

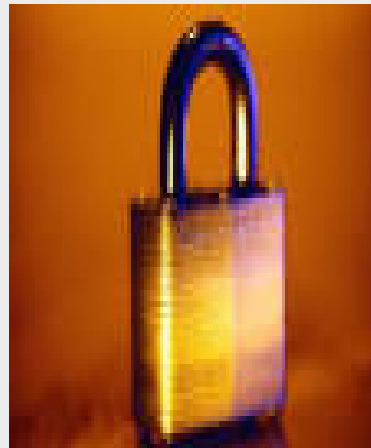
UNIVERSIDAD NACIONAL DEL NORDESTE

FACULTAD DE CIENCIAS EXACTAS
Y NATURALES Y AGRIMENSURA

Litwak, Noelia Desiree



SEGURIDAD INFORMATICA



Y

CRIPTOGRAFIA

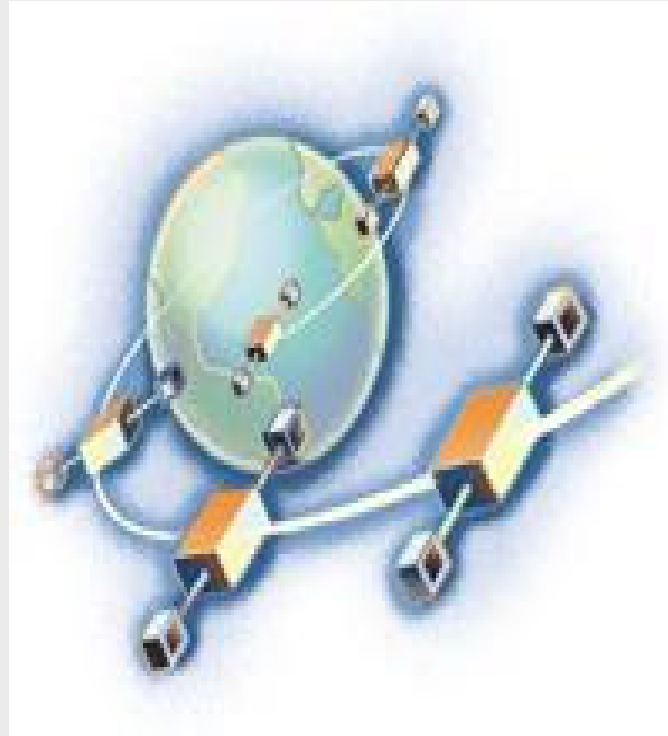


Por que la seguridad?

La masiva utilización de las computadoras y redes como medios para ***almacenar, transferir y procesar*** información se ha incrementado en los últimos años, al grado de convertirse en un elemento indispensable para el funcionamiento de la sociedad actual.

Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe ***proteger y asegurar*** para garantizar su ***integridad, confidencialidad y disponibilidad***, entre otros servicios de seguridad.

INTERNET



- Son abiertas y accesibles,

-Permiten intercambios rápidos y eficientes a nivel mundial y a bajo costo.

- Este concepto hace posible nuevas formas de funcionamiento de la sociedad actual que se ve dificultada por las inseguridades que van dejando al descubierto.

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción ***a conductas antisociales y delictivas*** manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de ***cometer delitos tradicionales en formas no tradicionales.***



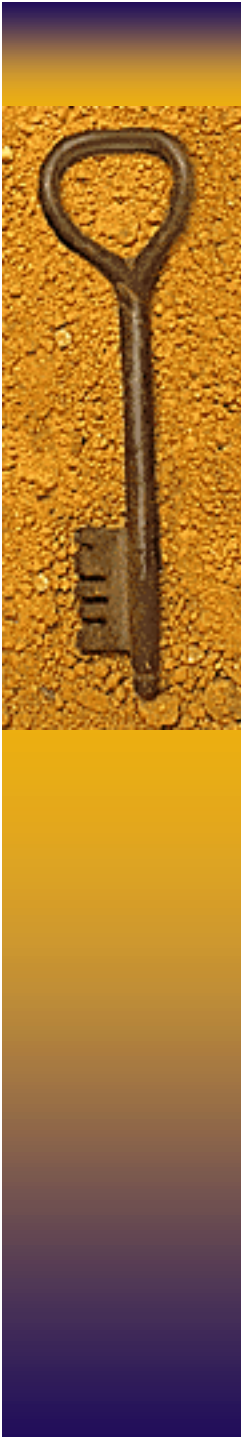


DEFINICIÓN FORMAL:

Se entiende por seguridad de los sistemas de información al conjunto de recursos:

- ◆ metodologías,
- ◆ planes,
- ◆ políticas,
- ◆ documentos,
- ◆ programas ó dispositivos físicos,

encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.



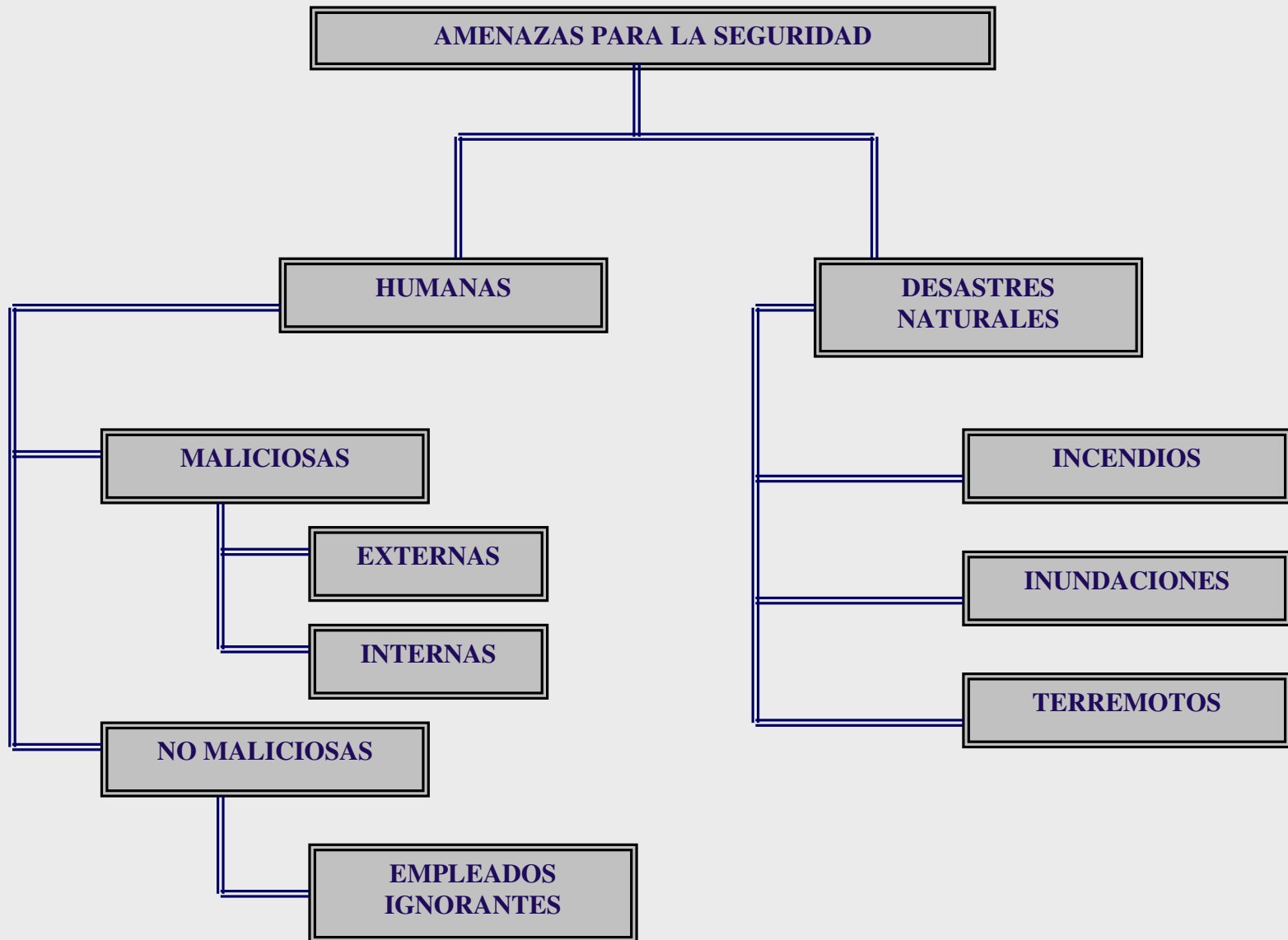
◆ **La Seguridad Informática debe vigilar principalmente por las siguientes propiedades:**

- ◆ **Confidencialidad**
- ◆ **Integridad**
- ◆ **Control**
- ◆ **Disponibilidad**
- ◆ **Autenticación**



- **Análisis del Objetivo de la Seguridad Informática,**
- **Requisitos,**
- **Seguridad:**
 - **Como Problema Cultural**
 - **Como Proceso.**

AMENAZAS PARA LA SEGURIDAD



Las amenazas pueden ser analizadas en tres momentos:

- ◆ La prevención (antes)
- ◆ La detección (durante)
- ◆ La recuperación (después)



Seguridad Física:

“Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos o información confidencial”.



Seguridad Lógica:

“Aplicación de barreras y procedimientos que resguarden el acceso a los datos y accedan a ellos sólo personas autorizadas”.

ESTRATEGIAS DE SEGURIDAD

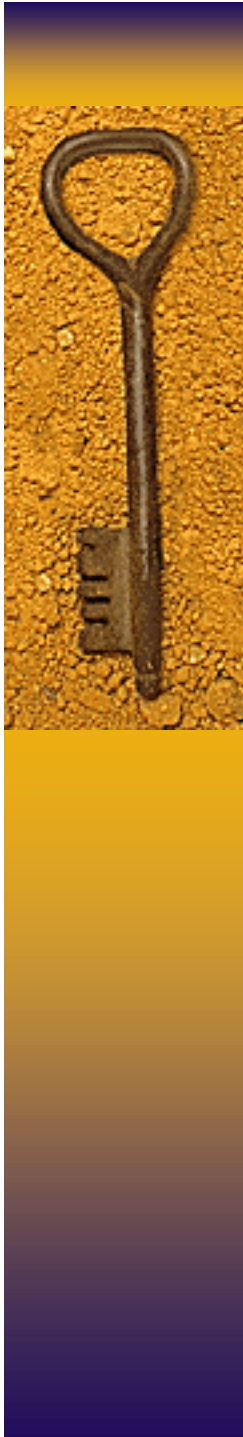
- ◆ 1) Creación política de la seguridad
El diseñar una estrategia de seguridad depende en general de la actividad que se desarrolla, sin embargo se pueden considerar tres
- 2) Realizar un análisis de riesgo.
- 3) Aplicar las medidas correspondientes de
pasos generales.
seguridad.





CRIPTOGRAFIA

- ◆ Para subsanar problemas relativos a la seguridad, surgieron distintos métodos o estrategias, siendo uno de los más antiguos pero actualmente utilizados: la criptografía
- ◆ Proviene del griego ***kryptos*** (esconder) y ***gráphein*** (escribir), es decir “Escritura escondida”

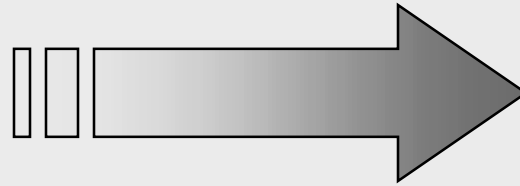


- ◆ Si bien no se la conocía como ciencia la criptografía existe desde muchísimos años atrás.
- ◆ Se dice que uno de los primeros algoritmos tuvo su origen durante el Imperio Romano, en la época de Julio César.
- ◆ César utilizó un esquema criptográfico simple pero efectivo para comunicarse con sus generales



Por ejemplo:

A



M

B



N

C

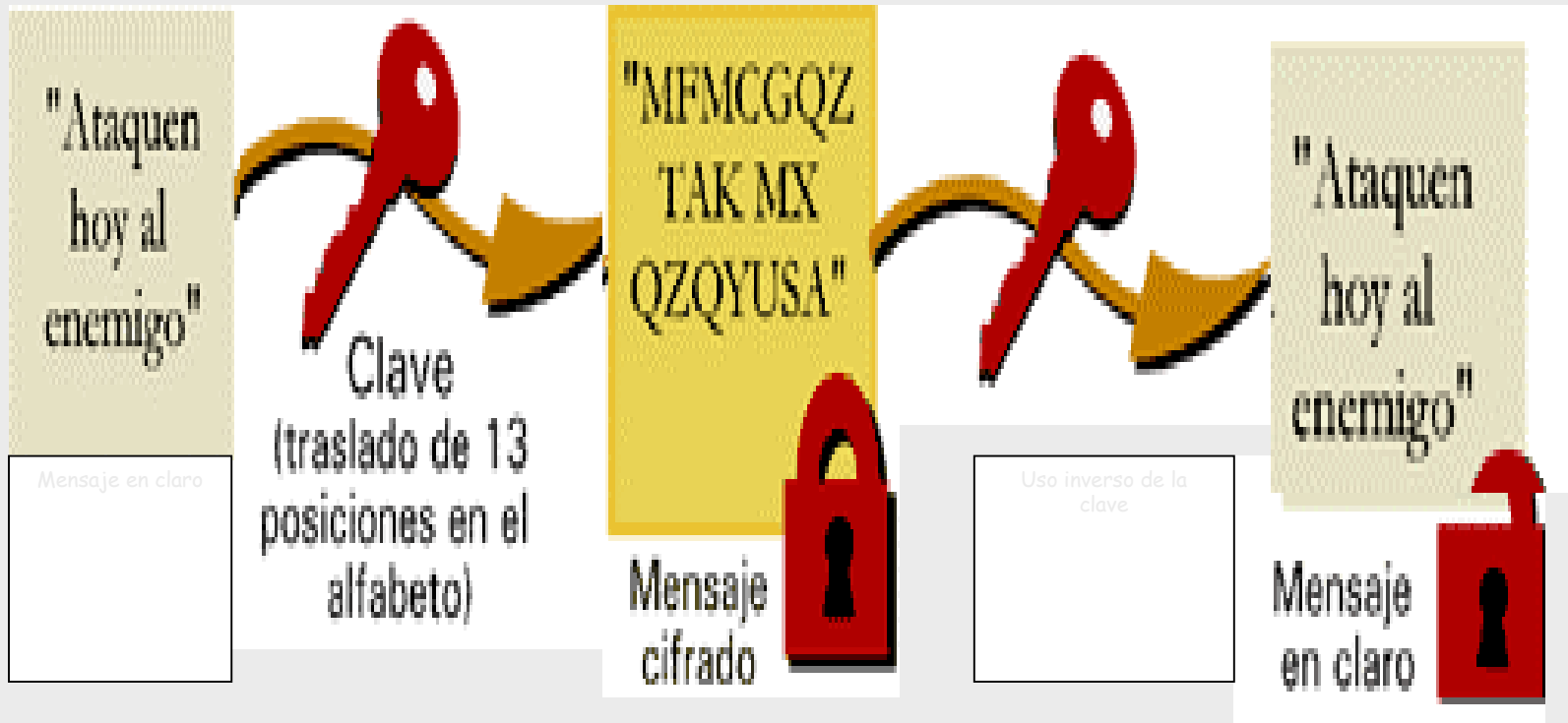


O

13



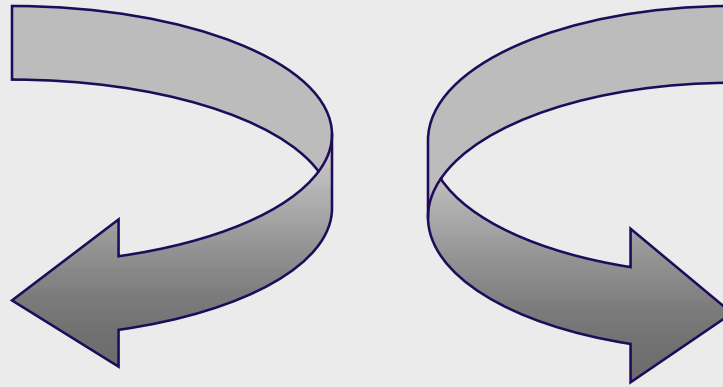
El método de cifrado introducido por Julio César introduce el concepto de "clave criptográfica".





Básicamente la criptografía se divide en dos ramas:

CRIPTOGRAFIA:



**1) CLAVE
PRIVADA O
SIMÉTRICA**

**2) CLAVE
PÚBLICA O
ASIMÉTRICA**

1) Criptografía Simétrica:

- ◆ Conjunto de métodos que permite una comunicación segura entre las partes componentes.
- ◆ Siempre y cuando previamente se haya intercambiado una clave que llamaremos clave simétrica,
- ◆ La simetría se refiere a que las partes usan la misma llave para cifrar, como para descifrar.



DES (Data Encryption Estándar)

- ◆ Es el más conocido;
- ◆ Desarrollado originalmente por IBM;
- ◆ Modificado y adaptado por el gobierno de los EE.UU;
- ◆ Trabajaba sobre bloques de 128 bits;
- ◆ Teniendo clave de igual longitud;
- ◆ Se basaba en operaciones lógicas booleanas.



**A
n
t
e
s**



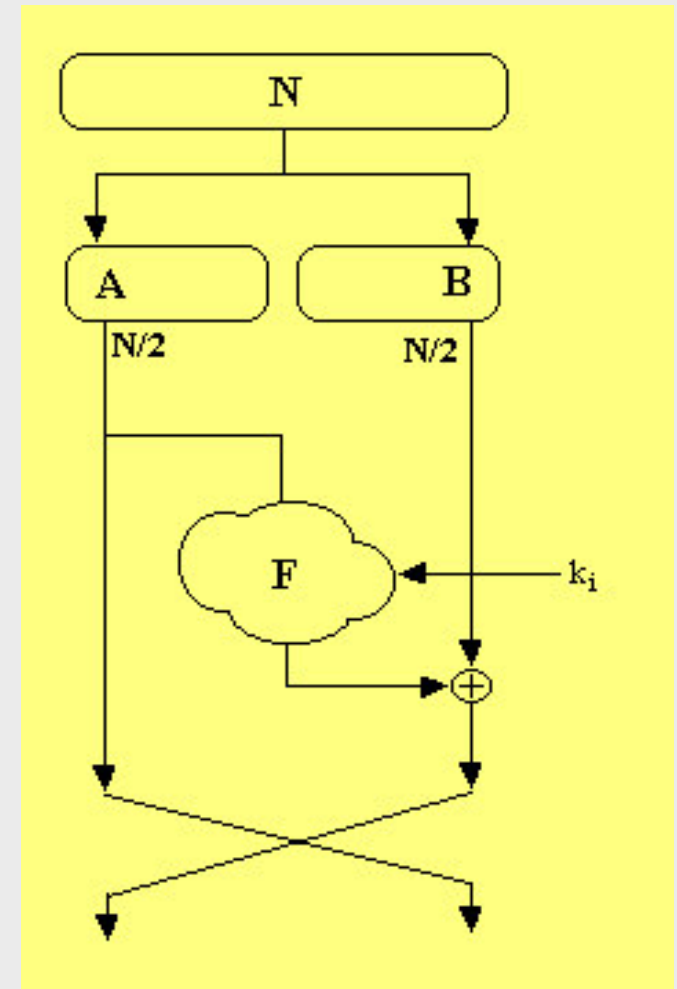
**A
h
o
r
a**

- ◆ Se produjo la reducción de clave y de bloques;
- ◆ DES tiene 19 etapas diferentes;
- ◆ La primera es una transposición, una permutación inicial (IP) del texto plano de 64 bits, independientemente de la clave.
- ◆ La última etapa es otra transposición (IP⁻¹), la inversa de la primera.
- ◆ La penúltima etapa intercambia los 32 bits de la izquierda y los 32 de la derecha.
- ◆ Las 16 etapas restantes son una red de Feistel de 16 iteraciones.

Cifrado de Feistel



- ◆ El bloque de datos se divide en dos mitades;
- ◆ En cada vuelta de encriptación se trabaja, con una de las mitades.





◆ *Seguridad en DES:*

- mediados de 1.988.
- debilidad no del algoritmo.
- sino que la tiene la clave.

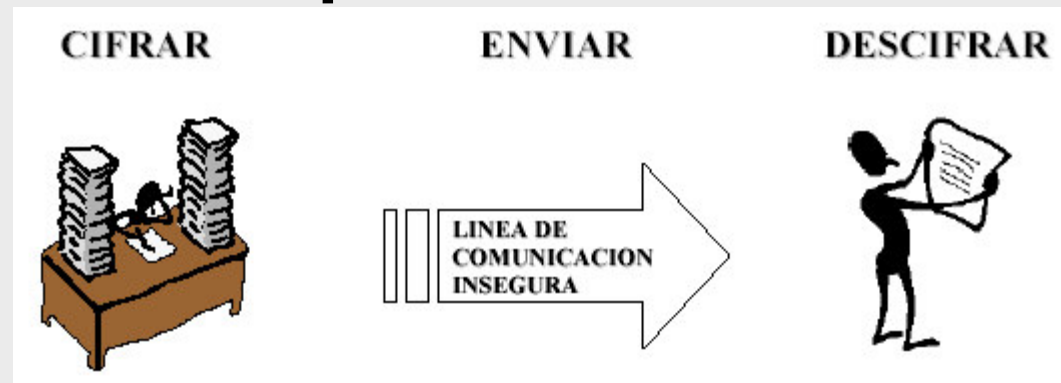
◆ *Variantes del DES:*

- DES múltiple:

- aplicar el algoritmo DES ,
- con diferentes claves,
- varias veces.

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° primos, ya que su robustez se basa en la dificultad 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



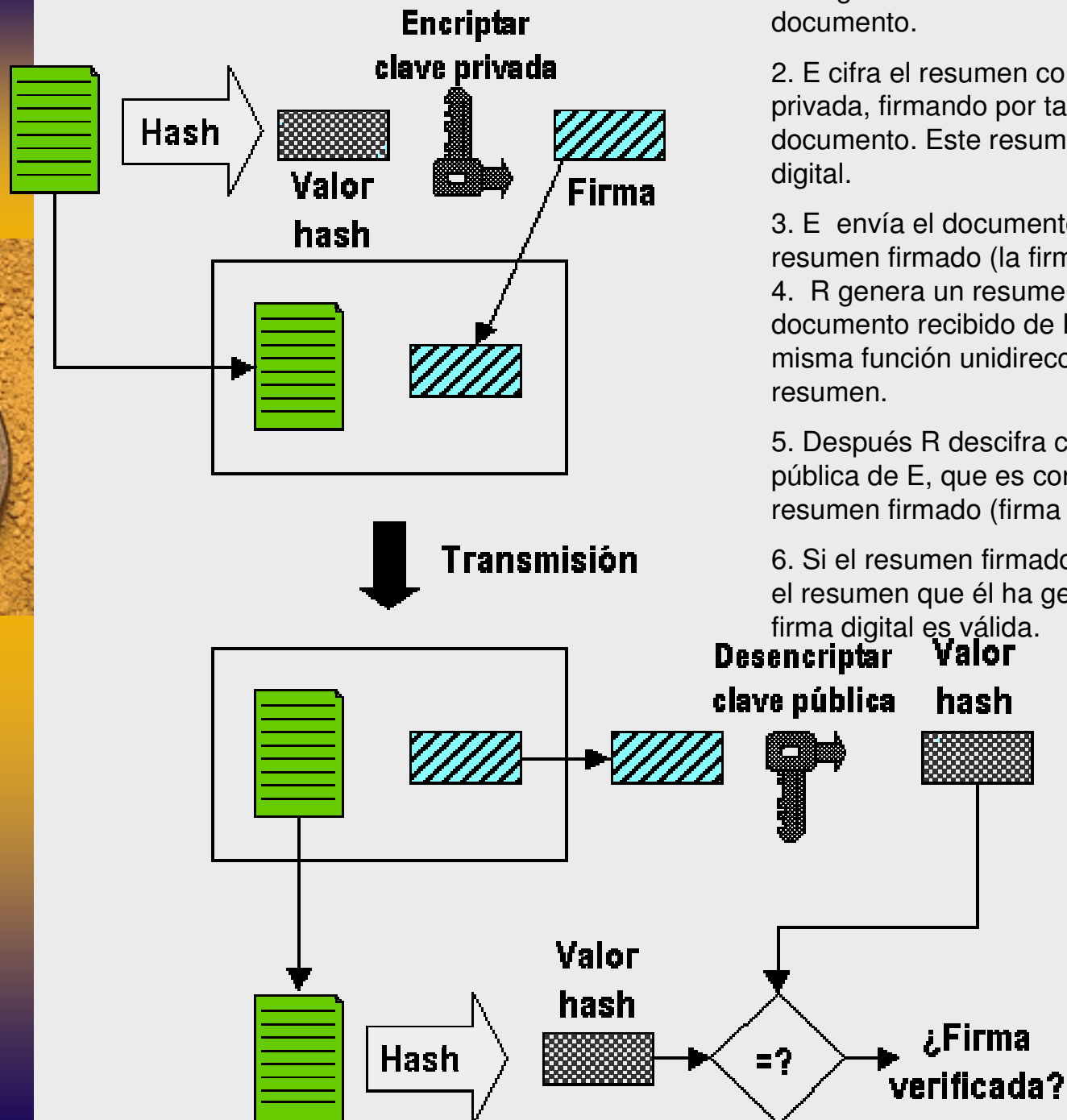
Permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación.

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.
- ◆ 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.



CERTIFICADOS DIGITALES

- 
- ◆ Para evitar esto se recurre a lo que se denomina los certificados de clave pública, y pública) independientemente del número que son emitidos por unas entidades de confianza llamadas Autoridades Certificadoras (CAs, Certification Authorities) y que
 - ◆ El único requisito que se ha de cumplir es la integridad de la clave, para así evitar que un posible atacante sustituya una clave pública y suplante a su usuario legítimo.



Estas entidades permiten garantizar los servicios de confidencialidad e integridad de los datos y el no repudio de origen y destino.

Una arquitectura de gestión de certificados (Public Key Infrastructure) ha de proporcionar un conjunto de mecanismos para que la autenticación de emisores y recipientes sea simple, automática y uniforme, independientemente de las políticas de certificación empleadas.

Las CAs tienen como misión la gestión de los denominados certificados (de clave pública).

Un certificado esta compuesto por varios campos:

- Identidad del propietario,**
- Clave pública,**
- Periodo de validez,**
- Identidad y clave pública de la CA que lo expidió,**
- Firma digital del certificado. (realizada por la CA).**



CONCLUSIÓN:

- ◆ Finalmente debemos mencionar que no existe un sistema computarizado que garantice al 100% la seguridad de la información, por la inmensa mayoría de diferentes formas con las cuales se pueden romper la seguridad de un sistema.
- ◆ Sin embargo realizando una buena planeación de estrategias de seguridad se podrían evitar importantes pérdidas y lograr la salvación de una organización o la obtención de grandes ganancias directas.





Información es conocimiento y como tal debemos atribuirle la importancia que merece.

- ◆ Esta importancia incluye estudiar y lograr la forma de protegerla.

Esto plantea una paradoja:

- ◆ Si sumamos seguridad, bajan las posibilidades de acceder a la información, lo que es igual al Aislamiento y la Marginación.
- ◆ Si sumamos información, lo hacemos de forma insegura, lo que nos hace Globalmente Vulnerables.

BIBLIOGRAFIA

- Firma Digital - Master en Dirección de Empresas - Universidad del Salvador (Argentina) – Universidad de Deusto (España) – 2002.

www.hfernandezdelpech.com.ar

- Criptografía y Seguridad en Computadores, 3^o Edición – 2002 - Manuel J. Lucena López
mlucena@ujaen.es

- Tesis de Seguridad Informática sus Implicancias e Implementación – UTN - Borghello, Cristian – 2001. www.Segu-info.com.ar

