
19. Criptografía
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Pérez

Conceptos

- La criptografía (del griego κρύπτω krypto, «oculto», y γράφω graphos, «escribir», literalmente «escritura oculta») es el arte o ciencia de cifrar y descifrar información medíante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leidos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

Conceptos

El cifrado es un procedimiento algorítmico (fórmulas matemáticas) mediante el cual se transforma un flujo de datos en contenido no legible, pudiendo recuperar su legibilidad al ser descifrado con la llave correcta.

Conceptos

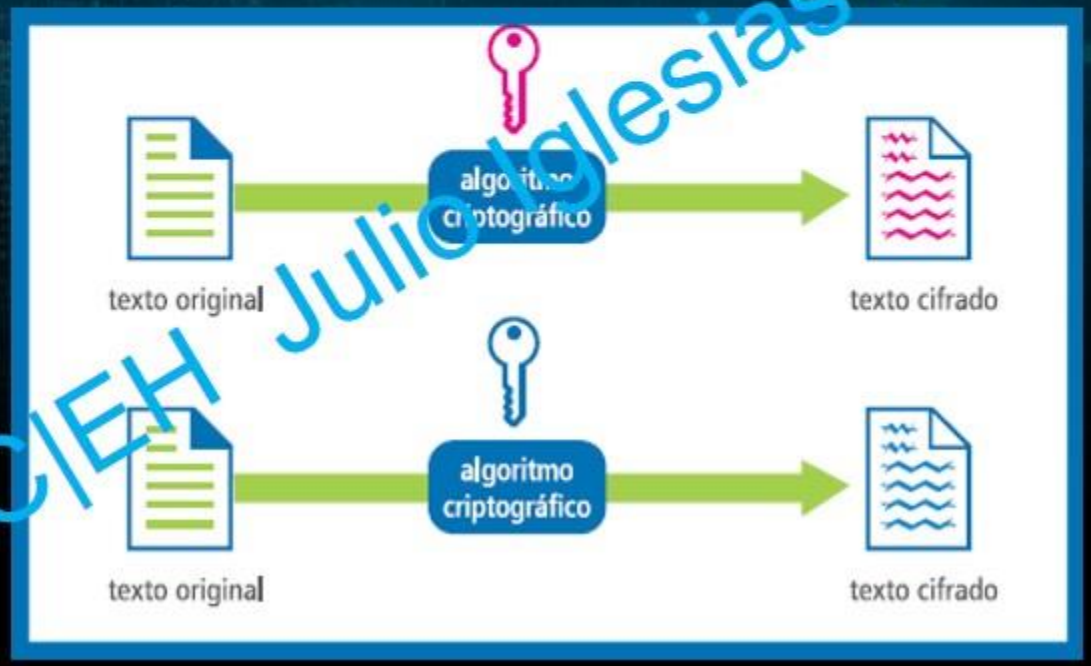
- **Cifrado de flujo (stream cipher):** Los cifradores de flujo son algoritmos de cifrado que pueden realizar el cifrado incrementalmente, convirtiendo el texto en claro en texto cifrado bit a bit. Esto se logra construyendo un generador de flujo de clave. Un flujo de clave es una secuencia de bits de tamaño arbitrario que puede emplearse para oscurecer los contenidos de un flujo de datos combinando el flujo de clave con el flujo de datos mediante la función XOR. Si el flujo de clave es seguro, el flujo de datos cifrados también lo será.

Conceptos

- **Cifrado de bloque:** Los bits de datos se dividen en bloques y se introduce en el sistema de cifrado. Cada bloque de datos (usualmente 64 bits a la vez) es encriptado con la llave y el algoritmo.
- Estos cifrados utilizan métodos como sustitución y transposición en algoritmos, y son considerados más lentos y simples que los cifrados de flujo.

Criptografía simétrica

(Clave sereta, clave compartida y clave privada) utiliza la misma clave para cifrar y descifrar la información.



Algunos algoritmos simétricos

- DES: Un cifrado de bloque que utiliza una llave de 56 bits (con 8 bits reservados para paridad). Debido al pequeño tamaño de su llave, este estándar se volvió obsoleto y no es considerado un algoritmo muy seguro.
- 3DES: Un cifrado de bloque que utiliza una lave de 168 bits. 3DES puede utilizar hasta tres llaves en un método de encriptación múltiple. Es más efectivo que DES, pero mucho más lento.
- AES (Advanced Encryption Standard): Un cifrado de bloque que utiliza una clave de 128, 192 o 256 bits, y remplaza efectivamente DES. Es mucho más rápido que DES o 3DES.
- IDEA (International Data Encryption Algorithm): Un cifrado de bloque que utiliza una llave de 128 bits, fue diseñado para remplazar a DES. IDEA fue patentado y utilizado principalmente en Europa.

Pseudocódigo AES

```
Cipher (bute in [4*NB], byte out[4*NB], word w[Nb*(Nr+1)])
begin
byte state[4,Nb]
state = in
AddRoundKey(state, w)
for round = 1 step 1 to Nr-1
        SubButes(state)
        ShiftRows(state)
        MixColumns(state)
        AddRoundKey(state, w+round*Nb)
end for
SubButes(state)
ShiftRows(state)
AddRoundKey(state, w+Nr*Nb)
out = state
end
```

Más algoritmos simétricos

- Twofish: Cifrado de bloque que utiliza llaves de hasta 256 bits.
- Blowfish: Cifrado de bloque, remplazado por AES, utiliza un bloque de 64 bits de tamaño y llaves desde 32 hasta 448 bits. Blowfish es considerado de dominio público.

Rivest Cipher

- RC (Rivest Cipher): Abarca varias versiones. Es un cifrado de bloque que utiliza llaves de hasta 2040 bits.
- RC4: Una llave variable de tamaño corriente con operaciones orientadas en bytes, y está basada en el uso de permutaciones aleatorias.
- RC5: Es un algoritmo parametrizado con un bloque de tamaño variable, una llave de tamaño variable y con número de rondas variables. El tamaño de la clave es de 128 bits.
- RC6: Agrega dos características a RC5; la inclusión de multiplicación entera, y el uso de cuatro registros de 4 bits en vez de los dos registros de 2 bits de RC5.

Criptografía asimétrica

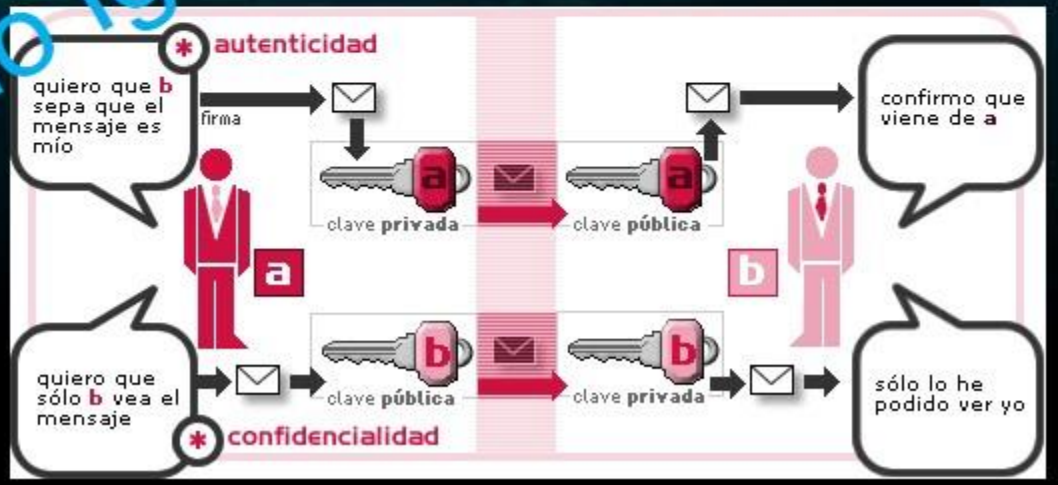
(Clave pública) utiliza distintas claves para cifrar y descifrar la información.

Estas claves son conocidas como claves privadas y públicas.

Recordar siempre esta regla:

La clave pública cifra.

La clave privada descifra.



Algunos algoritmos asimétricos

- Diffie-Hellman: Desarrollado para utilizarse como protocolo de intercambio. Diffie-Hellman es utilizado en Secure Sockets Layer (SSL) y en cifrado IPSec. Puede ser vulnerable a ataques Man-in-the-Middle.
- Elliptic Curve Cryptosystem (ECC): Utiliza puntos de una curva elíptica, en conjunto con problemas logarítmicos, para cifrado y firma. Utiliza menos poder de procesamiento que otros métodos, convirtiéndolo en una buena elección para dispositivos móviles.

Algunos otros

- El Gamal: No está basado en la factorización de números primos, este método utiliza la solución de los problemas del logaritmo discreto para el cifrado y firmas digitales.
- RSA: Un algoritmo de cifrado fuerte que se logra mediante el uso de dos números primos grandes. Factorizando estos números se crean llaves de hasta 4096 bits. RSA puede ser utilizado para el cifrado y firmas digitales, y es la norma moderna de facto.

Función HASH

Es una función matemática unidireccional que toma una entrada y produce una cadena que tiene una entrada y produce típicamente una cadena longitud fija, o hash, basado en la disposición de los bits de los datos en la entrada.

Algunos algoritmos HASH

- RC5: Es un algoritmo parametrizado con un bloque de tamaño variable, una llave de tamaño variable y con número de rondas variables. El tamaño de la clave es de 128 bits. Es obsoleto debido a algunas fallas en el algoritmo (U.S. CERT, Agosto 2010). Actualmente sigue siendo utilizado para la verificación de archivos descargados y en algunos casos para almacenar contraseñas.
- SHA1: Produce un valor de salida de 160 bits desde un mensaje con un tamaño máximo de (2 elevado a 64, menos 1) bits, se asemeja al algoritmo MD5.
- SHA2: Es una familia de dos funciones hash similares, con tamaños distintos de bloques, produce salidas de 224, 256, 384 y 512 bits.
- SHA3: Está aún en desarrollo.

¿Qué es Secure Shell?

- Comunicación Remota: Es el remplazo a Telnet y las utilidades “r” de Berkeley (rlogin, rsh, rcp, y rdist).
- Canal seguro: Provee un canal encriptado para el inicio de sesión remoto, ejecución de comandos y transferencia de archivos.
- Autenticación fuerte: Provee una autenticación de usuario y host a host fuerte, y asegura la comunicación sobre un internet inseguro.

Public Key Infraestructure

- Es un conjunto de hardware, software, personas, directivas y procedimientos requeridos para crear, administrar, distribuir, utilizar, almacenar y revocar certificados digitales.

Componentes de un PKI

- Un sistema de administración de certificados para la generación, distribución, almacenamiento, y verificación de certificados.
- Uno o más directorios donde los certificados (y sus llaves públicas) están.
- Una Autoridad de Registro (RA) que actúa como un verificador de la Autoridad de Certificación.
- Autoridad de Certificación (CA) emite y verifica los certificados digitales.

Autoridades de Certificación

- COMODO.
- THAWTE.
- VeriSign.
- Entrust.

Firma de correo

Firma Digital

- Utiliza criptografía asimétrica para simular las propiedades de seguridad de una firma en digital en vez de una forma de escritura.
- Los esquemas de firma digital incluye dos algoritmos, una clave privada para firmar el mensaje y una clave pública para verificar las firmas.

Secure Socket Layer

- Es un protocolo de la capa de aplicación desarrollado por Netscape para administrar la seguridad de la transmisión de un mensaje por Internet.
- Utiliza la encriptación asimétrica RSA (clave pública) para cifrar los datos transferidos sobre una conexión SSL.

Transport Layer Security (TLS)

Es un protocolo para establecer una conexión segura entre un cliente y un servidor y asegurar la privacidad y la integridad de la información durante la transmisión.

Utiliza el algoritmo RSA con 1024 y 2048 bits de fortaleza.

- TLS Record Protocol: Provee una conexión segura con algún método de encriptación como DES.
- TLS Handshake Protocol: Permite al cliente y servidor autentificarse mutuamente y transferir un algoritmo de encriptación y claves criptográficas antes del intercambio de datos.

Cifrado de disco

- Confidencialidad: La encriptación de disco es utilizada para proteger la confidencialidad de los datos almacenados en el disco. Volúmenes ocultos, Passphrase, Estenografía, Privacidad.
- Encriptación: Trabaja de manera similar que la encriptación de los mensajes de texto y protege los datos incluso cuando el S.O. no está activo. Encriptación de volumen.
- Protección: Con el uso de un programa de encriptación en su disco, se puede salvaguardar la información que se guardará en un disco y mantenerla segura si caen en las manos equivocadas.
- Herramientas de cifrado de disco: TrueCrypt, etc.

Ataques de criptografía

- Ataque Known-plaintex: La meta del atacante es descubrir la clave utilizada para cifrar el mensaje así los otros mensajes pueden ser descifrados y leídos.

- Chosen-plaintext: El atacante define su propio texto plano, alimenta el sistema de cifrado, y analiza el resultado del texto cifrado.

- Ataque Ciphertext only: La meta del atacante es descubrir el texto plano de los mensajes calculando la clave utilizada en el proceso de encriptación.

Ataques de criptografía

- Ataque Chosen Ciphertext: El atacante puede elegir el texto cifrado para que sea descifrado y tenga acceso al texto plano descifrado resultante.
- Ataque Chosen-key: Una generalización del ataque chosen-text.
- Ataque Timing: Está basado en medición repetida de los tiempos de ejecución exactos de operaciones exponenciales modulares.

Ataques de criptografía

- Ataque Adaptive chosen-plaintext: El atacante utiliza esta técnica cuando tiene libre uso de una pieza de hardware de descifrado, pero no puede extraer la clave de encriptación de él.

- Ataque Rubber hose: Extracción de secretos criptográficos (ej: la contraseña de un archivo encriptado) desde una persona coerción o tortura.

Metodologías Code Breaking

- Artimañas y engaños: Implica el uso de técnicas de ingeniería social para extraer las claves criptográficas.
- Fuerza bruta: Las claves criptográficas son descubiertas intentando todas las combinaciones posibles.
- One-time Pad: Contiene muchos grupos de letras no repetidas o números de claves, que son elegidas de manera aleatoria.
- Análisis de frecuencia: Es el estudio de la frecuencia de las letras o grupos de letras en un texto cifrado. Trabaja en el hecho de que en cualquier tramo determinado o lenguaje escrito, ciertas letras y combinaciones de letras ocurren con frecuencias variables.

Ataque de Fuerza Bruta

- Intentando un número largo de posibilidades hasta dar con la clave correcta.
- El éxito de este ataque depende del tamaño de la clave, el tiempo y los mecanismos de seguridad.
- Es un proceso que consume muchos recursos y tiempo.

Ataque MitM en esquemas de firma digital.

- Rompe un cifrado en dos partes, trabaja contra cada una de ellas separadamente y compara resultados.
- Puede ser utilizado para falsificar firmas en esquemas de firma digital mixtos, y toma menos tiempo que un ataque exhaustivo.
- El ataque trabaja cifrando desde un extremo y descifrando en el otro, así cumpliendo en el medio.


¡Muchas Gracias!
C|EH Julio Iglesias Perez