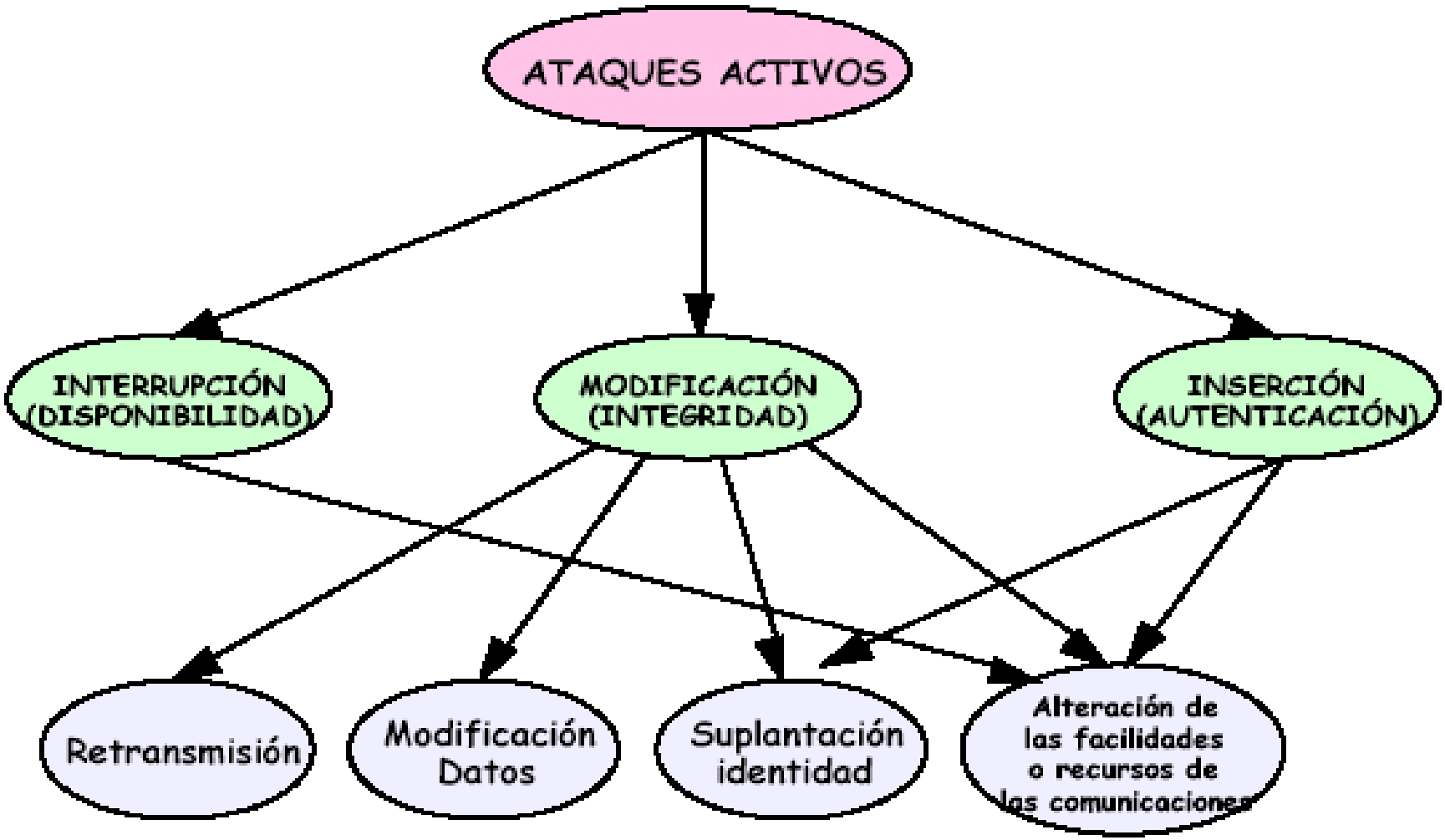
CRIPTOGRAFIA

El uso creciente de las redes de computadoras y la importancia del trafico cursado hace necesario proteger a los datos.

La criptografía es el uso de la transformación de datos para hacerlos incomprensibles a todos, excepto a los usuarios a quienes están destinados.

El problema de la intimidad trata de cómo evitar la obtención no autorizada de información de un canal de comunicaciones.

LO QUE SE TRATA DE EVITAR



Criptografía...

La encriptación es un mecanismo de seguridad

La criptografía es especialmente útil en los sistemas multiusuario, distribuidos y en las redes de computadoras.

Se debe utilizar para proteger a las contraseñas, almacenándolas cifradas.

Se puede utilizar para proteger todos los datos almacenados en un sistema de computación; se debe considerar el tiempo de cifrado / descifrado.

También es aplicable en los protocolos de redes de capas, que ofrecen varios niveles de cifrado.

Criptografía...

En el cifrado de enlace de redes se asume la responsabilidad de cifrado / descifrado de cada nodo:

- **Los datos se transmiten cifrados entre los nodos.**
- **En cada nodo se descifran, se determina a dónde transmitirlos y se los vuelve a cifrar.**

Existen ciertas limitaciones tales como la legibilidad de la dirección de destino en cada nodo:

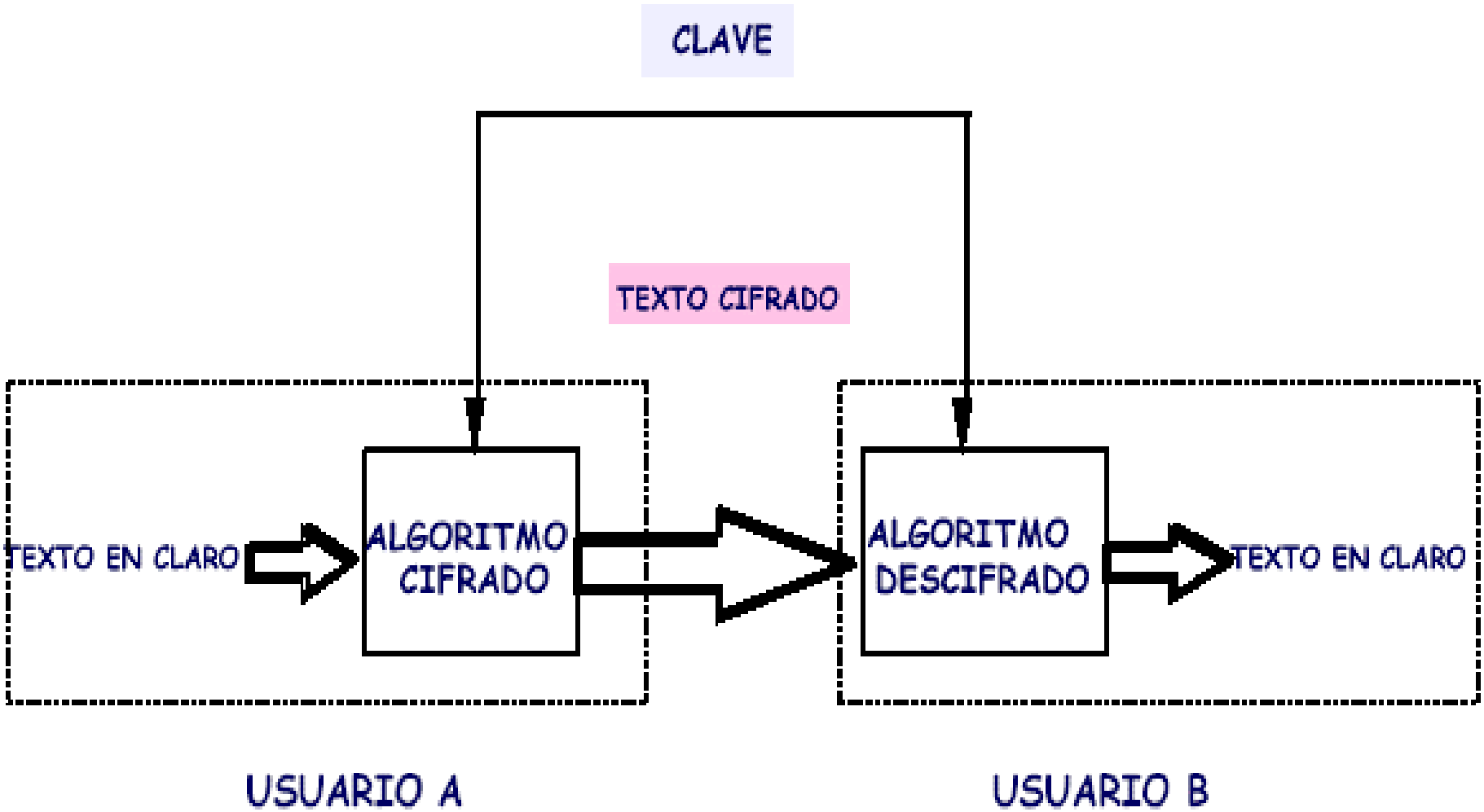
- **Debe ser legible para el encaminamiento del mensaje.**
- **Ej.: sistemas de conmutación de paquetes de almacenamiento y reenvío con cifrado; en este caso la dirección de destino asociada a un paquete no puede ser cifrada.**

CIFRADO SIMÉTRICO Y ASIMÉTRICO

Cifrado simétrico

Método criptográfico que usa una misma clave para cifrar y para descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar.
Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra
con la misma.

Cifrado simétrico



ALGORITMOS DE CIFRADO SIMETRICO

DES (Data Encryption Standard)

- **Adoptado en 1977 por el NIST (National Institute of Standars and Technology)**
- **Los datos a cifrar se procesan en bloques de 64 bits**
- **La longitud de la clave es de 56 bits**

Triple DES

- **Tres ejecuciones del algoritmo DES**
- **Longitud de clave efectiva de 168 bits**

IDEA (International Data Encyption Algorithm)

- **Desarrollado por Xuejia Lai y J. Massey (Swiss Federal**
- **Institute of Technology)**
- **Los datos a cifrar se procesan en bloques de 64 bits**
- **La longitud de la clave es de 128**

DES (Data Encryption Standard)

Se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones.

Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado .

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

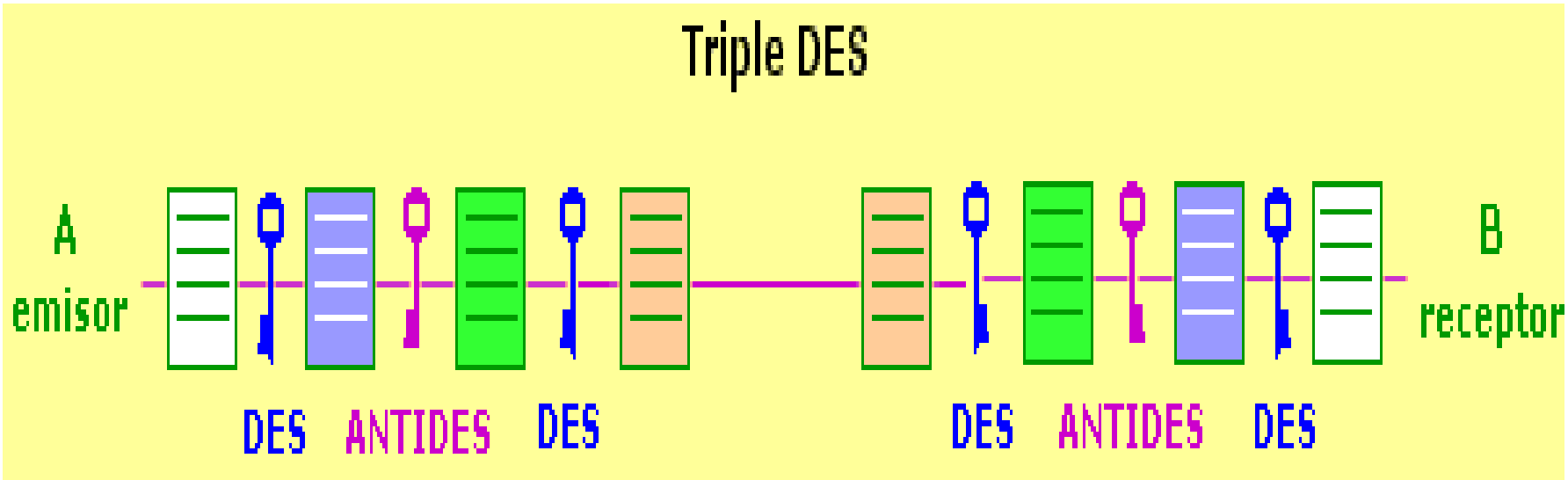
Como la clave efectiva es de 56 bits, son posible un total de 2 elevado a 56 = 72.057.594.037.927.936 claves posibles, es decir, unos 72.000 billones de claves, por lo que la ruptura del sistema por fuerza bruta o diccionario es súmamente improbable, aunque no imposible si se dispone de suerte y una grán potencia de cálculo.

Triple DES

el sistema DES se considera en la actualidad poco práctico, debido a la corta longitud de su clave. Para solventar este problema y continuar utilizando DES se creó el sistema Triple DES (TDES), basado en tres iteraciones sucesivas del algoritmo DES, con lo que se consigue una longitud de clave de 128 bits, y que es compatible con DES simple.

Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se encripta el mismo bloque dos veces con dos llaves diferentes se aumenta el tamaño efectivo de la llave.

Para implementarlo, se toma una clave de 128 bits y se divide en 2 diferentes de 64 bits, aplicándose el siguiente proceso al documento en claro:



- **Se le aplica al documento a cifrar un primer cifrado mediante la primera clave, C1.**
- **Al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2.**
- **Y al resultado se le vuelve a aplicar un tercer cifrado con la primera clave, C1.**

IDEA (International Data Encyption Algorithm)

- Sistema criptográfico simétrico, creado en 1990 por Lai y Massey, que trabaja con bloques de texto de 64 bits, operando siempre con números de 16 bits usando operaciones como OR-Exclusiva y suma y multiplicación de enteros.

- El algoritmo de desencriptación es muy parecido al de encriptación, por lo que resulta muy fácil y rápido de programar, y hasta ahora no ha sido roto nunca, aportando su longitud de clave una seguridad fuerte ante los ataques por fuerza bruta (prueba y ensayo o diccionarios).

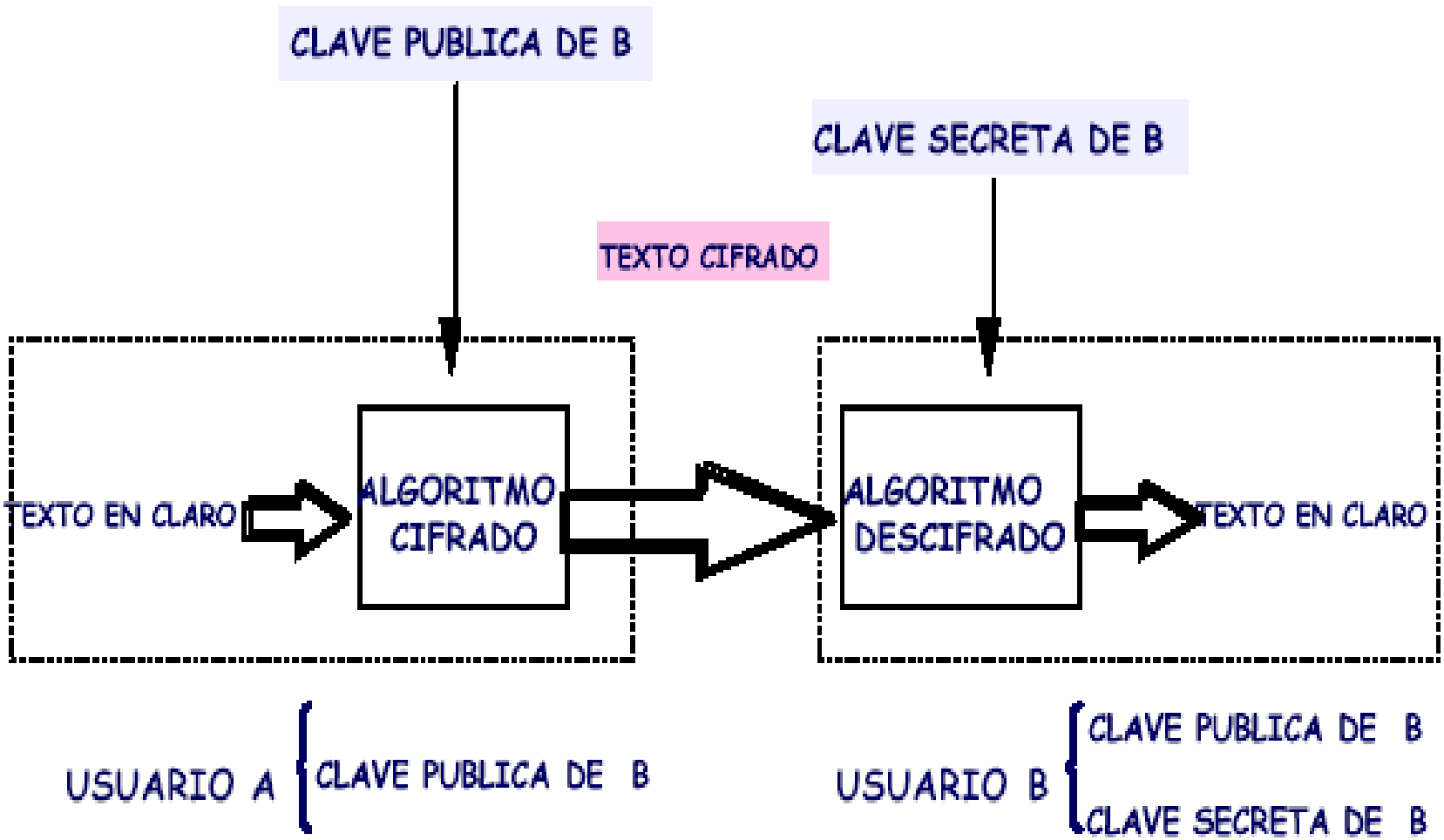
CIFRADO ASIMETRICO O DE CLAVE PUBLICA

La distribución de claves de un sistema criptográfico debe hacerse por canales muy seguros.

Los sistemas de clave pública rodean el problema de distribución de claves:

- **Las funciones de cifrado y descifrado están separadas y utilizan distintas claves.**
- **No es computacionalmente posible (en un tiempo "razonable") determinar la clave de desciframiento "D" a partir de la clave de ciframiento "C".**
- **"C" puede hacerse pública sin comprometer la seguridad de "D", que permanece privada.**

CIFRADO ASIMETRICO



ALGORITMOS DE CIFRADO ASIMETRICO
(CERTIFICADO DE CLAVE PUBLICA)

Diffie-Hellman

- **Primer sistema de Criptografía de clave pública. 1975**

RSA

- **Desarrollado por Rivest-Shamir-Adelman en el MIT en 1978**
- **Es el algoritmo más utilizado en criptografía asimétrica**

¿PORQUE SON NECESARIOS LOS CERTIFICADOS DE CLAVE PUBLICA?

A:->B: “Hola”

B:->A:”Hola, Yo soy B”, <Certificado de B>

A:->B: “Pruébala”

B:->A:”Soy B”, cifrar(KPrB, H[“Soy B”]);

Un intruso no podría crear una firma digital cifrando con la clave privada de B

¿QUÉ ES UN CERTIFICADO?

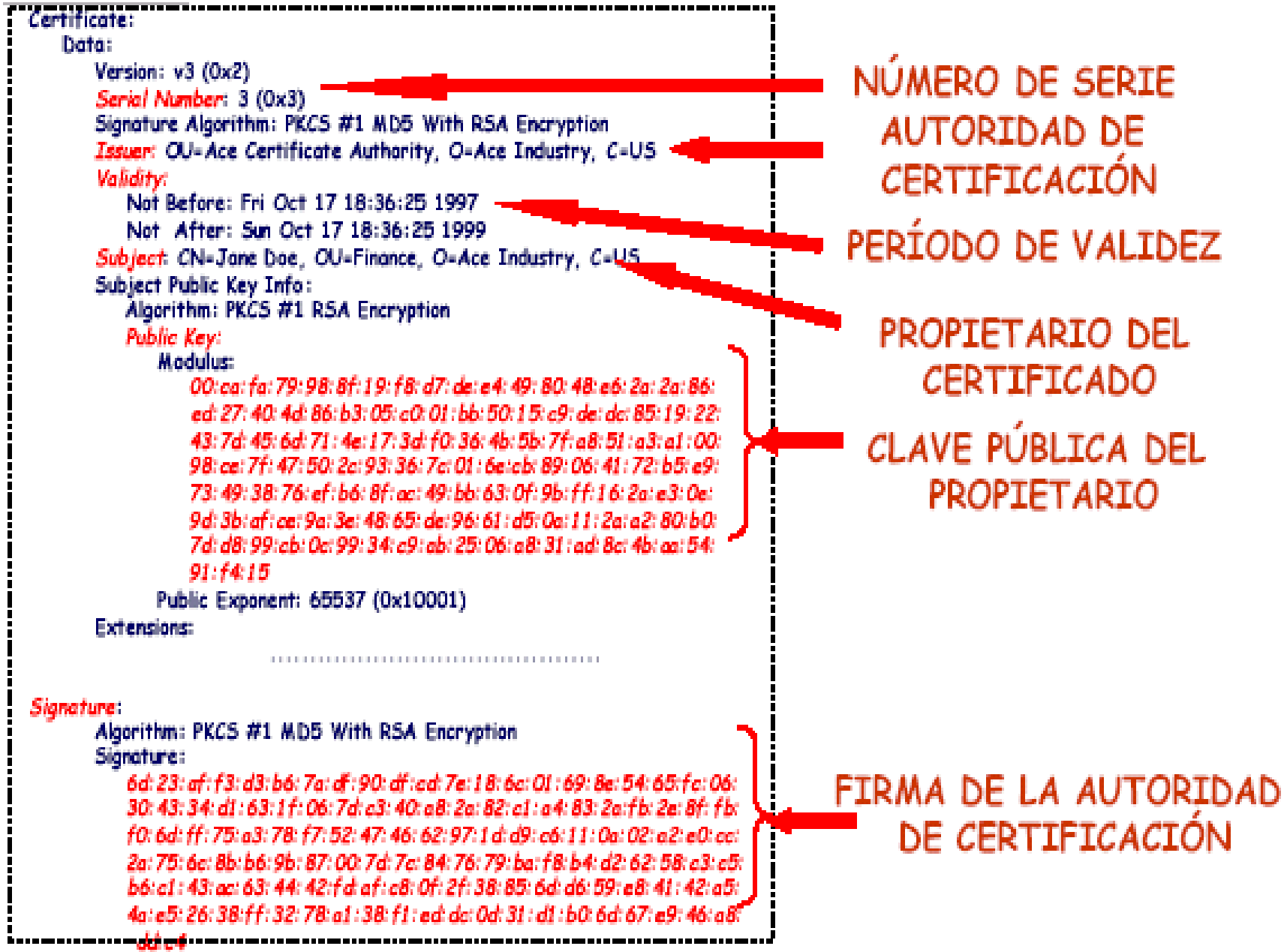
Un certificado digital (ó certificado de clave pública) establece la identidad de un usuario en un red.

- **Es equivalente a una tarjeta de crédito o a un carnet de conducir**
- **La estructura de un certificado está definida en el estándar ITU X.509**

En una red:

- **Los servidores pueden ser configurados para permitir el acceso a usuarios con ciertos certificados**
- **los clientes pueden ser configurados para confiar en servidores que presentan ciertos certificados.**

CERTIFICADO



NÚMERO DE SERIE

AUTORIDAD DE CERTIFICACIÓN

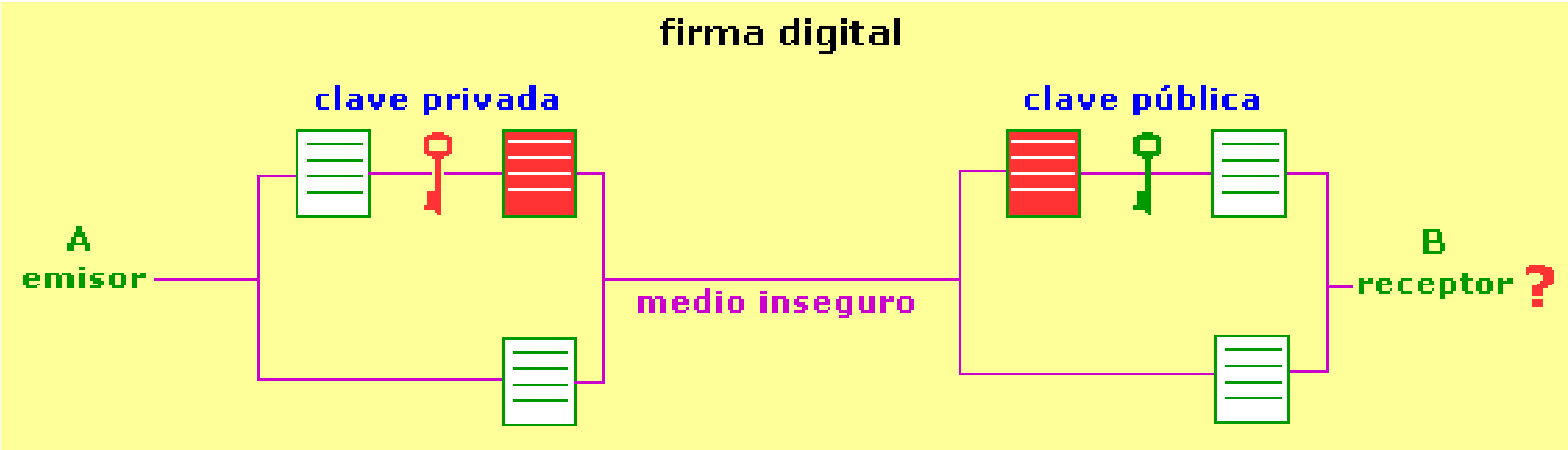
PERÍODO DE VALIDEZ

PROPIETARIO DEL CERTIFICADO

CLAVE PÚBLICA DEL PROPIETARIO

FIRMA DE LA AUTORIDAD DE CERTIFICACIÓN

FIRMAS DIGITALES



- **Proceso de Firma:** en el que el emisor encripta el documento con su llave privada, enviando al destinatario tanto el documento en claro como el encriptado.

- **Proceso de Verificacion de la Firma:** el receptor desencripta el documento cifrado con la clave pública de A y comprueba que coincide con el documento original, lo que atestígua de forma total que el emisor del mismo ha sido efectivamente A.

- A un mensaje resumido mediante una función hash y encriptado con una llave privada es lo que en la vida real se denomina firma digital.

AUTENTIFICACION

- **Los usuarios deben determinar si el hardware o el software con quien mantienen comunicación o les pide un servicio son los que dicen ser.**
- **La autentificación impide a un intruso reemplazar un programa sin conocimiento del usuario.**
- **No permite que un usuario inadvertidamente introduzca una contraseña en un programa de entrada falso, para realizar alguna operación en el servidor o en algún otro cliente que forme parte de la red distribuida.**
- **Para la autentificación se usa la función *HASH y los códigos de autentificación***

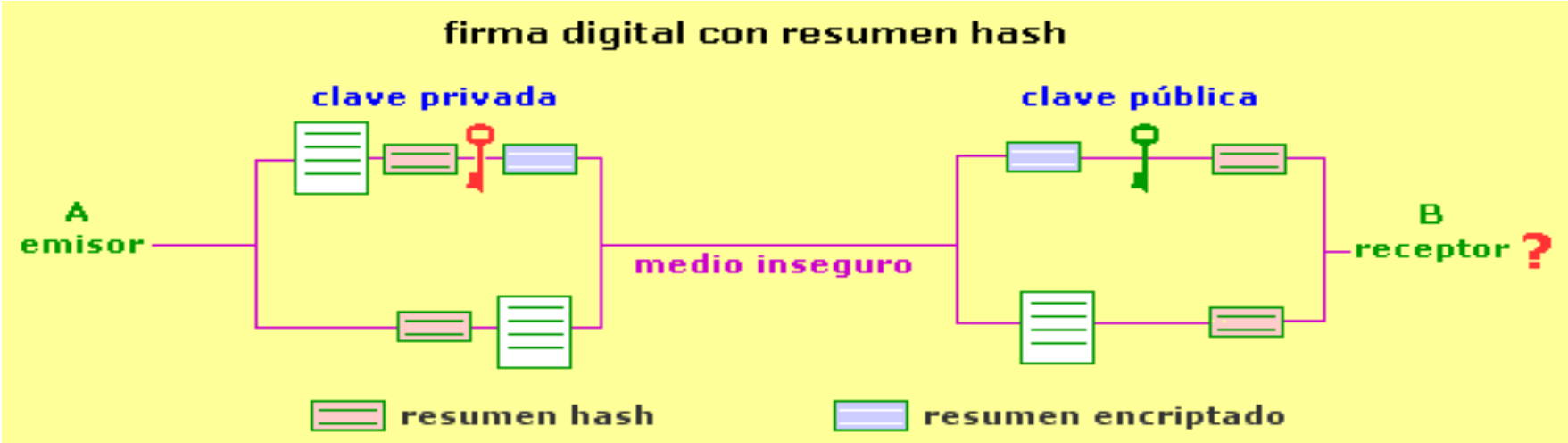
FUNCION HASH

Son unas funciones matemáticas que realizan un resumen del documento a firmar. Su forma de operar es comprimir el documento en un único bloque de longitud fija, bloque cuyo contenido es ilegible y no tiene ningún sentido real.

Tanto es así que por definición las funciones hash son irreversibles, es decir, que a partir de un bloque comprimido no se puede obtener el bloque sin comprimir, y si no es así no es una función hash.

Estas funciones son además de dominio público.

FUNCION HASH



su mecanismo es el siguiente:

- **El emisor aplica una función hash conocida al documento, con lo que obtiene un resumen hash del mismo.**
- **Encripta dicho resumen con su clave privada.**
- **Envía al receptor el documento original plano y el resumen hash encriptado.**
- **El receptor B aplica la función hash al resumen sin encriptar y desencripta el resumen encriptado con la llave pública de A.**
- **Si ambos coinciden está seguro de que ha sido A el que le ha enviado el documento. Si no coinciden, está seguro de que no ha sido A o de que el envío ha sido interceptado durante el medio de envío y modificado.**

AUTENTICACION DE MENSAJES

El mensaje lleva adicionalmente un Código de Autenticación de Mensajes (MAC)

Las entidades pares comparten una clave secreta

A:->B: "Hola"

B:->A:" Yo soy B", <certificado de B>

A:->B: "Pruébalo"

B:->A:" Soy B", cifrar(KPrB, H["Soy B"]);

A:->B: "ok,Aquí esta la clave", cifrar(KPuB,<clave sesión>);

B:->A:cifrar(clave sesión, <algunos mensajes, MAC>);

MAC:=H[mensaje, clave secreta]

IDENTIFICACION DE LA IDENTIDAD DE UN SERVIDOR POR UN CLIENTE

IDENTIFICACION DE LA IDENTIDAD DE UN CLIENTE POR UN SERVIDOR