CRIPTOGRAFIA

Introducción (I)

- Inicialmente la seguridad no fue un problema tenido en cuenta en las redes de ordenadores.
- Sin embargo, en la actualidad las redes transportan información sensible como:
  - Operaciones bancarias.
  - Compras (tarjetas de crédito).
  - Etc.
- Es necesario por tanto resolver la seguridad de las redes.

Qué es la seguridad

⌘ Toda cualidad de un sistema que nos indica el grado en el que dicho sistema está libre de peligro, daño o riesgo, siendo en cierta forma infalible

⌘ Hablamos de grados de fiabilidad

⌘ Aspectos básicos que afectan a la fiabilidad del sistema

⌘ La confidencialidad mide el grado en el que un sistema permite acceder a sus activos exclusivamente a los elementos autorizados, impidiendo su acceso a los demás elementos.

⌘ La integridad mide el grado en el que un sistema permite la modificación de alguno de sus activos por los elementos autorizados y de forma controlada.

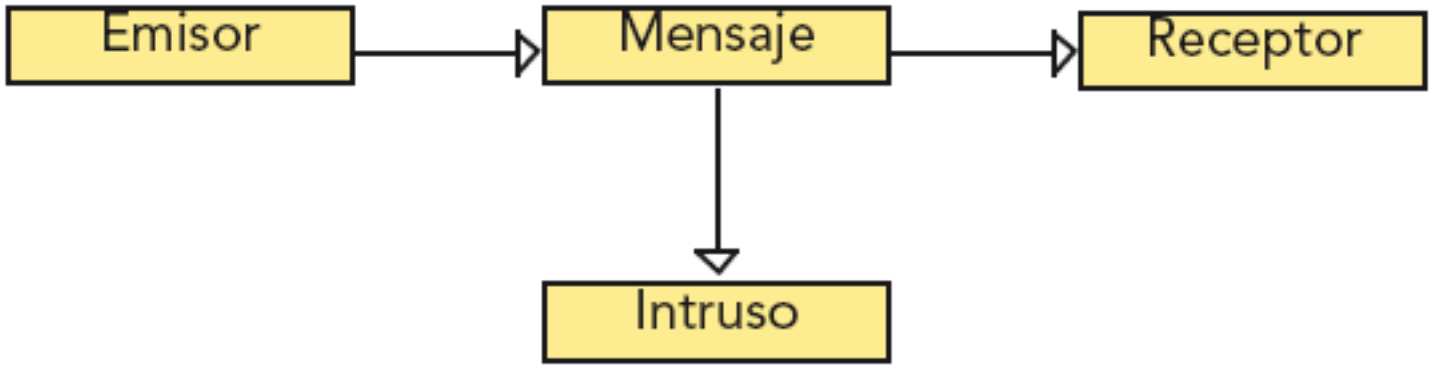
⌘ La disponibilidad indica el grado en el que un sistema ha de mantener a sus activos accesibles a los elementos autorizados.

Conceptos.

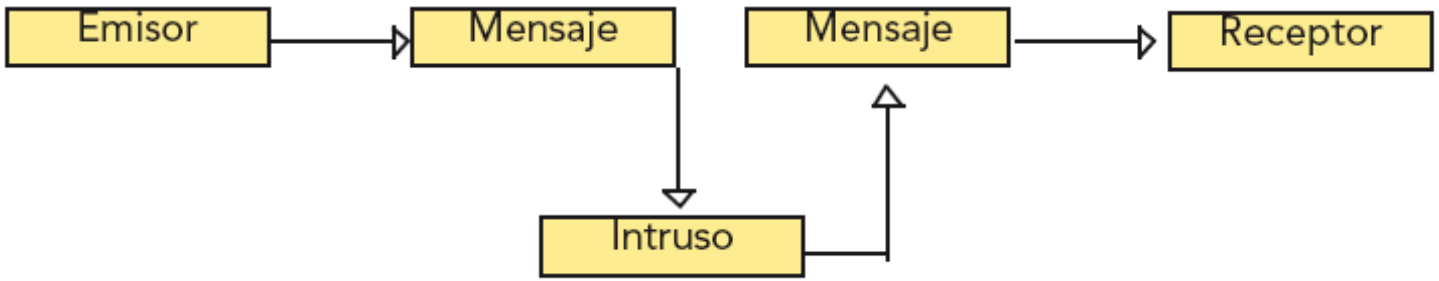
- CONFIDENCIALIDAD
  - +
  - INTEGRIDAD
  - +
- DISPONIBILIDAD

SISTEMA SEGURO

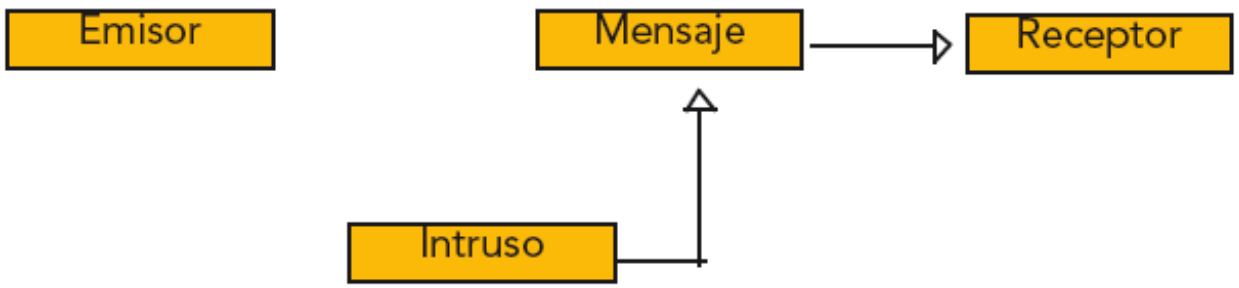
Problemas



Falsificación



Generación



Introducción (I)

- La criptografía es una herramienta muy útil cuando se desea tener seguridad informática; puede ser también entendida como un medio para garantizar las propiedades de confidencialidad, integridad y disponibilidad de los recursos de un sistema.

Para que exista seguridad ya sea de la información o informática hay que garantizar las propiedades de confidencialidad, integridad y disponibilidad..

Introducción (I)

•Para capturar paquetes podemos utilizar un analizador de protocolos: Wireshark es un analizador de protocolos que permite obtener parámetros de rendimiento de la red, comprobar configuraciones y analizar el tráfico de paquetes que por ella circula.

Introducción (II)

- Existen cuatro áreas de seguridad interrelacionadas:
  - El secreto.
    - Mantener la información fuera del alcance de los no autorizados.
  - La validación de identificación.
    - Asegurar la identidad del otro lado del canal de comunicación.
  - El control de integridad.
    - Asegurar que los mensajes recibidos no han sido manipulados por el camino.
  - El no repudio.
    - Firmar un mensaje de igual forma que se firma un documento.

Introducción (II)

- También es posible relacionar los nuevos problemas introducidos por las redes informáticas con cada uno de los principales aspectos de la seguridad informática.

- Privacidad de la información
- Integridad y autenticidad
- Disponibilidad
- Control de acceso y confidencialidad
- No repudiación

Secreto (I)

- El secreto en la red y en las comunicaciones esta ligado al cifrado (codificación) de los mensajes.
- En el cifrado:
  - Los mensajes a cifrar se conocen como texto normal
  - Se transforman mediante una función parametrizada por una clave.
  - El texto que se obtiene se conoce como texto cifrado.
  - La transmisión se realiza mediante el texto cifrado.
  - Si un intruso captura el texto cifrado no puede descifrarlo al no conocer el algoritmo y/o la clave.
- La persona que descifra mensajes sin conocer la clave se llama criptoanalista y a la técnica se la llama criptoanálisis.

Criptografía clásica

- Se basa en:
  - Algoritmos sencillos.
  - Claves muy largas.
- Sus técnicas son:
  - Cifrado por sustitución.
  - Cifrado por trasposición.

Cifrado por sustitución (I)

- Se basa en:
  - Sustituir cada letra o grupo de letras por otra letra o grupo de letras.
- Uno de los más antiguos conocidos. Cifrado de Cesar.
  - Cambiar la a por la D, la b por la E, etc.
  - La palabra ataque se convierte en *DWDTXH* .
- Una generalización mínima es cambiar la letra por la situada k posiciones, con lo que k es la clave de cifrado.

Cifrado por sustitución (I)

- 

Todo criptosistema debe satisfacer los siguientes requisitos para ser utilizado en la práctica:

1. Las transformaciones de cifrado y descifrado deben ser computacionalmente eficientes
2. Principio de Kerckhoff

Cifrado por sustitución (II)

- Generalización del cifrado por sustitución:
  - Establecer una correspondencia biunívoca entre las letras del alfabeto y cualquier permutación de las mismas.
- Ejemplo:

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
Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

- Este sistema se llama sustitución monoalfabética.
- La clave es la cadena de 26 letras por la que se sustituyen las letras del alfabeto.

Cifrado por sustitución (II)

- Cifrado del Cesar

Alfabeto	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
Alfabeto	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

Mensaje original: MENSAJE DE PRUEBA

Mensaje cifrado: OHPVDM GH SUXHED

Cifrado por sustitución (II)

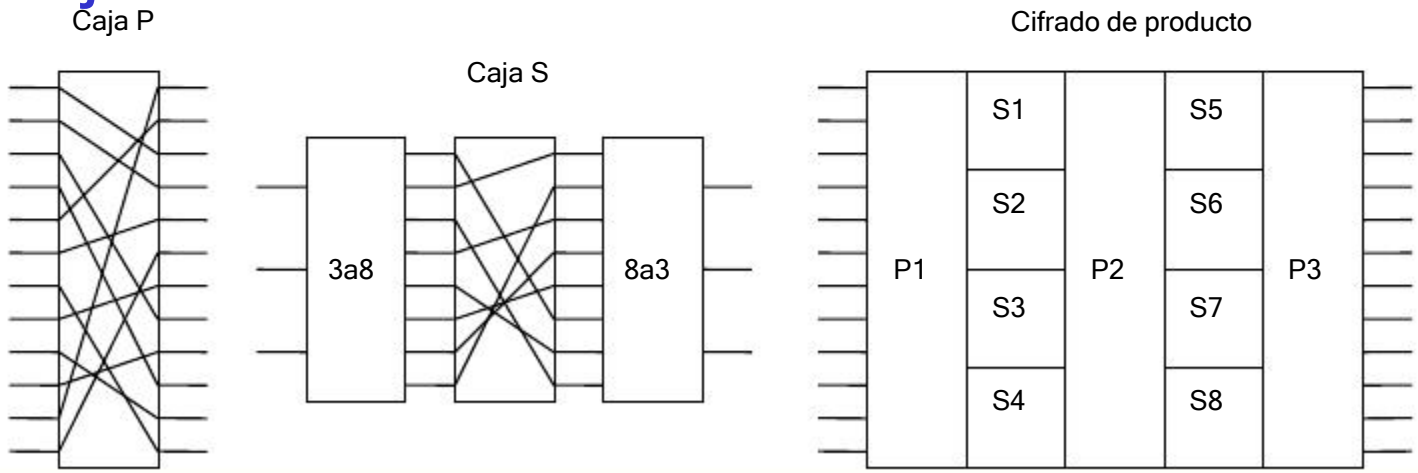
- Cifrado Vigenère

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
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	A
C	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
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
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	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	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

Mensaje: P A R I S V A U T B I E N U N E M E S S E
Clave: L O U P L O U P L O U P L O U P L O U P L
Criptograma: A O L X D J U J E P C T Y I H T X S M H P

Criptografía moderna (I)

- Se basa en:
  - Algoritmos complicados.
  - Claves cortas.
- Utiliza dos dispositivos de bloques básicos:
  - Cajas P.
  - Cajas S.



Criptografía moderna (II)

- Se divide en:
  - Clave privada:
    - La clave de cifrado y descifrado es la misma (o se deriva una de otra).
    - Debe mantenerse en secreto.
  - Clave pública.
    - La clave de cifrado y descifrado son distintas.
    - Puede hacerse pública la clave de cifrado mientras se mantenga en secreto la clave de descifrado.

Criptografía Simétrica

- Cifra y descifra con la misma clave

Criptografía Simétrica por bloques

- Cifra y descifra con la misma clave

Algoritmo	Bloque (bits)	Llave (bits)	Vueltas
Lucifer	128	128	16
DES	64	56	16
Loki	64	64	16
CAST	64	64	8
Blowfish	64	Variable	16

Cifrado DES (I)

- Fue desarrollado a principios de los 70.
- Se basa en el algoritmo Lucifer de IBM de 112 bits de clave.
- Utiliza una clave de 56 bits.
- Se desarrollo para poder ser implementado en un circuito electrónico de los años 70.
- El texto normal se cifra en bloques de 64 bits, utilizando los 56 bits de clave dando un texto cifrado de 64 bits.

Cifrado DES triple (II)

- Solución: Cifrar 3 veces con DES.

- Se utilizan dos claves de 56 bits.
- Se utiliza EDE en lugar de EEE porque:
  - Da igual utilizar la función en cifrado o descifrado, la seguridad es la misma.
  - Permite utilizar dos claves K_1 y K_2 , y haciendo $K_1 = K_2$ tenemos el algoritmo DES.

Cifrado IDEA (I)

- Utiliza una clave de 128 bits.
  - La clave genera 52 subclaves de 16 bits.
    - 6 para cada una de las 8 iteraciones.
    - 4 para la transformación final.
- Cifra en bloques de 64 bits como DES.
- Utiliza aritmética de 16 bits sin signo.
  - Fácilmente implementable en computadores.

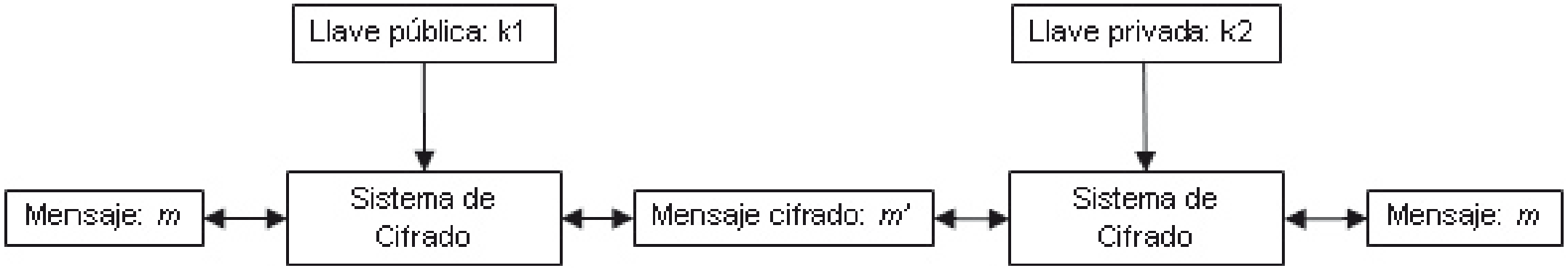
Cifrado AES (I)

- En 1997 se propuso el desarrollo de un nuevo algoritmo de cifrado: AES.
- AES es:
  - Público.
  - Utiliza criptografía de clave simétrica con bloques de 128 bits.
  - Permite claves de 128, 192 y 256 bits.
  - Puede ser implementado por software o hardware.

Cifrado AES (II)

- AES opera en matrices de datos de 4x4 realizando:
  - Una sustitución no lineal de cada byte de la matriz por otro byte de acuerdo a una tabla.
  - Una transposición donde las filas son rotadas.
  - Un mezclado de columnas con otras mediante una transformación lineal.
  - Una combinación del resultado con la clave.
- AES utiliza:
  - 10 rondas para claves de 128 bits.
  - 12 rondas para claves de 192 bits.
  - 14 rondas para claves de 256 bits.
  - Una ronda final donde el mezclado de columnas se sustituye por otra combinación del resultado con la clave.

Cifrado Asimétrico



Cifrado RSA (I)

- En 1976, investigadores de Stanford propusieron una clase nueva de criptosistema:
  - Las claves de cifrado y descifrado eran diferentes.
  - El algoritmo de cifrado, con clave E y el de descifrado, con clave D, debían cumplir:
    - D(E(P))=P
    - Es difícil deducir D de E.
    - E no puede descifrarse mediante prueba.

Cifrado RSA (II)

- El funcionamiento es el siguiente:
  - Tenemos dos algoritmos E y D que cumplen lo anterior.
  - A escoge una clave de cifrado E_A y de descifrado D_A .
  - B escoge otra clave de cifrado E_B y de descifrado D_B .
  - E, D, E_A y E_B son públicos.
- A quiere enviar un mensaje P a B:
  - Con E_B calcula E_B (P) y lo envía a B.
  - B lo recibe y calcula D_B (E_B (P)) y obtiene P.
  - Nadie más que B puede descifrar el mensaje.
- Un algoritmo que cumple la propiedad propuesta es el RSA.

Cifrado RSA (III)

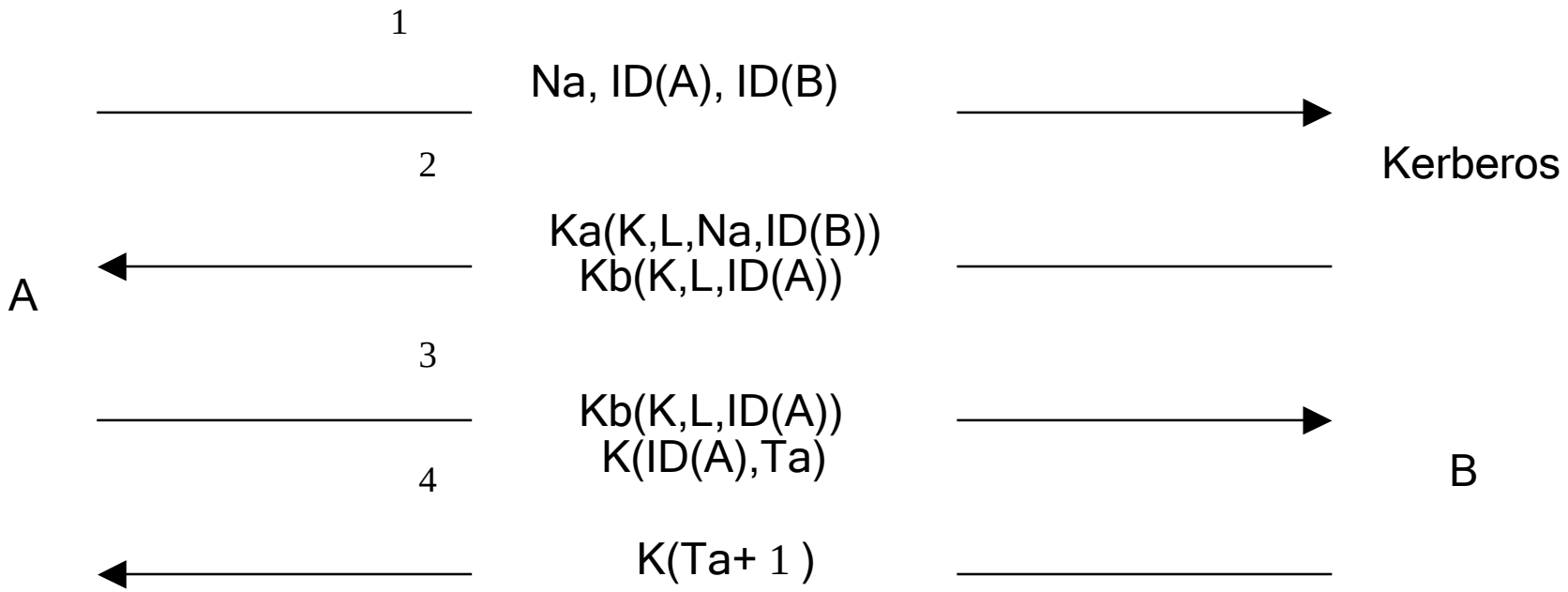
- El RSA se basa en:
  - Escoger dos números primos grandes p y q mayores de 10^{100} .
  - Calcular n=p*q y z=(p-1)*(q-1).
  - Seleccionar un primo d respecto a z (un número sin factores comunes con z).
  - Encontrar e tal que (e*d)%z = 1.
  - El texto se cifra en bloques de k bits de forma que $0<2^k<n$.
  - Para cifrar calculamos $C=P^e \%n$.
  - Para descifrar calculamos $P=C^d \%n$.

Cifrado RSA (IV)

- La parte pública de la clave es (e,n).
- La parte privada de la clave es (d,n).
- La dificultad consiste en factorizar números grandes como n.
  - Si se factoriza n se puede obtener z, y con z y e se obtiene d mediante el algoritmo de Euclides.
  - En la actualidad, suponiendo un tiempo de instrucción de 1 nanosegundo, se requieren 4 millones de años para factorizar un número de 200 dígitos.

Protocolo de autenticación Kerberos

- Todo usuario:
  - Se identifica ante Kerberos.
  - Acuerda una clave criptográfica K propia para él.



Compendio MD5

- Es la quinta función de una serie de funciones de dispersión diseñadas por Ron Rivest.
- El algoritmo es:
  - Se coge el mensaje original P y se rellena hasta que su tamaño sea 448 módulo 512.
  - Se añade la longitud del mensaje como un entero de 64 bits, con lo que la longitud final es múltiplo de 512 bits.
  - Se inicializa un buffer de 128 bits con un valor fijo.
  - Se toma el mensaje en bloques de 512 bits y se mezclan con el buffer actual de 128 bits junto con una tabla construida a partir de la función seno.
  - Cuando se acaban los bloques el valor del buffer es el MD5 del mensaje original, MD5(P).

Compendio SHA

- Fue desarrollado por la NSA.
- El algoritmo es:
  - Se coge el mensaje original P y se rellena hasta que su tamaño sea 448 módulo 512.
  - Se añade la longitud del mensaje como un entero de 64 bits, con lo que la longitud final es múltiplo de 512 bits.
  - Se inicializa un buffer de 160 bits con un valor fijo.
  - Se toma el mensaje en bloques de 512 bits y se mezclan con el buffer actual de 160 bits:
    - Utiliza 80 rondas para cada bloque de entrada.
    - Cada 20 rondas modifica las funciones de mezcla del bloque y del buffer.
  - Cuando se acaban los bloques el valor del buffer es el SHA del mensaje original, SHA(P).

Firma digital

- Una firma digital es un documento que permite garantizar la integridad de un documento y se puede relacionar de manera única al firmante con su firma, ya que realiza ésta con la llave privada y únicamente el firmante posee esa llave, esto se traduce en que se verifica la autenticidad del firmante.

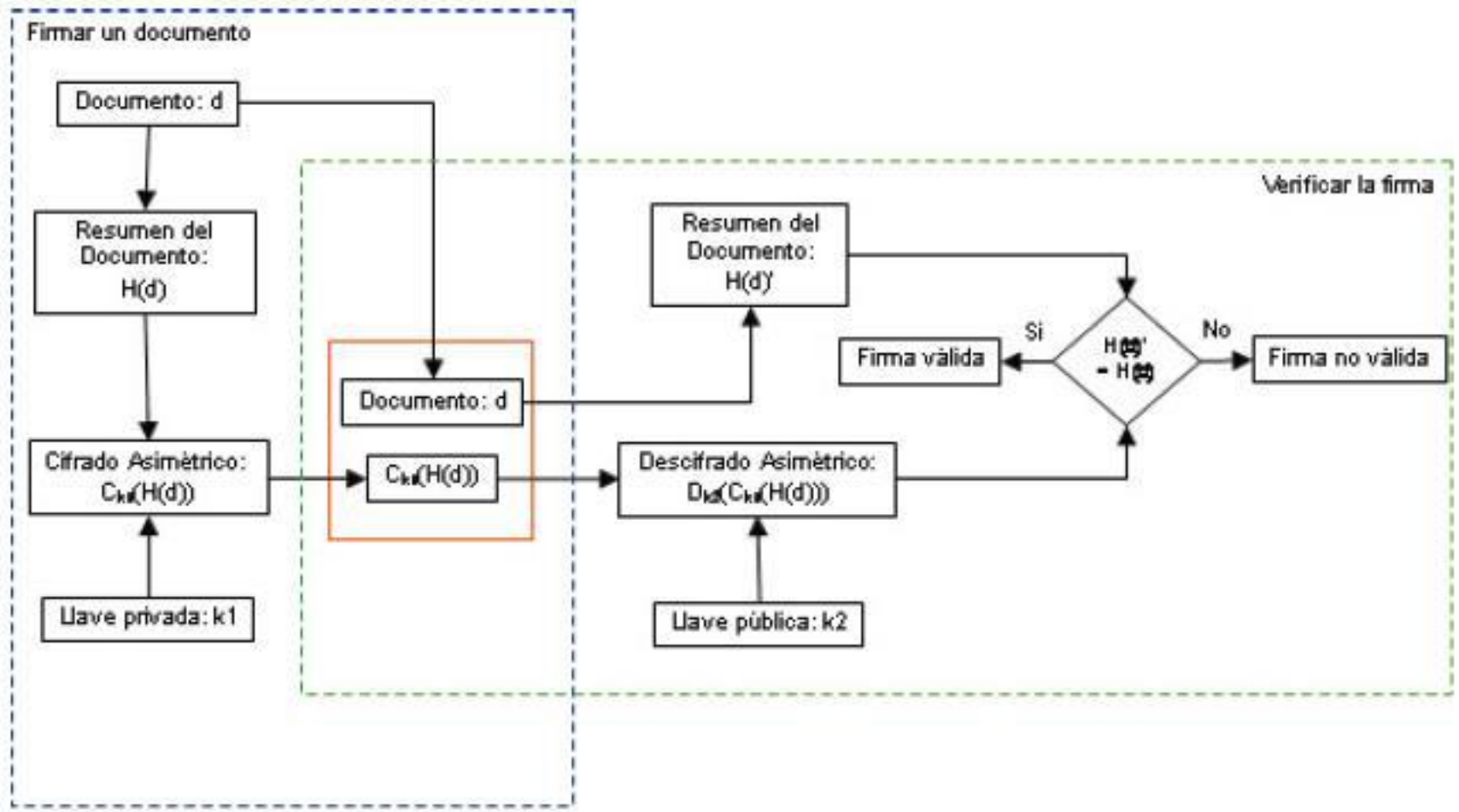
Firma digital

- Función HASH:

Esta función lo que hace es que a partir de
un documento de tamaño N bits entrega una cadena de M bits.
No hay límite para el tamaño de N, pero M siempre es de tamaño constante de acuerdo con el algoritmo usado, normalmente es de 128 o 256 bits.
Una de las características de este tipo de funciones es que son unidireccionales, es decir, que debe de ser imposible a partir del resumen del documento encontrar el mensaje original. También deben cumplir la propiedad de dispersión, lo que significa que si se cambia al menos un bit del documento, su resumen debe de cambiar la mitad de sus bits aproximadamente.

Firma digital

- Función HASH:

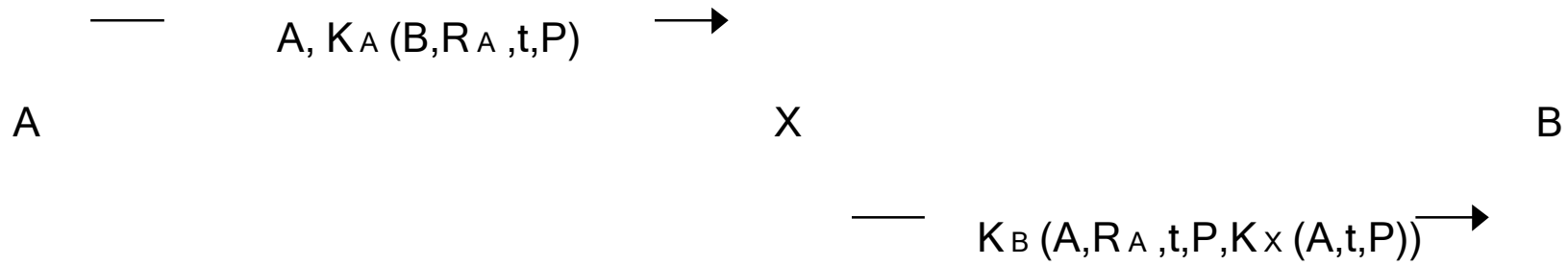


Firma digital

- Una firma digital debe cumplir:
  - El receptor pueda verificar la identidad del emisor.
    - Una computadora de un banco necesita saber que la otra computadora es quién dice ser.
  - El emisor no pueda repudiar el mensaje enviado.
    - Si se compra una tonelada de oro y cae el precio, el cliente puede decir que el no mando comprar la tonelada de oro.
  - El receptor no pueda confeccionar el mensaje.
    - Si se compra una tonelada de oro y sube el precio, el banco puede decir que el cliente solo pidió un kilo de oro.

Firma de clave secreta

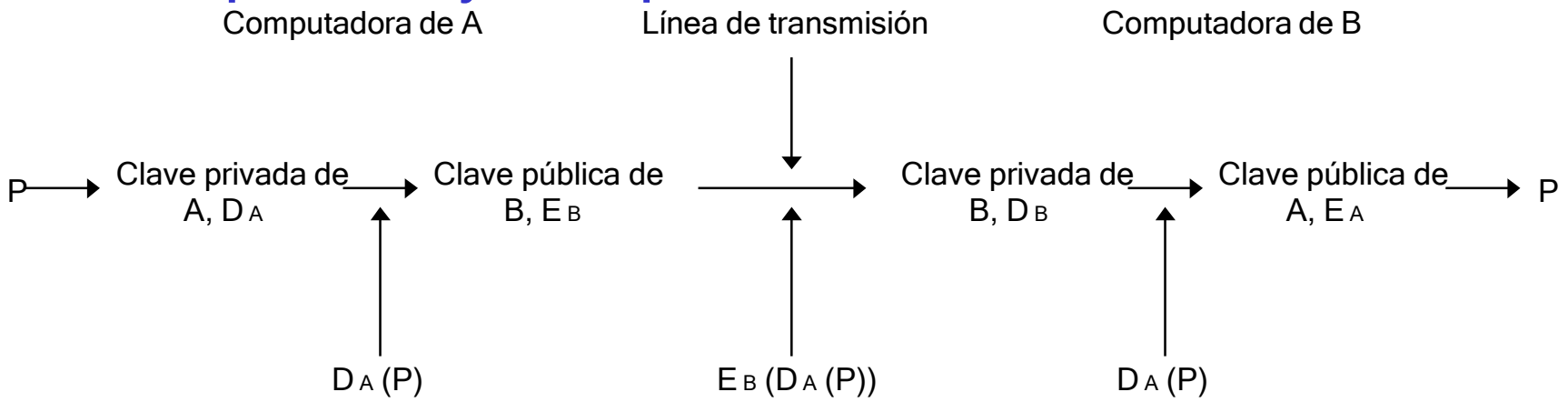
- Todo usuario:
  - Se identifica ante la autoridad X.
  - Acuerda una clave secreta K propia para él.



- El problema es que X debe leer todos los mensajes.

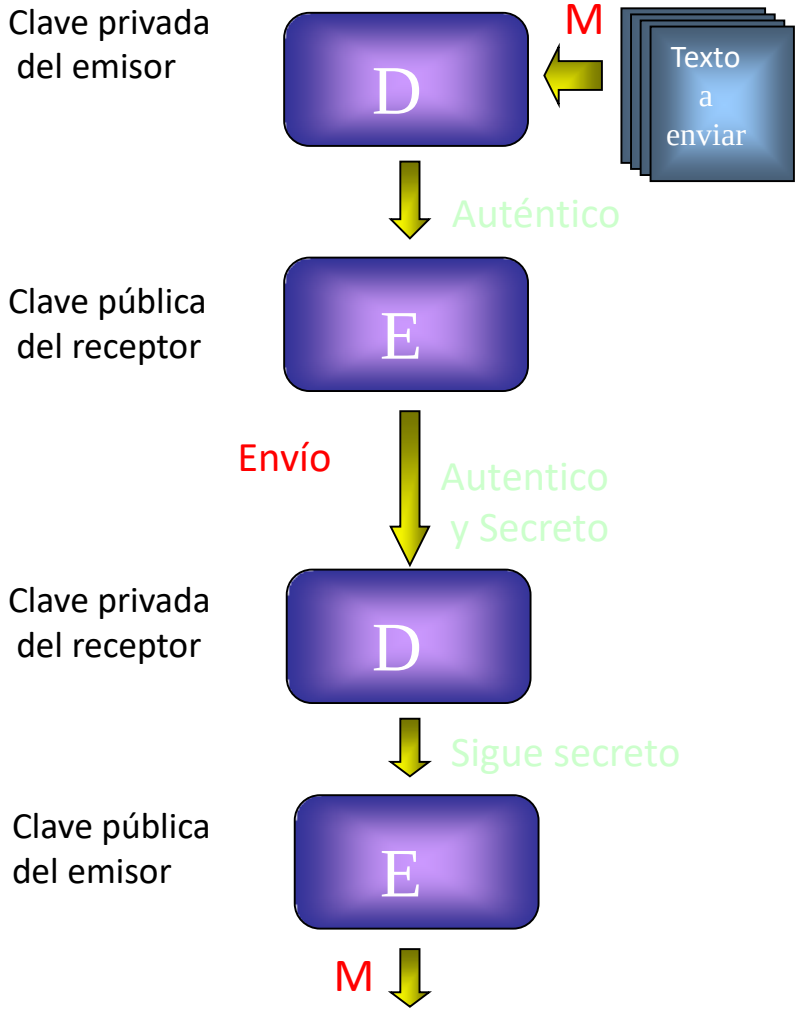
Firma de clave pública

- Un usuario utiliza, por ejemplo, RSA y genera una clave pública y una privada.



- Problemas:
  - A puede decir que le han robado su clave privada DA.
  - A puede cambiar las claves y entonces lo que ya ha firmado no es valido.
  - Se requiere una autoridad que controle estos casos .

Firma de clave pública



Para generar un HASH existen diferentes algoritmos de cifrado entre los cuales tenemos:

- **Algoritmos asimétricos**
- Son aquellos que no poseen un algoritmo reverso para descifrar su contenido original
- **MD5**
- Longitud fija: 32 caracteres

Caracteres: 0 al 9, A a la Z mayúsculas y minúsculas

- **SHA**
- Longitud fija: 40 caracteres

Caracteres: 0 al 9, A a la Z mayúsculas y minúsculas

- **Algoritmos simétricos**
- Son aquellos que una vez cifrados poseen un algoritmo inverso que puede descifrar su contenido, por ejemplo:
- **BASE64**
- Longitud: variable
  Caracteres: 0 al 9 A a la Z solo mayúsculas
  Finaliza comúnmente en un igual “=” o doble igual “==”
- **BASE32**
- Longitud: variable
  Caracteres: 2 al 7 A a la Z solo mayúsculas, no se toma en cuenta el 0 porque podría confundirse con la O mayúscula, el 1 podría confundirse con la letra I y el 8 podría confundirse con la letra B
  Finaliza comúnmente con varios símbolos de igual “====”
- **CAESAR**
- Este es uno de los primeros algoritmos que aprenden los estudiantes en clases de criptografía, y consiste en tener 2 alfabetos y un número constante que nos indica cuantas posiciones se debe mover el alfabeto como indica la siguiente figura:

Algoritmos

- Los caracteres iniciales del /etc/shadow identifican el algoritmo:

- 1 is Message Digest 5 (MD5)
- $2a$ is blowfish
- 5 is 256-bit Secure Hash Algorithm (SHA-256)
- 6 is 512-bit Secure Hash Algorithm (SHA-512)
- y (or 7) is yescrypt
- none of the above means DES

Certificado

- Un certificado es esencialmente una clave pública y un identificador, firmados digitalmente por una autoridad de certificación, y su utilidad es demostrar que una clave pública pertenece a un usuario concreto.

El formato de certificados X.509 es el más común y extendido en la actualidad, , y contempla los siguientes campos:

-Versión.
-Número de serie.
-Identificador del algoritmo empleado para la firma digital.
-Nombre del certificador.
- etc ...

Certificado

- Emitidos por CA de confianza
- Autocertificados