



Sistemas Operativos 2

Unidad 5: Seguridad

Criptografía

René Ornelis
Primer semestre de 2025

Contenido

1	Definición	4
1	Esteganografía.....	5
1.1	Diferencia entre esteganografía y criptografía.....	6
1.2	Aplicaciones de la esteganografía.....	6
1.3	Desafíos y limitaciones	6
2	Encriptación simétrica o privada	7
3	Encriptación asimétrica o pública.....	8
4	Certificados digitales	10
1.3.1	Componentes Clave de un Certificado Digital:	10
5	Firma electrónica de documentos	11
6	Protocolos de seguridad con RSA.....	11
6.1	PGP	11
6.2	HTTPS	12
6.2.1	Autoridades certificadoras	12
7	Referencias.....	12

Índice de figuras

Figura 1: Proceso de encripción.....	4
Figura 2: Ejemplo de un escítalo	5

Criptografía

Dentro de todos los componentes de la seguridad se encuentra inmerso el tema de la criptografía, como un medio de proteger la información que se almacena o se transmite.

1 Definición

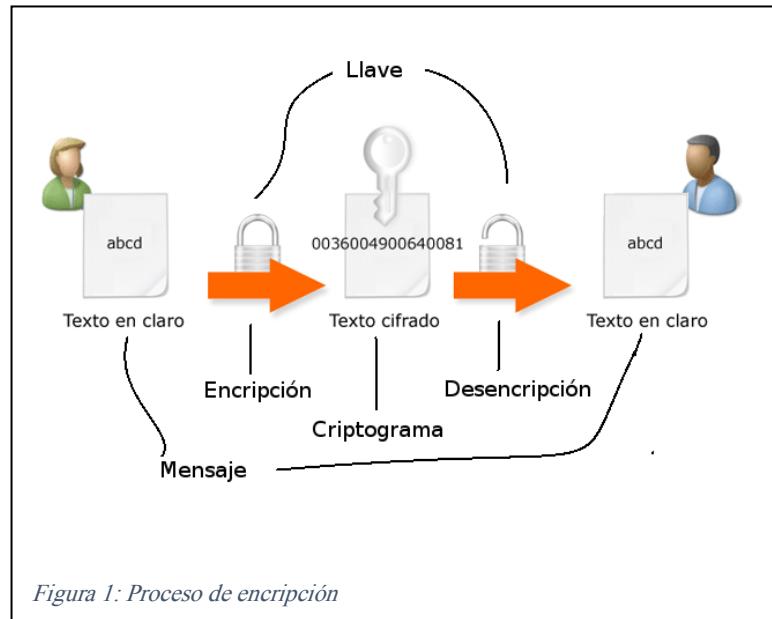
El encriptado es una transformación, reversible, que se aplica a un texto cualquiera, con el fin de hacerlo ilegible para quien no conozca la transformación aplicada. Es decir:

Sí se tiene un texto T y una clave K , se puede aplicar una función de encriptación $E(T,K) = C$, donde C se llama criptograma, al cual se le puede aplicar una función de desencriptación $D(C,K) = T$ para obtener el texto original

Gráficamente lo podemos representar como se muestra en la Figura 1.

La encriptación tiene muchas aplicaciones para la protección de datos sensibles o simplemente para privacidad de las personas.

La encriptación viene desde principios de la historia, aplicado principalmente en la guerra y en las sociedades secretas. Por ejemplo: se sabe que los espartanos utilizaban un bastón de madera llamado escítalo, sobre el cual se enrollaba una cinta de lino, y el mensaje se escribía transversalmente, tal como se muestra en la Figura 2.



El mensajero era portador de la cinta, que desenrollada, era ilegible ya que resultaba en una **transposición** de las letras.

El destinatario, para leer el mensaje debería repetir el proceso, enrollando la cinta sobre un bastón del mismo diámetro. De esta forma, la cinta funcionaba como criptograma y el bastón como la llave, ya que, si no se sabía el diámetro, no se podía entender el mensaje.



Figura 2: Ejemplo de un escitalo

Durante el imperio romano, Julio César creó un método de encriptación que consistía en un corrimiento de caracteres, en el cual se sustituye la A por la B, la B

por la C y así sucesivamente. Ejemplo:

JUAN -> KVBO (corrimiento de 1 carácter)

Claro que, en la computación moderna, estos métodos distan mucho de ser efectivos, ya que serían fácilmente descifrados por algoritmos de fuerza bruta. Actualmente se han desarrollado una gran cantidad de algoritmos y métodos de encriptación, los cuales clasificaremos en dos grupos:

1. Encriptación simétrica o privada
2. Encriptación asimétrica o pública

Adicionalmente, también se pueden aplicar técnicas de ocultación de información como la **esteganografía**. La esteganografía es el arte y la ciencia de ocultar la presencia de información dentro de otros datos de manera que no se perciba la existencia de la información oculta.

1 Esteganografía

La **esteganografía** es una técnica de ocultación de información dentro de otros tipos de datos, de manera que la existencia misma de la información oculta no sea perceptible para el observador. Su objetivo principal es esconder un mensaje o archivo dentro de otro de tal forma que no se detecte que hay algo oculto.

El término "esteganografía" proviene del griego: "**steganos**" que significa "cubierto" u "oculto", y "**grapho**" que significa "escribir". Por lo tanto, la esteganografía puede interpretarse como "escribir de forma oculta".

En la práctica, la esteganografía se utiliza para ocultar información en diversos tipos de medios, como imágenes, audio, video o incluso texto. Algunos ejemplos comunes de cómo se oculta la información incluyen:

1. **Imágenes:** Uno de los métodos más utilizados es modificar ligeramente los valores de los píxeles en una imagen para esconder datos. Esto se hace de manera que los cambios sean tan

pequeños que no sean detectables por el ojo humano. Por ejemplo, en una imagen digital, los valores de los píxeles pueden alterarse en los bits menos significativos (LSB, por sus siglas en inglés), que son imperceptibles a simple vista pero pueden almacenar datos.

2. **Audio:** En archivos de audio, la información puede ser oculta en las variaciones mínimas de las ondas sonoras. Al igual que en las imágenes, los cambios son tan pequeños que no afectan la calidad del audio de manera significativa.
3. **Texto:** Aunque menos común, también se pueden ocultar mensajes dentro de un texto. Esto puede lograrse a través de técnicas como el uso de espacios en blanco, la alteración de la puntuación, o incluso a través de patrones complejos en las palabras y letras que solo un receptor específico puede descifrar.
4. **Videos:** En los videos, la esteganografía puede implicar la modificación de los cuadros individuales o la manipulación de las secuencias de imágenes y sonido para ocultar la información.

1.1 Diferencia entre esteganografía y criptografía

Es importante no confundir **esteganografía** con **criptografía**, aunque ambas son técnicas utilizadas para la seguridad de la información. La criptografía se basa en transformar un mensaje en un formato ilegible para que solo aquellos con la clave adecuada puedan descifrarlo, pero el hecho de que el mensaje esté presente es evidente. En cambio, en la esteganografía, la información está oculta de manera que no se sabe ni siquiera que existe un mensaje.

1.2 Aplicaciones de la esteganografía

1. **Protección de datos:** Se puede utilizar para proteger la privacidad y ocultar información sensible, de modo que, incluso si un archivo es interceptado, el mensaje no será descubierto fácilmente.
2. **Comunicación secreta:** En contextos de espionaje o censura, los mensajes se pueden ocultar dentro de otros archivos para evitar que los interceptores detecten que se está transmitiendo información.
3. **Marcas de agua digitales:** La esteganografía también se usa para insertar marcas de agua invisibles en imágenes o videos, lo que puede ser útil para la protección de derechos de autor y la autenticidad de los contenidos.

1.3 Desafíos y limitaciones

Aunque la esteganografía puede ser muy efectiva, no está exenta de desafíos. La principal limitación es que, si alguien sospecha que un archivo contiene información oculta, puede intentar detectarlo mediante análisis forenses. Además, el tamaño del mensaje oculto suele ser limitado debido a las restricciones en el tamaño de los cambios que se pueden realizar sin alterar perceptiblemente el archivo original.

2 Encriptación simétrica o privada

Es el primer tipo de encriptación moderno trabajado a nivel computacional, incluyen máquinas como la codificadora **enigma**, durante la Segunda Guerra Mundial, en el cual la misma llave utilizada para encriptar, es la que se necesita para realizar la desencriptación.

Un ejemplo simple es la **mezcla con secuencias fijas aleatorias**, en la cual se aprovecha la siguiente propiedad de la operación *xor*

sea x & y dos enteros independientes, entonces se cumple que

$$(x \text{ xor } y) \text{ xor } x = y$$

$$(x \text{ xor } y) \text{ xor } y = x$$

Si T es el texto para encriptar, T se ve como una secuencia de enteros $T_1 T_2 T_3 \dots T_n$. La llave secreta K , también se ve como una secuencia de enteros $K_1 K_2 K_3 \dots K_m$, donde $m \leq n$. El criptograma C , visto como $C_1 C_2 C_3 \dots C_n$ se forma por sucesivas operaciones xor, de superposiciones de la llave K sobre el texto T , así:

T	T_1	T_2	...	T_m	T_{m+1}	T_{m+2}	...	T_{n-1}	T_n
Xor									
K	K_1	K_2	...	K_m	K_1	K_2	...	K_i	K_{i+1}
=									
C	C_1	C_2	...	C_m	C_{m+1}	C_{m+2}	...	C_{n-1}	C_n

y la operación de desencriptación sería así:

C	C_1	C_2	...	C_m	C_{m+1}	C_{m+2}	...	C_{n-1}	C_n
XOR									
K	K_1	K_2	...	K_m	K_1	K_2	...	K_i	K_{i+1}
=									
T	T_1	T_2	...	T_m	T_{m+1}	T_{m+2}	...	T_{n-1}	T_n

Una encriptación simple y eficiente, pero en una combinatoria de 16^m puede encontrarse la llave K (suponiendo que 16 bits es el tamaño de un entero).

Entre los algoritmos de encriptación simétrica actuales se encuentran:

- DES (Data Encryption Standard): llave de 56 bits de longitud. Se calcula tiempo menor a 3 meses para desencriptar el mensaje utilizando fuerza bruta
- Triple DES
- Advanced Encryption Standard (AES)
- Blowfish

A pesar de la importancia que han tenido (y seguirán teniendo) la encriptación simétrica, en nuestro mundo actual de comunicación masiva y globalizada, tener comunicación privada a través de estos métodos, presentan dos problemas importantes:

1. **La paradoja del canal seguro:** si deseamos encriptar un mensaje, es porque seguramente debemos enviarlo a través de un medio o canal que se considera inseguro, como el correo electrónico. La paradoja del canal seguro se deriva de que el destinatario está geográficamente distante y no es posible enviar la contraseña por un medio seguro, y si hubiera un medio seguro, no sería necesario encriptar el mensaje
2. **La multiplicidad de intercambios:** Si 2 personas necesitan comunicación privada, deben realizar un intercambio de llaves. Si son 3 personas, deben realizar un total de 6 intercambios (2 por cada participante), sin son 4, 12 intercambios y así sucesivamente, que resulta en que, si personas desean comunicarse privadamente, debe haber $n*(n-1)$ intercambio, lo que representa un orden cuadrático.

Estos problemas hicieron que la encriptación simétrica fuera insuficiente para lograr una comunicación privada eficiente en el Internet, y es allí donde cobra importancia la encriptación asimétrica.

3 Encriptación asimétrica o pública

El RSA es el criptosistema de llave pública más popular basado en el modelo de Diffie-Hellman, el cual ofrece encriptación y firmas digitales (autenticación). Ron Rivest, Adl Shamir y Leonard Adleman desarrollaron el RSA en 1977, de ahí su nombre formado por la primera letra del apellido de sus inventores.

La base de este sistema es la compleja matemática detrás de la factorización de números primos grandes (ver links publicados), que van desde 128 bits hasta 1024, lo cual está fuera del alcance del curso. Sin embargo, lo importante de este método es que tiene las siguientes propiedades:

1. Cada usuario tiene dos llaves: una privada y otra pública. La llave privada es conocida sólo por el propietario y normalmente es almacenada en un archivo protegido por una llave simétrica, conocida sólo por el dueño. La llave pública, por el contrario, debe ser conocida por todos los posibles destinatarios, y generalmente se publica por cualquier canal inseguro (correo electrónico, redes sociales, directorios públicos, etc)

2. Sea

1. T el texto o mensaje en claro.
2. X_{priv} la llave privada de la persona X.
3. X_{pub} la llave pública de X.
4. $C=E(T,K)$ la función de encriptación del texto T con la llave K, que da como resultado el criptograma C.
5. $T=D(C, K)$ la función de desencriptación del criptograma C, con la llave K, que da como resultado el texto T.
6. Entonces, para RSA se cumple que:
 1. si $C=E(T, X_{\text{priv}})$ entonces $T = D(C, X_{\text{pub}})$, es decir lo que se encripta con la llave privada, sólo puede desencriptarse con la llave pública
 2. si $C=E(T, X_{\text{pub}})$ entonces $T = D(C, X_{\text{priv}})$, es decir los que se encripta con la llave pública, sólo puede desencriptarse con la llave privada

Estas propiedades eliminan los problemas de la paradoja del canal seguro, por el uso de la llave pública, y la multiplicidad de intercambios, ya que para que n personas se comunican, sólo se necesitan n intercambios de llaves públicas.

Además ya se puede realizar una comunicación privada o encriptación extremo a extremo (E2E del inglés *End to End*) así:

- Si X envía un mensaje a Y, encriptado con X_{priv} , Y lo desencriptará con X_{pub} , con lo cual Y estará seguro que X es el remitente, ya que el mensaje fue encriptado con X_{priv}
- Si X envía un mensaje a Y, encriptado con Y_{pub} , Y lo desencriptará con Y_{priv} , con lo cual X estará seguro que sólo Y podrá leerlo, ya que sólo Y conoce Y_{priv}
- Al combinar ambos mecanismos, X puede crear un criptograma, en el cual se X se asegure que sólo Y puede verlo y Y estará seguro de que X es el remitente, así:
 - X encriptará así:
 - $C_1 = E(T, X_{\text{priv}})$
 - $C_2 = E(C_1, Y_{\text{pub}})$
 - Se envía C_2 a Y
 - Y desencriptará así:
 - $C_1 = D(C_2, Y_{\text{priv}})$
 - $T = D(C_1, X_{\text{pub}})$

Estas propiedades han hecho de RSA la base de todos los protocolos de seguridad que conocemos, como PGP, HTTP, SSL, etc. Sin embargo, debido a su complejidad matemática, que involucra operaciones de exponentes y módulos con número grandes (de hasta 1024 bits o sea 2^{1024}), su rendimiento es mucho menor que el de un algoritmo simétrico. Por lo tanto, los protocolos mencionados, hacen una combinación de métodos simétricos y asimétricos, en los que éstos últimos se utilizan sólo para intercambiar una llave simétrica temporal generada en tiempo de corrida, al principio de la comunicación y luego la información se intercambia utilizando un algoritmo simétrico.

De esta forma se logra una privacidad completa, a través de la asimetría, con un rendimiento aceptable, a través de la simetría.

4 Certificados digitales

Un **certificado digital** es un documento electrónico que sirve para identificar a una persona, organización o dispositivo en el entorno digital. Actúa como una "identidad" digital y se emite por una **Autoridad de Certificación (CA)**, que es una entidad confiable encargada de verificar la identidad del solicitante y emitir el certificado.

1.3.1 Componentes Clave de un Certificado Digital:

1. **Clave Pública:** Contiene la clave pública del propietario, que se utiliza para cifrar datos o verificar firmas digitales.
2. **Información del Propietario:** Incluye detalles como el nombre, la dirección de correo electrónico, y a veces otros datos relevantes del titular.
3. **Autoridad de Certificación:** Información sobre la CA que emite el certificado, incluyendo su firma digital.
4. **Fecha de Validez:** Indica el período durante el cual el certificado es considerado válido. Incluye fechas de inicio y expiración.
5. **Número de Serie:** Un identificador único para el certificado, que ayuda a prevenir la duplicación.
6. **Algoritmo de Firma:** El método criptográfico utilizado para firmar el certificado digital.

Formato PEM:

```
-----BEGIN RSA PRIVATE KEY-----
RSAPrivateKey ::= SEQUENCE {
    version            Version,
    modulus           INTEGER,   -- n
    publicExponent    INTEGER,   -- e
    privateExponent   INTEGER,   -- d
    prime1            INTEGER,   -- p
    prime2            INTEGER,   -- q
    exponent1         INTEGER,   -- d mod (p-1)
    exponent2         INTEGER,   -- d mod (q-1)
    coefficient       INTEGER,   -- (inverse of q) mod p
    otherPrimeInfos   OtherPrimeInfos OPTIONAL
}
-----END RSA PRIVATE KEY-----
```

Mientras que una clave pública RSA contiene solo los siguientes datos:

```
-----BEGIN RSA PUBLIC KEY-----
RSAPublicKey ::= SEQUENCE {
    modulus          INTEGER,   -- n
    publicExponent   INTEGER    -- e
}
-----END RSA PUBLIC KEY-----
```

5 Firma electrónica de documentos

La firma digital es un mecanismo criptográfico utilizado para garantizar la autenticidad, integridad y no repudio de un documento electrónico. Es un proceso que permite al firmante verificar su identidad y autoría de un documento, asegurando que no haya sido modificado después de haber sido firmado.

El firmante utiliza su **clave privada** para generar la firma digital, que se adjunta al documento. Esta firma se crea a partir de un algoritmo criptográfico que toma el contenido del documento y lo convierte en un "hash" que luego se cifra utilizando la clave privada.

El receptor del documento utiliza la **clave pública** del firmante para verificar la firma. Para ello, se calcula un "hash" del documento recibido y se compara con el "hash" desencriptado de la firma. Si coinciden, se asegura que el documento no ha sido alterado y que la firma proviene del titular de la clave privada.

En Guatemala, la firma electrónica avanzada está regulada bajo el **Decreto Número 47-2008 del Congreso de la República**, conocido como la **Ley de Comercio Electrónico, Firma Electrónica y Documentos Electrónicos**. Esta ley establece un marco legal que regula el uso de las firmas electrónicas y digitales en el contexto de transacciones electrónicas. Las bases legales principales son:

6 Protocolos de seguridad con RSA

6.1 PGP

PGP, que significa **Pretty Good Privacy**, es un protocolo de criptografía que se utiliza para la encriptación y firma de datos, especialmente correos electrónicos. Los principios criptográficos de PGP se basan en varios conceptos fundamentales:

2 1. Cifrado de Clave Pública

- **Clave pública y Clave privada:** PGP utiliza un sistema de cifrado asimétrico, donde cada usuario tiene un par de claves: una clave pública (que se puede compartir con otros) y una clave privada (que se mantiene en secreto). La clave pública se utiliza para cifrar los mensajes, y solo la clave privada puede descifrarlos.
- **Confidencialidad:** Al cifrar un mensaje con la clave pública del destinatario, se asegura que solo este destinatario, que posee la clave privada correspondiente, puede leer el mensaje.

3 2. Firma Digital

- **Autenticación e integridad:** PGP permite a los usuarios firmar digitalmente un mensaje utilizando su clave privada. Esto garantiza que el mensaje proviene realmente del remitente (autenticación) y que no ha sido modificado (integridad).
- **Verificación:** El destinatario puede usar la clave pública del remitente para verificar la firma, asegurándose de que el mensaje es auténtico y ha llegado sin alteraciones.

4 3. Hashing

- **Función hash:** PGP utiliza funciones hash para crear un resumen del mensaje antes de la firma. Este resumen (o hash) es mucho más pequeño que el mensaje original y se firma digitalmente.
- **Eficiencia:** Esto hace que el proceso de firma sea más eficiente, ya que se trabaja con un hash en lugar de un mensaje completo.

5 4. Red de confianza

- **Modelo de confianza:** PGP emplea un modelo de "red de confianza" en lugar de un modelo jerárquico de autoridad de certificación. Los usuarios pueden certificar las claves públicas de otros, creando un vínculo de confianza basado en la verificación personal.
- **Verificación de identidad:** Esto permite que los usuarios confíen en las claves públicas de otras personas con base en las recomendaciones y firmas de amigos o conocidos.

6 5. Cifrado simétrico para datos

- **Cifrado híbrido:** Para cifrar el contenido de los mensajes, PGP combina el cifrado simétrico (donde se utiliza una sola clave para cifrar y descifrar) con el cifrado asimétrico. Se genera una clave de sesión aleatoria para cada mensaje, que se utiliza para cifrar el mensaje con un algoritmo simétrico, y luego esta clave se cifra con la clave pública del destinatario.

6.2 HTTPS

6.2.1 Autoridades certificadoras

7 Referencias

- **RSA encryption:** <https://www.britannica.com/topic/RSA-encryption>
- **RSA (cryptosystem):** [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))
- **What is RSA encryption and how does it work?:**
<https://www.comparitech.com/blog/information-security/rsa-encryption/>