Navegación segura en Internet

Juan Fdo. Hurtado R.

juan.hurtado@comfenalcoantioquia.com
fhenet@yahoo.es

Comfenalco ANTIOQUIA

OBJETIVOS

- Tener claros conceptos relacionados con la criptografía
- Conocer los tipos de sistemas criptográficos
- Identificar los protocolos para navegación segura en Internet
- Reconocer sitios en Internet que brinden un entorno seguro para el comercio electrónico
- Utilizar herramienta para analizar tráfico y conocer servidores de correo seguro

AGENDA

- Sistemas criptográficos
  - Definición
  - Origen
  - Sistemas simétricos
  - Sistemas asimétricos
- Protocolos de seguridad
  - Transporte seguro
    - SSL
    - SSH
- E-commerce
  - Firma digital
  - Certificado digital
- Correo seguro

Sistemas criptográficos: Definición

- **Criptografía se considera la rama inicial de las Matemáticas y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto, proteger un mensaje o archivo por medio de un algoritmo usando una o más claves.**

- Esto dará lugar a diferentes tipos de sistemas de cifra, denominados criptosistemas, que nos permiten asegurar al menos tres de los cuatro aspectos básicos de la seguridad informática: la confidencialidad o secreto del mensaje, la integridad del mensaje y autenticidad del emisor, así como el no repudio mutuo entre emisor (cliente) y receptor (servidor).

Sistemas criptográficos: Origen

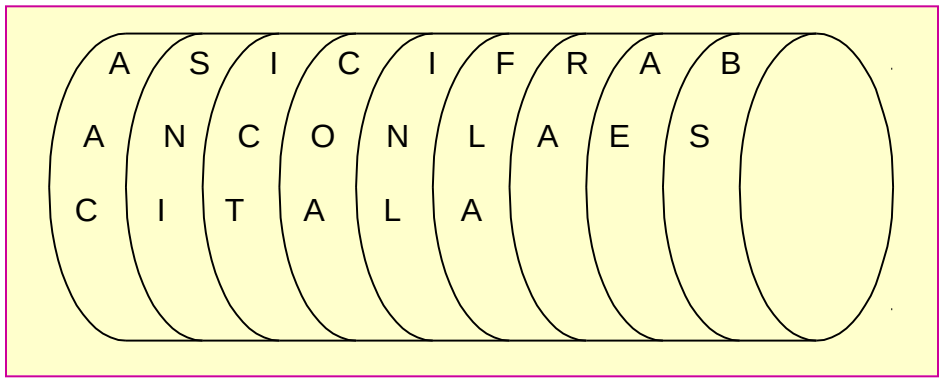
- La criptografía clásica abarca desde tiempos inmemoriales hasta la mitad del siglo XX.
- El punto de inflexión en esta clasificación la marcan tres hechos relevantes:
  - En el año 1948 se publica el estudio de Claude Shannon sobre la Teoría de la Información.
  - En 1974 aparece el estándar de cifra DES.
  - Y en el año 1976 se publica el estudio realizado por Whitfield Diffie y Martin Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifra, denominado cifrado con clave pública.

Sistemas criptográficos: Origen

- Primer cifrador por transposición: escítala
  - La escítala era usada en el siglo V a. d. C. por el pueblo griego de los lacedemonios. Consistía en un bastón en el que se enrollaba una cinta de cuero y luego se escribía en ella el mensaje de forma longitudinal.
  - Al desenrollar la cinta, las letras aparecerán desordenadas.
  - Para descifrar el criptograma y recuperar el mensaje en claro habrá que enrollar dicha cinta en un bastón con el mismo diámetro que el usado en el extremo emisor y leer el mensaje de forma longitudinal. La clave del sistema se encuentra en el diámetro del bastón. Se trata de una cifra por transposición pues los caracteres del criptograma son los mismos que en el texto en claro pero están distribuidos de otra forma dentro del criptograma.

Sistemas criptográficos: Origen

Bastón y cinta para cifrar



En ese bastón residía la fortaleza de un pueblo.

Por ello, y como símbolo de poder, el bastón de mando que se le entrega al alcalde de una ciudad en la ceremonia de su nombramiento, proviene de estos tiempos tan remotos.

El texto en claro es:

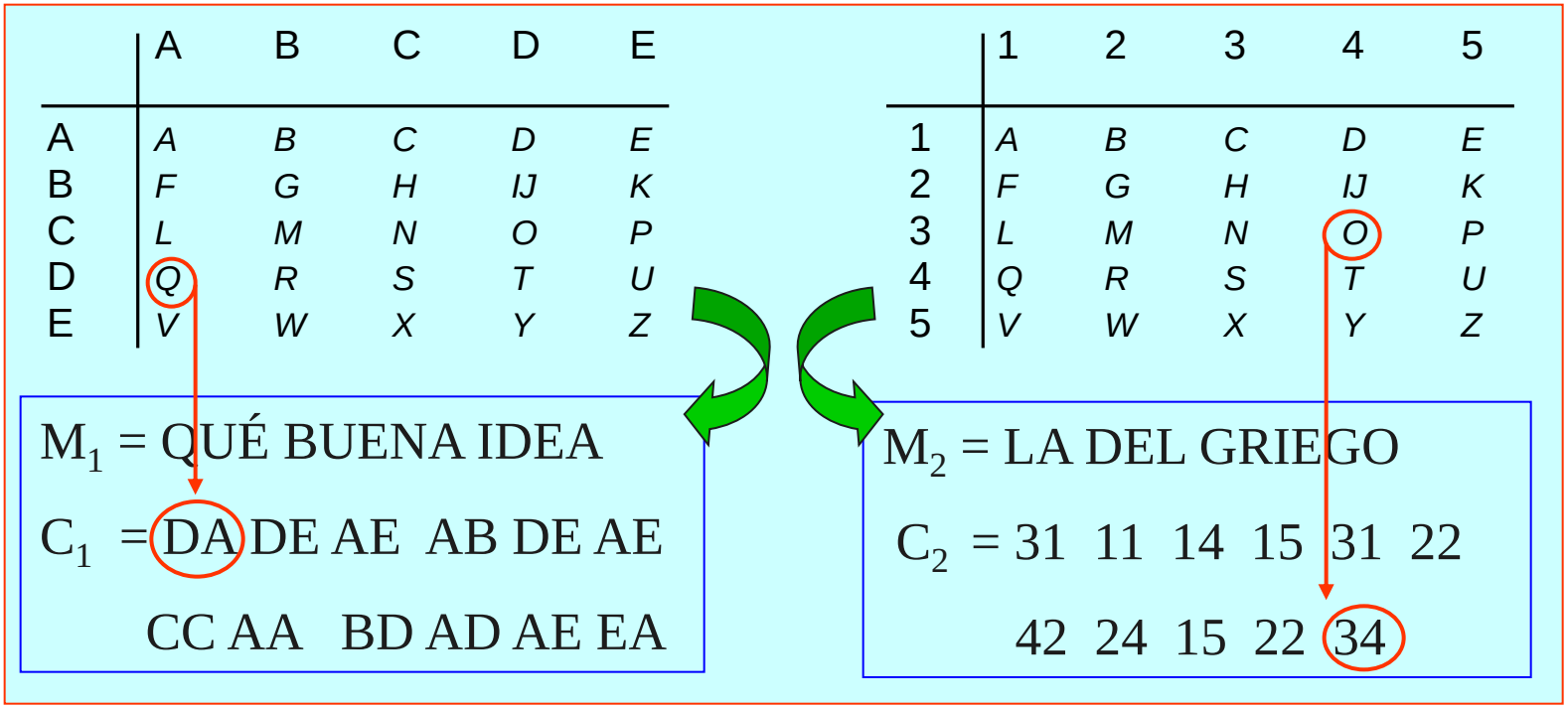
M = ASI CIFRABAN CON LA ESCITALA

El texto cifrado o criptograma será:

C = AAC SNI ICT COA INL FLA RA AE BS

Sistemas criptográficos: Origen

- Primer cifrador por sustitución: Polybios
  - Es el cifrador por sustitución de caracteres más antiguo que se conoce (siglo II a. d. C.) pero como duplica el tamaño del texto en claro, con letras o números, ... no fue tan buena la idea.



Sistemas criptográficos: Origen

- El cifrador del César
  - En el siglo I a.d.C., Julio César usaba este cifrador. El algoritmo consiste en el desplazamiento de tres espacios hacia la derecha de los caracteres del texto en claro. Es un cifrador por sustitución monoalfabético en el que las operaciones se realizan módulo n, siendo n el número de elementos del alfabeto (en aquel entonces el latín).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
M_i	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
C_i	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Sistemas simétricos

- Existirá una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra por lo que la seguridad reside en mantener dicha clave en secreto.

Ej: DES (Data Encryption Standard)

Sistemas simétricos: DES

- Esquema de encriptación simétrico desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de EEUU en colaboración con la empresa IBM
- Se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones.

Sistemas asimétricos

- Cada usuario crea un par de claves, una privada y otra pública, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa. La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública.

Ej: Diffie y Hellman y RSA

Sistemas asimétricos: RSA

- El algoritmo de clave pública RSA fue creado en 1978 por Rivest, Shamir y Adlman, y es el sistema criptográfico asimétrico más conocido y usado. Estos señores se basaron en el artículo de Diffie-Hellman sobre sistemas de llave pública, crearon su algoritmo y fundaron la empresa RSA Data Security Inc., que es actualmente una de las más prestigiosas en el entorno de la protección de datos.
- En cuanto a las longitudes de claves, el sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 ordenadores trabajando juntos para hacerlo).
- Claves compuestas por un exponente y un módulo que es producto de 2 números primos (grandes).

Protocolos de seguridad

- SSL (Secure Socket Layer)
- SSH (**S**ecure **SH**ell)

Protocolos de seguridad: SSL

- SSL (Secure Socket Layer - Capa de Conexiones Seguras) es un protocolo que corre sobre TCP (protocolo de transporte punto a punto de Internet) y fue propuesto por Netscape Communications Corporation. Este se compone de dos capas y funciona de la siguiente manera:
  - La primera capa se encarga de encapsular los protocolos de nivel más alto
  - La segunda capa que se llama SSL Handshake Protocol se encarga de la negociación de los algoritmos que van a encriptar y también la autenticación entre el cliente y el servidor.

- Cuando se realiza una conexión inicial el cliente lo primero que hace es enviar una información con todo los sistemas de encriptación que soporta, el primero de la lista es el que prefiere utilizar el cliente. Entonces el servidor responde con una clave certificada e información sobre los sistemas de encriptación que este soporta.

Protocolos de seguridad: SSL

- Entonces el cliente seleccionará un sistema de encriptación, tratará de desencriptar el mensaje y obtendrá la clave pública del servidor.

- Este método de seguridad es de lo mejor ya que por cada conexión que se hace el servidor envía una clave diferente. Entonces si alguien consigue desencriptar la clave lo único que podrá hacer es cerrarnos la conexión que corresponde a esa clave.

- Cuando se logra este primer proceso que es la sesión solamente, los que actuarán ahora son los protocolos de capa 7 del OSI o sea la capa de Aplicación, claro que todo lo que se realice a partir de que tenemos una sesión SSL establecida estará encriptado con SSL.

Protocolos de seguridad: SSH

- Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo el ordenador mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X arrancado.

- Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro de SSH.

E-commerce

- Para el comercio electrónico se han desarrollado elementos como la firma digital y el certificado digital.

E-commerce: Firma digital

Es una firma electrónica que puede ser utilizada para autenticar la identidad de quien envía un mensaje o quien firma un documento, y hace posible garantizar que el contenido original de un mensaje o documento ha sido enviado sin modificaciones.

Requisitos de la firma digital:

a) Debe ser fácil de generar.
b) Será irrevocable, no rechazable por su propietario.
c) Será única, sólo posible de generar por su propietario.
d) Será fácil de autenticar o reconocer por su propietario y los usuarios receptores.
e) Debe depender del mensaje y del autor.

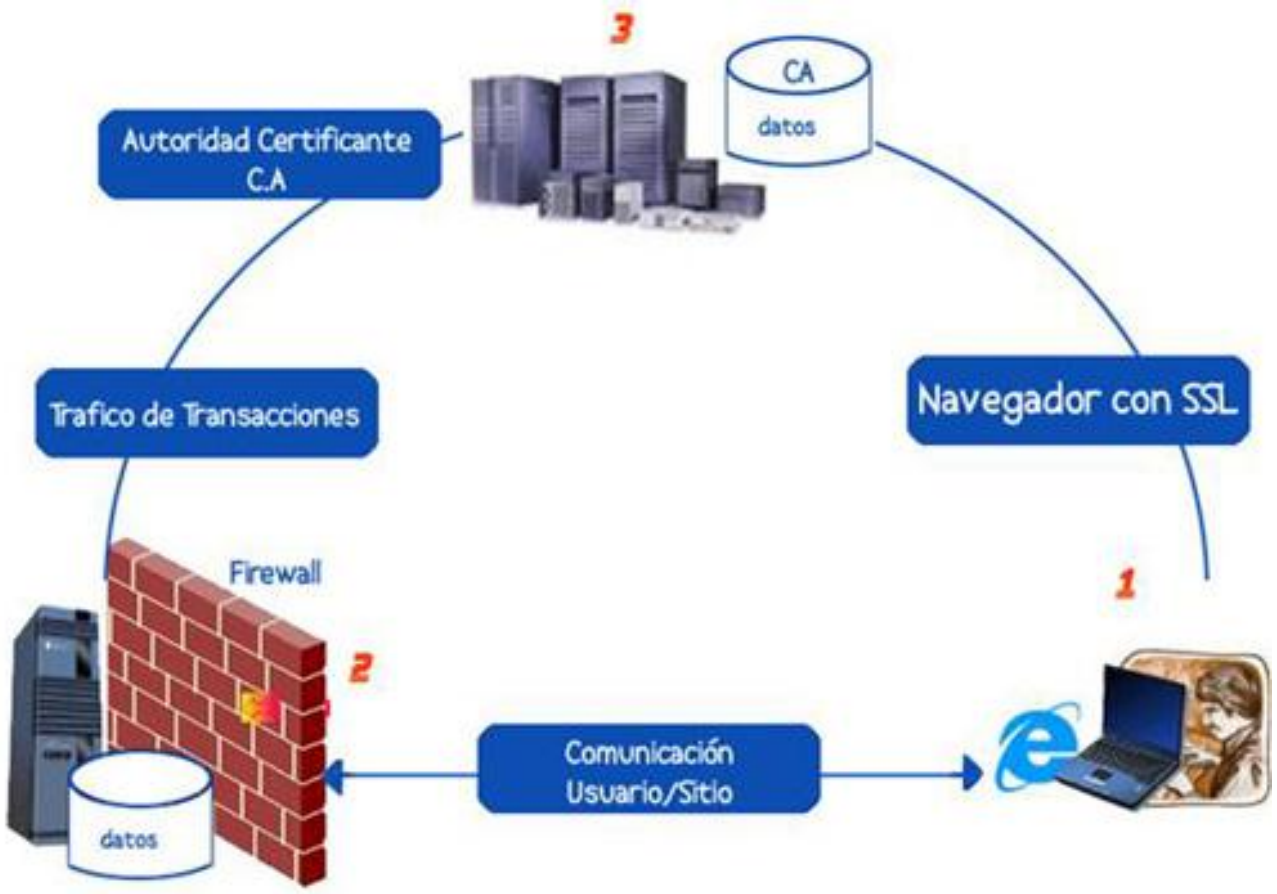
E-commerce: Certificado digital

Un certificado digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Un Certificate Authority (CA) es generalmente una empresa que emite certificados digitales.

- Verifican la información de la entidad solicitante y crea un certificado que contiene la clave pública de ésta además de información que la identifica.
- La CA utiliza su clave privada para generar una firma digital asociada al certificado que garantiza que realmente fue expedido por ella.
- Ejemplos:
  - Certicámara (www.certicamara.com)
  - VeriSign (www.verisign.com)
  - US Postal Service (www.usps.com)
  - CommerceNet (www.commercenet.com)

E-commerce: Certificado digital



E-commerce: Certificado digital

Un certificado contiene la siguiente información:

- Dominio para el que se expidió (por ejemplo http://www.segurired.com/)
- Dueño del Certificado
- Domicilio del Dueño
- Y la fecha de validez del mismo.
- Un ejemplo es cuando compramos un libro de amazon.com o virtualexito.com o hacemos una transacción en un entidad bancaria (www.grupobancolombia.com)

- El estándar X509 define cómo manejar claves públicas a través de certificados.

Correo seguro

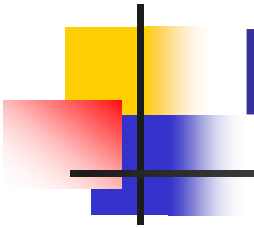
- Ingresar a cuentas de correo desde Mozilla Firefox y activar la opción de recordar contraseñas.
- Verificar las opciones de Mozilla para identificar las cuentas almacenadas y sus contraseñas.
- Instalar un analizador de protocolos de red para verificar el tráfico en tiempo real.
- Realizar pruebas a servidores de correo no seguros para rastrear cuentas de correo y comparar información con servidores seguros.

CONCLUSIONES

- En un sistema de información se deben definir políticas claras de seguridad
- Igualmente, se deben llevar procedimientos adecuados de respaldo y monitoreo de la red.
- Los sistemas criptográficos son fundamentales para establecer seguridad a través del comercio electrónico.
- Para realizar transacciones a través de Internet se debe verificar la validez del sitio.

BIBLIOGRAFÍA

- Libro Electrónico de Seguridad Informática y Criptografía Versión 4.1
- http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html
- http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/rsa.html
- http://www.iec.csic.es/criptonomicon/ssl.html
- http://es.wikipedia.org/wiki/Secure_Shell
- http://http://www.dit.upm.es/doc/acceso/introduccion.html



Dudas o Preguntas

FIN