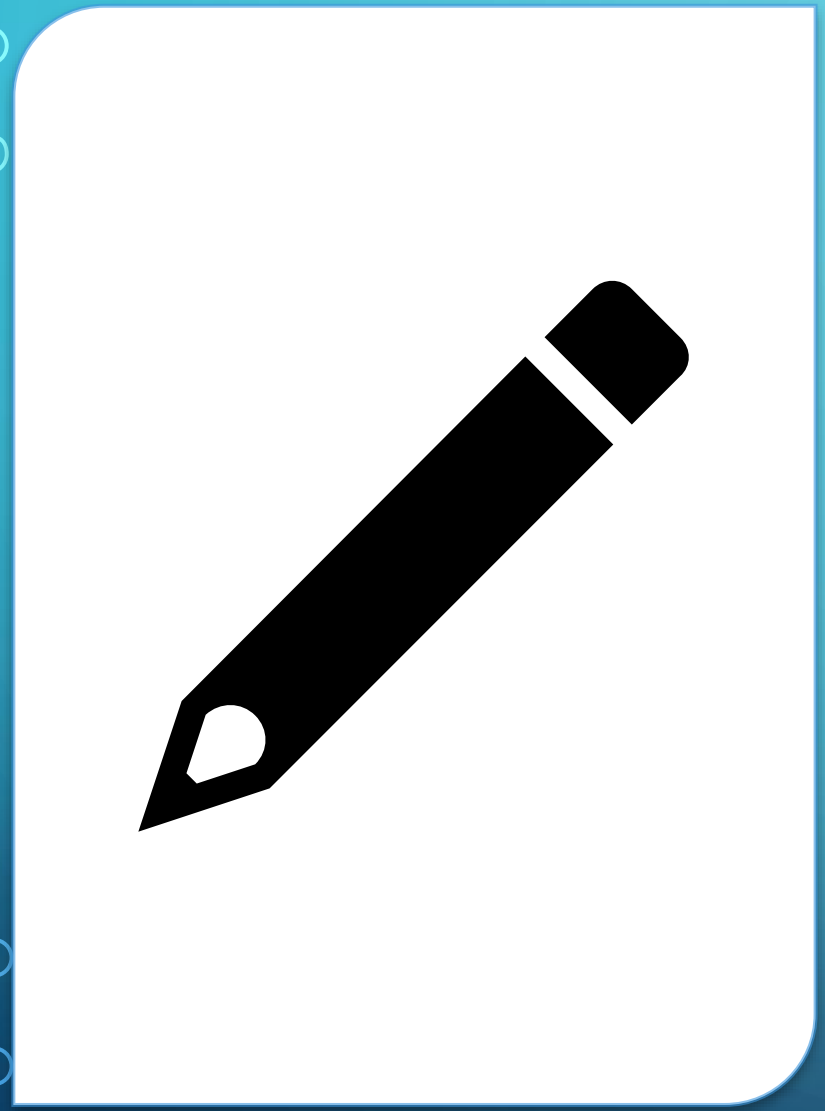
Debe consumir pocos recursos computacionales (memoria, procesador), ejecutarse en poco tiempo y, en dispositivos con batería reducida (e.g. teléfonos móviles), debe emplear una cantidad moderada de energía.

Implementación física.



Ejemplo.

UNA EMPRESA FARMACÉUTICA ESPAÑOLA HA DESARROLLADO UNAS PASTILLAS CONTRA LA CAÍDA CAPILAR. SIN EMBARGO, EN ESPAÑA NO DISPONE DE FÁBRICAS DONDE REALIZAR LA PRODUCCIÓN Y HA COMPRADO UNA FÁBRICA EN HOLANDA. LA COMPRA SE HA PRODUCIDO HACE UNA SEMANA Y URGE LA NECESIDAD DE MANDAR LA FÓRMULA DE LAS PASTILLAS PARA COMENZAR LO ANTES POSIBLE LA PRODUCCIÓN. DADA LA RELEVANCIA DE DICHA FÓRMULA, LA INFORMACIÓN NO PUEDE SER TRANSMITIDA EN CLARO Y HA DE IR CIFRADA. TENIENDO EN CUENTA QUE SON INADMISIBLES EL ROBO, LA PÉRDIDA O EL DESVELADO DE LA FÓRMULA, JUNTO CON EL HECHO DE QUE EL FICHERO EN EL QUE SE ALMACENA LA FÓRMULA TIENE UN TAMAÑO DE 100 GB, ¿QUÉ TIPO DE CRIPTOSISTEMA ESCOGERÍA? ¿POR QUÉ MOTIVOS? ¿QUÉ PROTOCOLO DE INTERCAMBIO DE CLAVES ESCOGERÍA?



Ejemplo. Solución.

A PRIMERA VISTA, TENIENDO EN CUENTA LA NECESIDAD DE MANDAR LA FÓRMULA CON LA MAYOR RAPIDEZ POSIBLE Y DADO EL GRAN TAMAÑO DEL FICHERO, ES IMPRESCINDIBLE HACER USO DE UN CIFRADO SIMÉTRICO, QUE DESTACA POR SU RAPIDEZ. POR OTRO LADO, LA CLAVE DE CIFRADO SIMÉTRICO HA DE ENVIARSE ASEGURANDO LA AUTENTICIDAD DEL EMISOR Y DEL RECEPTOR Y LA CONFIDENCIALIDAD DEL ENVÍO. POR ESTOS MOTIVOS, SE HACE USO DE UN PROTOCOLO DE INTERCAMBIO DE CLAVES SECRETAS MEDIANTE CRIPTOGRAFÍA ASIMÉTRICA EN EL QUE AMBOS PARTICIPANTES (EMPRESA ESPAÑOLA Y FÁBRICA HOLANDESA) DISPONEN DE UN PAR DE CLAVES (PÚBLICO-PRIVADA), ASOCIADAS A UN CERTIFICADO, Y SE HACE USO DE NONCES EN LOS MENSAJES INTERCAMBIADOS. EN RESUMEN, LA MEJOR OPCIÓN ES HACER USO DE UN CRIPTOSISTEMA HÍBRIDO EN EL QUE LOS DATOS SE CIFRAN DE FORMA SIMÉTRICA Y LA CLAVE SE ENVÍA POR CIFRADO ASIMÉTRICO.

9. ELEMENTOS DE LOS CERTIFICADOS DIGITALES

Existen distintos formatos de certificados, pudiendo destacar los certificados X.509 y PGP.

En líneas generales, los certificados contienen:

- Número de serie.
- Nombre de la entidad emisora.
- Periodo de validez.
- Nombre del sujeto propietario del certificado.
- Clave pública del sujeto propietario del certificado.

9. ELEMENTOS DE LOS CERTIFICADOS DIGITALES

La primera versión apareció en 1988, X.509v1, utilizándose la Infraestructura de Clave Pública (PKI).

1993 apareció la segunda versión, X.509v2, en la que se añadieron campos para identificar unívocamente al emisor (AC, de Autoridad de Certificación) y al propietario del certificado.

X.509v3. Esta nueva versión extendía las anteriores con un conjunto de campos adicionales que debían estar definidos en estándares o registrados por alguna comunidad u organización.

9.1. CERTIFICADOS X.509

El principal contenido de los certificados x.509v3 es el siguiente:

- Versión
- Número de serie
- Identificador del algoritmo de firma
- Nombre del emisor
- Validez
- Nombre del sujeto
- Información de la clave pública del sujeto
- Firma digital del emisor
- Extensiones (opcional):
    - Información de la clave y la política
    - Atributos del sujeto y de la AC emisora
    - Limitaciones del camino de los certificados

Los usos de los certificados X.509 son muy diversos, destacando los trámites relacionados con la administración electrónica (en España), la transmisión segura de información entre servidores (uso del protocolo SSL, detallado más adelante), etc.

9.2. CERTIFICADOS PGP

Pretty Good Privacy (PGP) es un algoritmo desarrollado en 1991 por Phil Zimmermann con el propósito de transmitir información por Internet de forma segura, haciendo uso de la criptografía de clave pública. Actualmente PGP sigue el estándar de OpenPGP.

9.2. CERTIFICADOS PGP

Los **certificados de PGP** son habitualmente creados por los propios usuarios.

Cada usuario crea un par de claves (pública-privada), almacenando la pública en un certificado PGP y haciendo uso de las mismas de igual modo que con otros certificados.

No hay ninguna autoridad de confianza que certifique la posesión de unas claves por un determinado usuario, la confianza se establece en función de los usuarios que firmen el certificado PGP (la clave pública), introduciéndose así el concepto de **anillo de confianza**.

9.2. CERTIFICADOS PGP

Cuando se hace uso de un certificado PGP el receptor tiene que verificar las firmas realizadas sobre este.

Si las firmas realizadas sobre un certificado se verifican, entonces el certificado también será confiable y además, dicho receptor puede realizar una nueva firma sobre él para reflejar su confianza.

Cada usuario establece el nivel de confianza a cada una de las claves (voto).

En PGP es remarcable la relevancia de depositar confianza automática en claves firmadas por terceros en los cuales confiamos.

9.2. CERTIFICADOS PGP

El contenido de los certificados PGP se puede resumir en:

- Número de versión.
- Clave pública.
- Algoritmo de creación de claves.
- Información del sujeto.
- Firma digital del sujeto.
- Periodo de validez.
- Algoritmo simétrico preferido.