

Criptografía



SEGURIDAD INFORMÁTICA UNIDAD 7.

Criptología

Criptografía (Kripto=oculto, graphos=escritura)

Es la **ciencia** que se encarga de estudiar las distintas técnicas empleadas para **transformar** (encriptar o cifrar) la información y hacerla **irreconocible** a todos aquellos **usuarios no autorizados** de un sistema informático de modo que solo los legítimos **propietarios** pueden **recuperar** (desencriptar o descifrar) la información original.

Es un mecanismo para garantizar la confidencialidad, la integridad y la autenticidad de los mensajes y documentos

Criptografía

La criptografía o el cifrado designan a un **procedimiento que traduce un texto sin formato (plain text o texto plano) en una secuencia ininteligible de caracteres mediante una clave**. El objetivo es que el contenido del texto secreto resultante o criptograma (texto cifrado) solo sea accesible para aquellos que disponen de la clave para descifrarlo.

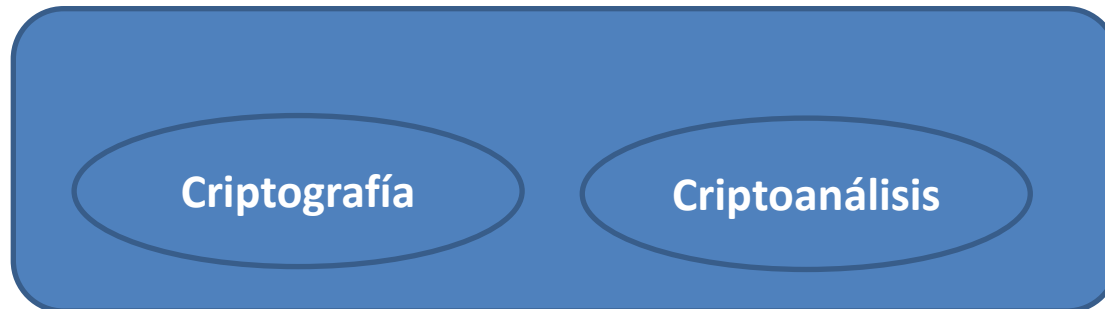
Aunque expresiones tales como "texto plano" o "texto cifrado" provengan de la estrategia militar, los métodos criptográficos pueden ser también aplicados a otro tipo de información electrónica como mensajes de voz, archivos de imagen o códigos de programación, además de a mensajes de texto.

Criptología

Criptoanálisis

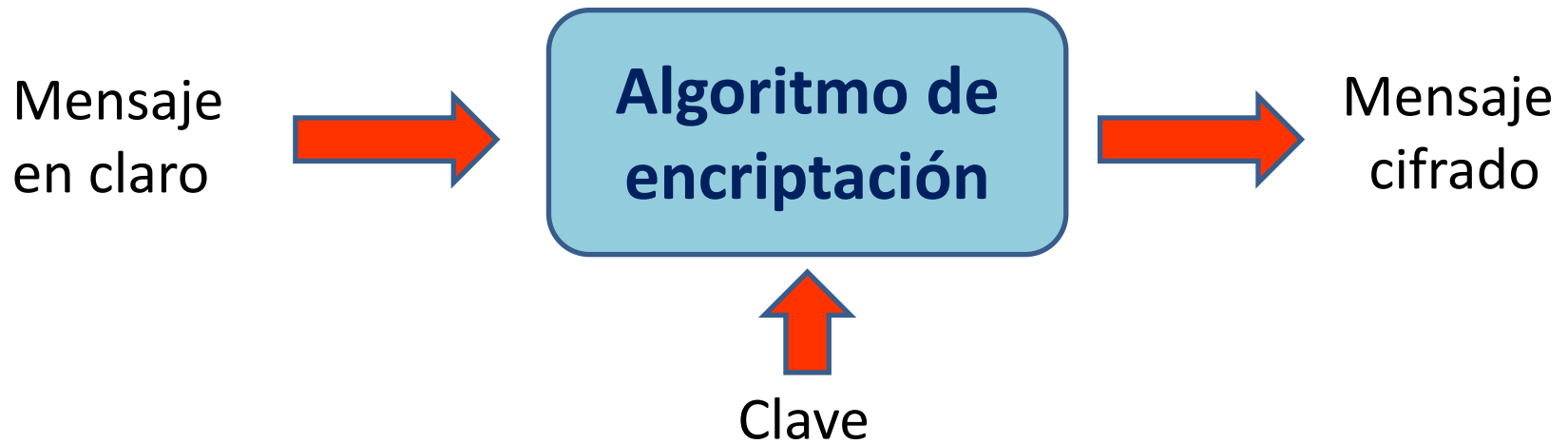
Es la ciencia que se estudia las herramientas y técnicas que permitan conocer los códigos y sistemas de protección definidos por la criptografía.

Criptología



Criptología

Componentes de un sistema de cifrado

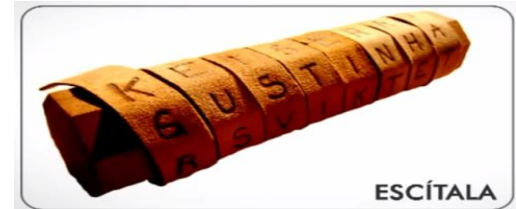


Historia de los sistemas criptográficos

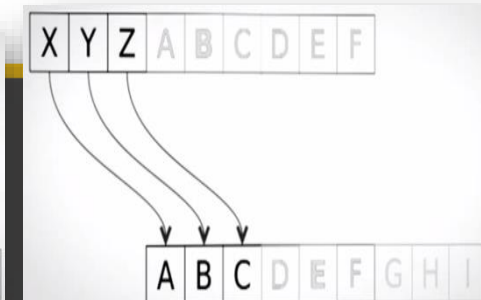
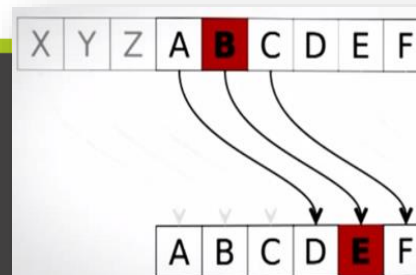
Las aplicaciones de los sistemas criptográficos tienen aplicación principal en guerras y gobierno.

Las primeras prácticas en los griegos y romanos: Uso del cilindro scytala era empleado por los griegos. Método **Transposición**.

Componentes: correa de cuero, cilindro, mensaje sobre el cuero enrollado. La clave: el diámetro del cilindro.



El Cifrado César, usada por romanos. Consiste en una simple sustitución de cada letra del mensaje por otra distanciada tres posiciones del alfabeto latino. Método **Sustitución**.



Historia de los sistemas criptográficos

En los califatos islámicos, en el siglo IX d.C., en Bagdad nace el moderno criptoanálisis. Cada lengua tiene una frecuencia característica de aparición de sus letras. Esto constituyó en la decadencia de los **métodos de sustitución monoalfabéticos**.



En el renacimiento León Batista Alberti, creo el cifrados en disco. **Método de sustitución polialfabético.**

A Vigenere square, a 26x26 grid of letters used for encryption and decryption. The grid is composed of the alphabet (A-Z) repeated in a circular fashion. The first row is the alphabet in order. Each subsequent row is shifted one letter to the left. This grid is used to find the intersection of a letter from the message and a letter from the key to determine the encrypted letter.

Otro método de este tipo es el del diplomático francés Vigenere en 1586. Usado 200 años después y “roto” a mediados del siglo XIX.

Historia de los sistemas criptográficos

En el siglo XX aparecen las máquinas de cifrado: **ENIGMA**.



ENIGMA

Patentada por Arthur Scherbius en 1918

Usados por el ejército alemán en la Segunda Guerra Mundial.

Historia de los sistemas criptográficos

Otras máquinas similares fueron el TYPEX en Reino Unido y la Converter M-209 en los Estados Unidos



Typex



Converter M-209

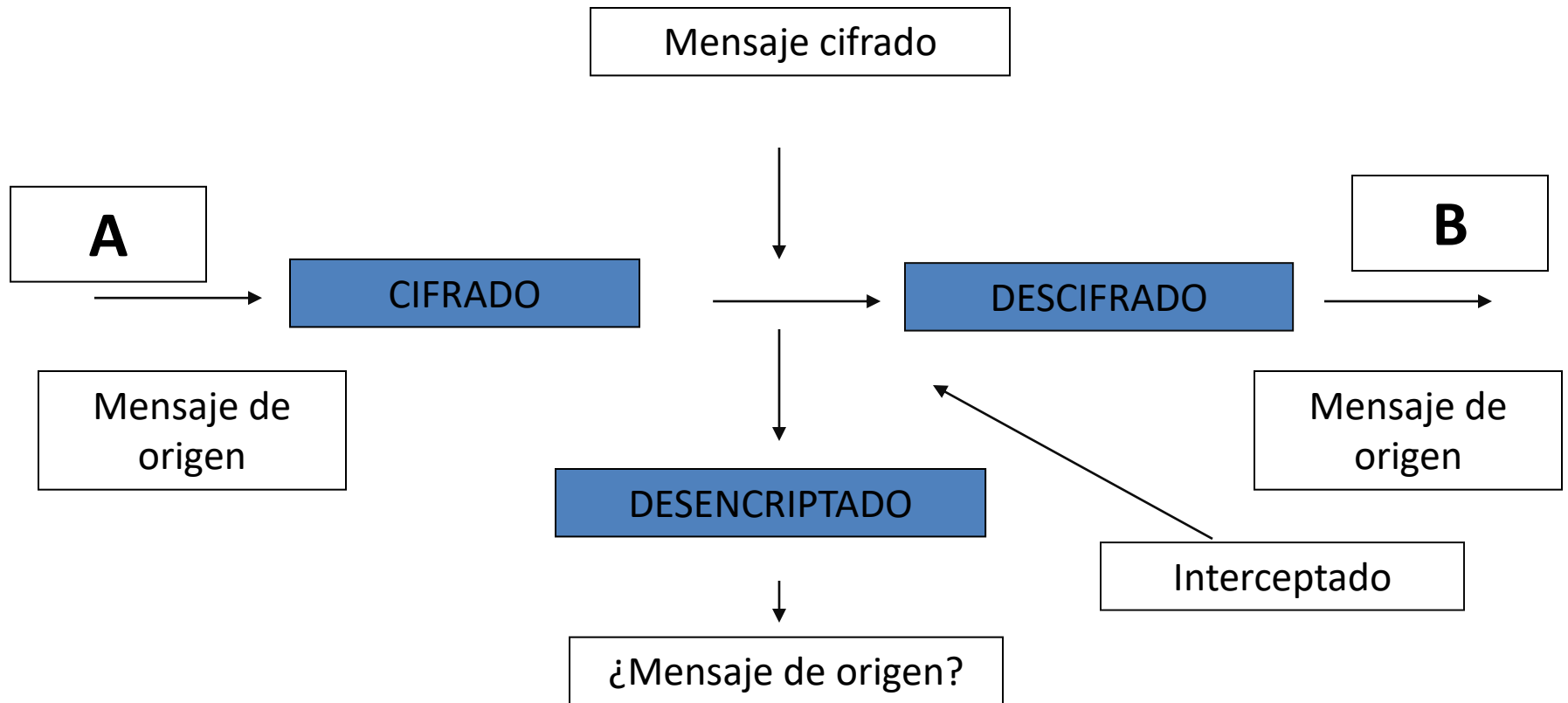
Historia de los sistemas criptográficos

Los inventores de Enigma creían que era infalible. Sin embargo cometieron numerosos errores:

1. Cadenas de texto predecibles: Mein Furher
2. Utilización de la misma clave por periodos prolongados de tiempo.
3. Cifrado del mismo texto con claves nuevas y antiguas. Hasta que un día se apoderaron de una máquina Enigma:



Proceso Criptográfico



Características de los algoritmos de encriptación

- El algoritmo de cifrado debe ser público. Para poder ser estudiado y determinar su nivel de seguridad.
- La robustez de un sistema depende de la clave utilizada.
- La clave actúa como modificador del algoritmo, de esta manera el algoritmo puede ser reutilizado.
- Es diferente la clave de la contraseña.

Tipos de algoritmos de encriptación:

Transposición: Cambiar el orden de los símbolos que forman parte del texto.

Sustitución: Reemplazan unos símbolos por otros.

Características de los algoritmos de encriptación

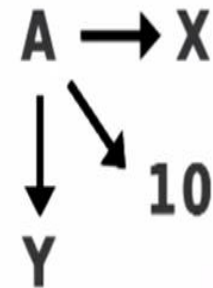
Dentro de la técnica de *sustitución*:

Sustitución monoalfabética: Cada símbolo se reemplaza solo por otro símbolo.

Sustitución polialfabética: Diversos caracteres del texto cifrado representan a un mismo carácter del texto original.



TABLA DE VIGENÈRE



Cifrado

- ❑ Es el mecanismo para proporcionar confidencialidad a través de funciones matemáticas aplicadas al mensaje transmitido.

El cifrado tiene como finalidad proteger archivos, unidades de disco o directorios de intrusiones o transmitir datos de forma confidencial. Ya en la antigüedad se utilizaban métodos criptográficos sencillos que se reducían en primera instancia a la codificación de la información que se quería proteger, permutando caracteres aislados, palabras o frases enteras del texto plano del mensaje (cifrado por **transposición o permutación**) o substituyendo los caracteres por combinaciones alternativas (cifrado por **substitución**).

Para decodificar un texto encriptado es necesario que el destinatario conozca la regla por la cual se ha cifrado el texto. En el cifrado por transposición, las permutaciones suelen llevarse a cabo a partir de una matriz (matriz de transposición) que ha de conocerse o poderse reconstruir. El cifrado por sustitución se basa en una ordenación tabular de caracteres y cifras en forma de código secreto.

Tipos De cifrado

- Simétricos o de Llave Privada (DES).
- Asimétricos o de Llave Pública (RSA).
- Híbrido (SSL).

Elementos comunes del cifrado

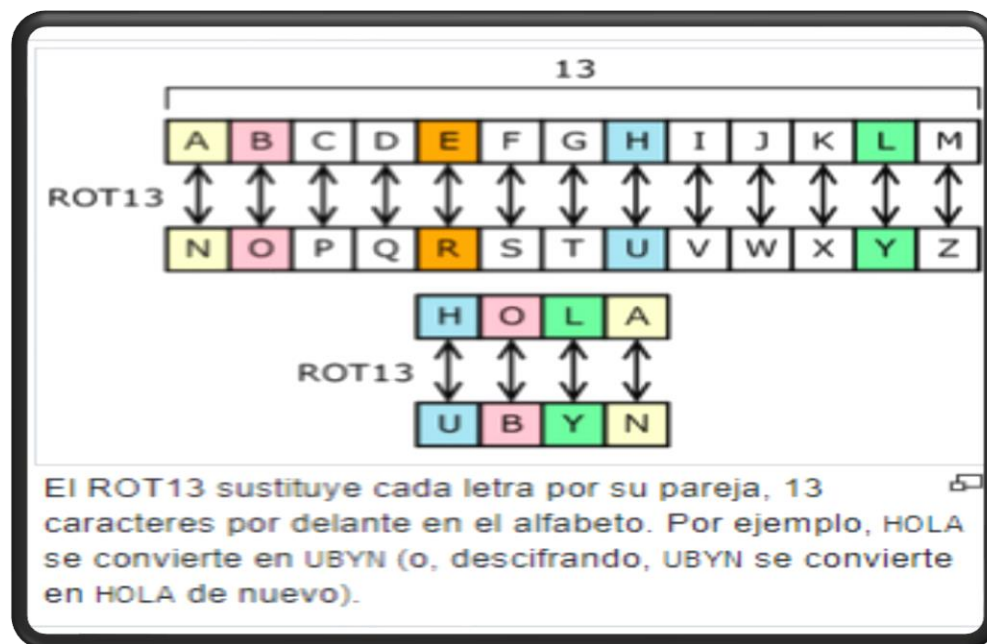
- Algoritmo cifrador (cifra y descifra datos)
- Claves de cifrado
- Longitud de clave (claves largas)
- Texto en claro (información a cifrar)
- Texto cifrado (información después de cifrar)

Algoritmos de encriptación

Uno de los primeros y más sencillos métodos de cifrado tiene su origen en la época de Cayo Julio César. Para proteger su correspondencia militar de ojos ajenos, el astuto estratega desarrolló el denominado **cifrado César**, también conocido como cifrado por desplazamiento o código de César, que se basaba en la **substitución alfabética simple** y consistía en substituir cada letra por la que se encuentra algunas posiciones más adelante en el alfabeto, en su caso, tres. La tabla de codificación resulta así:


<u>Texto</u> plano	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
<u>Código:</u>	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- **ROT13**, («rotar 13 posiciones») sencillo cifrado César

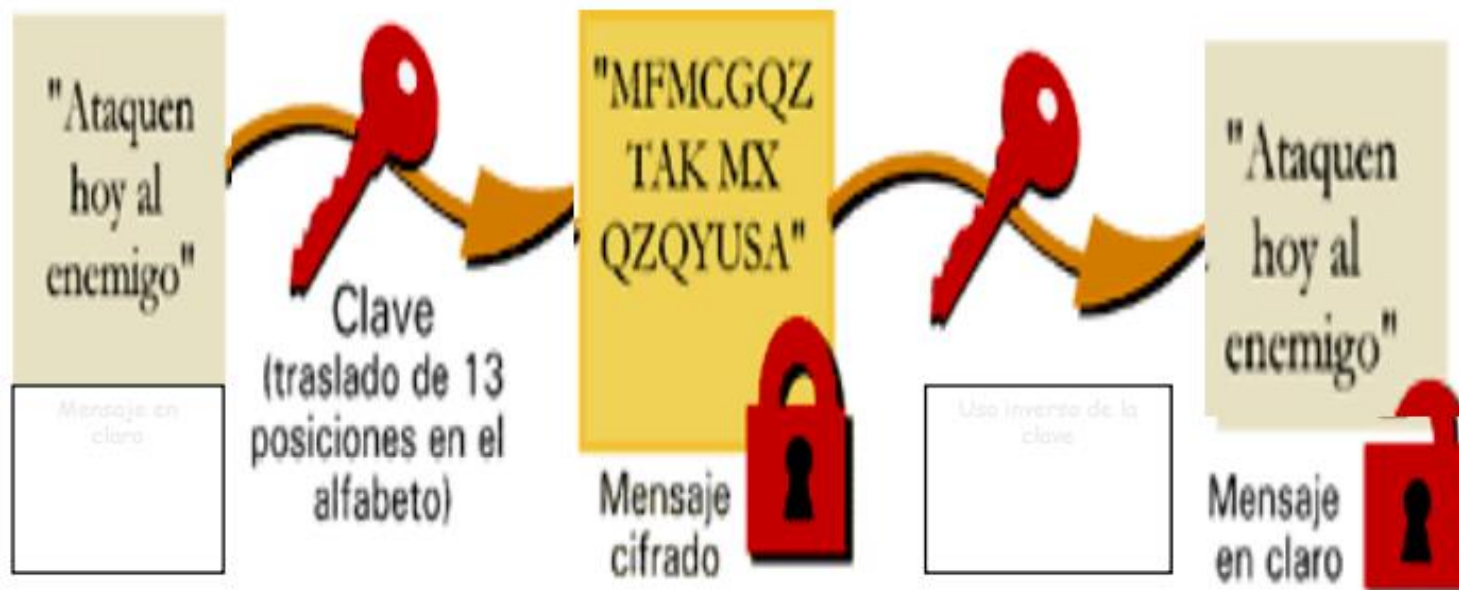


A cada letra se asigna a un número y se le suma 13, después se reemplaza el número por otra letra. Si es mayor de 26 se le resta 26 y se convierte. Ejemplo:

“HELLO” 8,5,12,12,15 + 13 = 21,18,25,25,28-26 = “URYYB”



El método de cifrado introducido por Julio César introduce el concepto de "clave criptográfica".



ALGORITMO O CRIPTOGRAFÍA SIMÉTRICA:

Hasta la década de 1970, el cifrado de la información se basaba en la criptografía simétrica, cuyos orígenes se remontan a métodos de la antigüedad como el mencionado código César. Este tipo de criptografía solo usa una clave para cifrar y descifrar un contenido.

La clave tiene que ser conocida por el emisor y el destinatario. Presenta un importante debilidad, ya que la clave puede ser interceptada en el momento en que es intercambiada. También es necesario usar tantas claves como son los destinatarios. (Ej. DES, IDEA)

D.E.S.: DATA ENCRYPTION STANDARD: ESTÁNDAR DE ENCRIPCIÓN DE DATOS:

- Es un sistema Criptográfico Simétrico.
- Es uno de los sistemas utilizados por las agencias del gobierno de EE.UU. no relacionadas con la seguridad nacional.
- Fue creado por IBM partiendo del proyecto Lucifer y propuesto al NBS (National Bureau of Standards), hoy NIST (National Institute of Standards and Technology), que lo adoptó en 1977 al igual que el ANSI (American National Standards Institute).
- Está disponible en "chips" pero su exportación está controlada por el departamento de estado de EE.UU.



D.E.S.: DATA ENCRYPTION STANDARD: ESTÁNDAR DE ENCRIPCIÓN DE DATOS:

- Cifra bloques de 64 bits en bloques de 64 bits:
 - Modificación del NBS, inicialmente eran 128.
- Utiliza una clave de 64 bits (8 de paridad, el último bit de cada byte):
 - Modificación del NBS, inicialmente eran 128.
- Divide los datos o mensajes en bloques de 64 bits y los cifra por separado.
- Utiliza un “dispositivo” denominado **SBB** (standard building block o constructor estandar de bloques):
 - Requiere como entrada un bloque de 64 bits y una clave de 48 bits.
 - Produce una salida de 64 bits.
 - Requiere 16 dispositivos sbb.



D.E.S.: DATA ENCRYPTION STANDARD: ESTÁNDAR DE ENCRIPCIÓN DE DATOS:

- En 1988 se demostró que un ataque por **fuerza bruta** contra el algoritmo DES ya era posible:
 - Gracias al avance de la informática paralela, entre otras cosas.
- La **debilidad** no está en el algoritmo, sino en la **clave**:
 - La clave no posee suficiente longitud.
 - Si se aumenta la clave el des sigue siendo seguro.
- También se conocen claves débiles y semidébiles para este algoritmo:
 - Su número es tan pequeño en comparación con el total de claves posibles que no supone un gran problema.

Variantes del DES:

- **DES múltiple:**

- consiste en aplicar el algoritmo des, con diferentes claves, varias veces.
- aumenta la seguridad ya que el des **no** posee estructura de grupo (algebraico):
 - si la poseyera significaría que:
 - habría una tercer clave que produciría el mismo resultado logrado al aplicar dos veces el des con dos claves diferentes.
 - no se habría incrementado la seguridad.
 - para un algoritmo con estructura de grupo:

$$E(E(m, k_2), k_1) = E(m, k_3)$$

Variantes del DES:

- **La variante más utilizada es el triple-des (3des):**
 - **Se eligen dos claves k_1 y k_2 , el procedimiento es el siguiente:**

$$C = E_{K_1}(D_{K_2}(E_{K_1}(M)))$$

- **La clave en este caso tendrá 112 bits y 16 de paridad (128 en total).**

2) Criptografía Asimétrica:

- Utiliza complicados algoritmo matemáticos con números primos grandes y curvas elípticas.
- Cada usuario ha de poseer una pareja de claves:
 - * **Clave privada;**
 - * **Clave pública.**



Criptosistema RSA

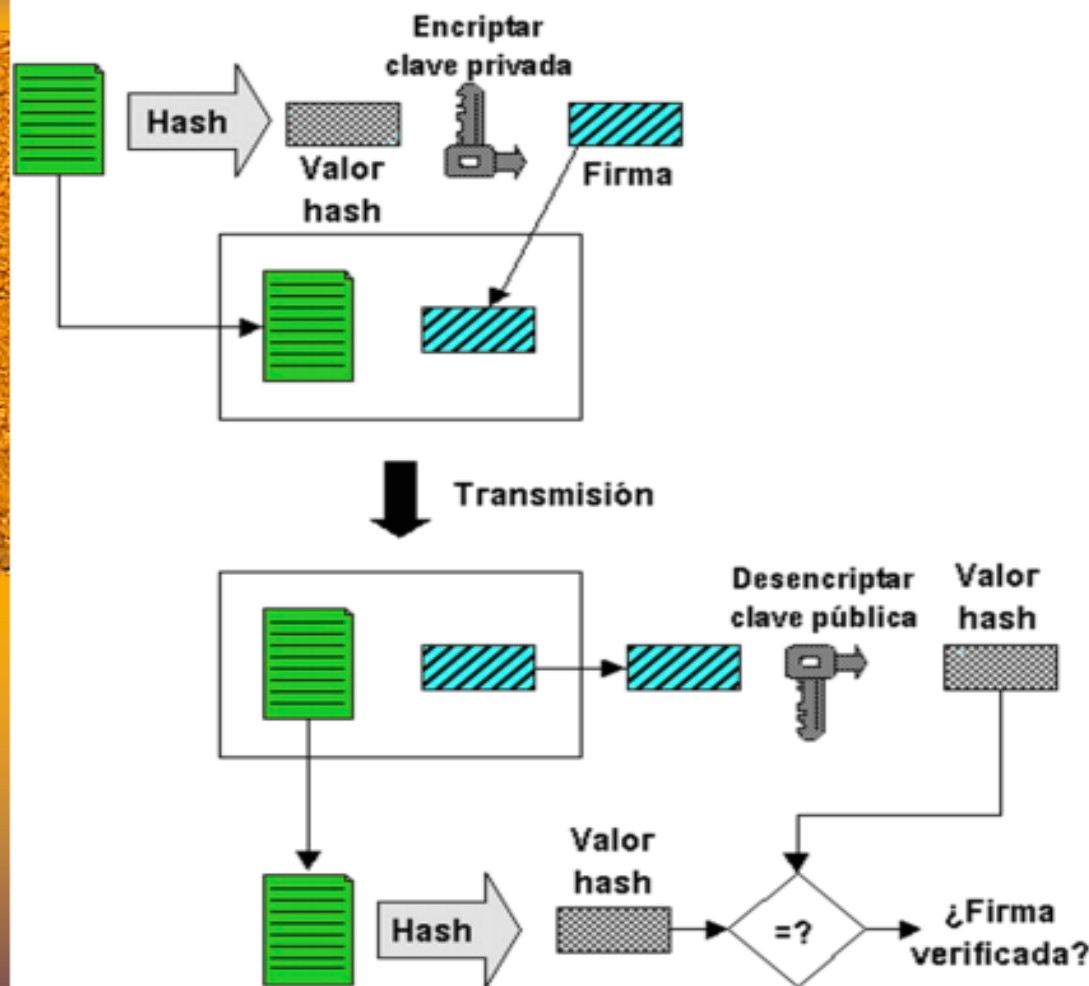
- Las siglas provienen de su inventor (Rivest, Shamir, Adleman).
- Emplea las ventajas proporcionados por las propiedades de los n^o primos, ya que su robustez se basa en la facilidad para encontrarlos.
- **DES** implementado en software es 100 veces más rápido que **RSA**. Por tanto para mensajes cortos se debe utilizar RSA y para los largos DES.
- Desde el punto de vista de la confidencialidad los algoritmos asimétricos proporcionan una mayor seguridad que los simétricos a costa de una mayor carga computacional. Es por esta razón que generalmente se emplea una combinación de ambos.

Firmas digitales

Permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación.

Son una solución que ofrece la criptografía para verificar:

- La integridad de documentos.
- La procedencia de documentos.
- Se basa en la criptografía de clave pública o asimétrica.
- Se puede definir una función Hash como aquella que reduce el mensaje a un conjunto de datos, denominado resumen, de longitud mucho menor que el mensaje, usualmente 128 ó 254 bits y que viaja junto con el mensaje original.



1. E genera un resumen del documento.
2. E cifra el resumen con su clave privada, firmando por tanto el documento. Este resumen es su firma digital.
3. E envía el documento junto con el resumen firmado (la firma digital) a R.
4. R genera un resumen del documento recibido de E, usando la misma función unidireccional de resumen.
5. Después R descifra con la clave pública de E, que es conocida, el resumen firmado (firma digital de E).
6. Si el resumen firmado coincide con el resumen que él ha generado, la firma digital es válida.



Algunas aplicaciones de la firma digital

Se puede aplicar en las siguientes situaciones:

- E-mail.
- Contratos electrónicos.
- Procesos de aplicaciones electrónicos.
- Formas de procesamiento automatizado.
- Transacciones realizadas desde financieras alejadas.
- Transferencia en sistemas electrónicos.
- En aplicaciones de negocios, un ejemplo es el (EDI).
intercambio electrónico de datos de computadora a computadora intercambiando mensajes que representan documentos de negocios.

Algoritmos criptográficos

- Función Hash o de Digestión del mensaje:
 - No involucran el uso de claves
 - Determina una suma de verificación única (checksum) criptográfica sobre el mensaje
 - El algoritmo más usado es el MD5 (Message Digest versión 5)

Ventajas del cifrado

- Protege la información almacenada en la computadora contra accesos no autorizados
- Protege la información mientras transita de un sistema de cómputo a otro
- Puede detectar y evitar alteraciones accidentales o intencionales a los datos
- Puede verificar si el autor de un documento es realmente quien se cree que es.

Desventajas del cifrado

- No puede prevenir que un agresor borre intencionalmente todos los datos
- No es posible saber si está siendo descifrado.
- Acceder al archivo antes de que sea cifrado o después de descifrar

Niveles De Seguridad En Encriptación

En las comunicaciones los más seguros son los algoritmos AES Y 3DES:

- **El algoritmo AES (Advanced Encryption Standard)** es uno de los algoritmos más seguros que existen hoy en día. Está clasificado por la National Security Agency (NSA) de EE.UU. para la más alta seguridad de la información secreta. Se basa en varias sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloque de datos de 16 bytes, que se repiten varias veces.

Hasta el momento no existe posibilidad de ataque contra AES, por lo que este algoritmo sigue siendo el estándar de cifrado preferido por gobiernos, bancos y sistemas de alta seguridad de todo el mundo.

Niveles De Seguridad En Encriptación

- **El algoritmo 3DES (Triple Data Encryption Standard)**, se basa en el algoritmo DES, que aplica una serie de operaciones básicas para convertir un texto en otro cifrado, empleando una clave criptográfica. 3DES es el algoritmo que hace triple cifrado del DES; se basa en aplicarlo tres veces, con tres claves distintas, por lo que resulta mucho más seguro.

Este método está siendo paulatinamente sustituido por el AES, ya que éste tiene una velocidad hasta seis veces más rápida, sin embargo, aún existen medios de pago electrónicos, tarjetas de crédito, etc. que utilizan el estándar 3DES, por lo que continua estando muy vigente.

Sistemas de claves privadas

- RC2
 - Cifrador de bloque permite de 1 a 2048 bits
- IDEA – International Data Encryption Algorithm
 - Usa una clave de 128 bits, utilizado por el programa PGP (para e-mail).
- SKIPJACK
 - Utilizado por el circuito integrado de cifrado CLIPPER, utiliza 80 bits

Sistemas de clave privada – DES (Data Encryption Std. IBM-1980)

- Usa las técnicas de confusión y difusión
- Cifra por bloques de 64 bits con una llave secreta de 64 bits (56 útiles y 8 de paridad)
- Realiza 16 iteraciones y en cada una hace una sustitución y una permutación con la llave.
- En Hardware es más rápido hasta 1Gb/seg.
- La llave privada se puede enviar con cada mensaje