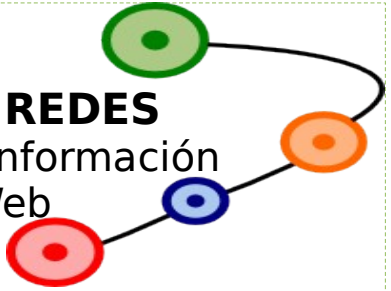
Administración y Gestión de Redes
Lic. en Sistemas de Información



Laboratorio de REDES
Recuperación de Información
y Estudios de la Web

Introducción a la Seguridad en Redes de Datos 2 - Criptografía

Equipo docente:

Fernando Lorge (florge@unlu.edu.ar)
Santiago Ricci (sricci@unlu.edu.ar)
Alejandro Iglesias (aaiglesias@unlu.edu.ar)
Mauro Meloni (maurom@unlu.edu.ar)
Patricio Torres (ptorres@unlu.edu.ar)

- 2026 -

Criptosistema

- **m: (Plaintext)** mensaje en claro o grupos de mensajes en claro que se desean cifrar.
- **c: (Ciphertext)** mensaje o grupos de mensajes cifrados
- **K: (Keys)** conjunto de claves que se emplean en el criptosistema
- **E: (Encryption Algorithm)** es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de m para obtener un elemento de c. Existe una transformación diferente, denominada E_k, para cada valor posible de la clave k.
- **D: (Decryption Algorithm)** es el conjunto de transformaciones de descifrado.

Todo criptosistema cumple $D_k(E_k(m)) = m$

Sistemas Criptográficos: Clasificación I

- Por **tipo de operaciones usadas para transformar** el texto plano en texto cifrado:
  - *Sustitución*: cada elemento del texto plano (bit, letra) se mapea a otro elemento.
  - *Transposición*: los elementos del texto plano son reacomodados.

Sistemas Criptográficos: Clasificación II

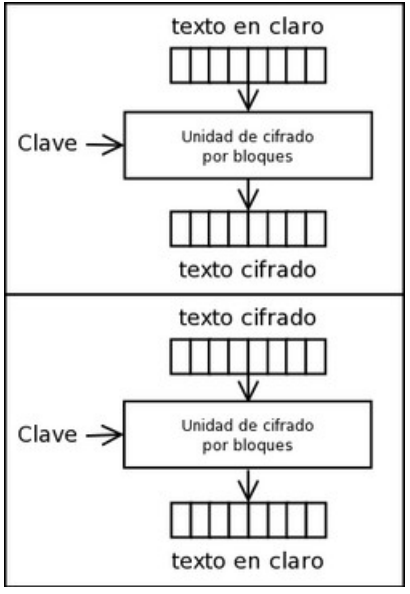
- Por el **número de claves utilizadas**:
  - *Simétricos*: emisor y receptor utilizan la misma clave. También se los suele denominar como de una clave, de clave secreta o cifrado convencional.
  - *Asimétricos*: Emisor y receptor utilizan claves diferentes. Denominados también de doble clave, o cifrado de clave pública.

Sistemas Criptográficos: Clasificación III

- Por la **forma en que el texto plano es procesado**.
  - *Cifrado por bloque*: procesa un bloque de elementos por vez, produciendo un bloque de salida por cada bloque de entrada.
  - *Cifrado continuo (stream)*:Procesa los elementos de manera continua, produciendo un elemento de salida por vez, a medida que se va alimentando.

Criptografía

Sistemas Criptográficos: Clasificación III



Cifrado por bloques

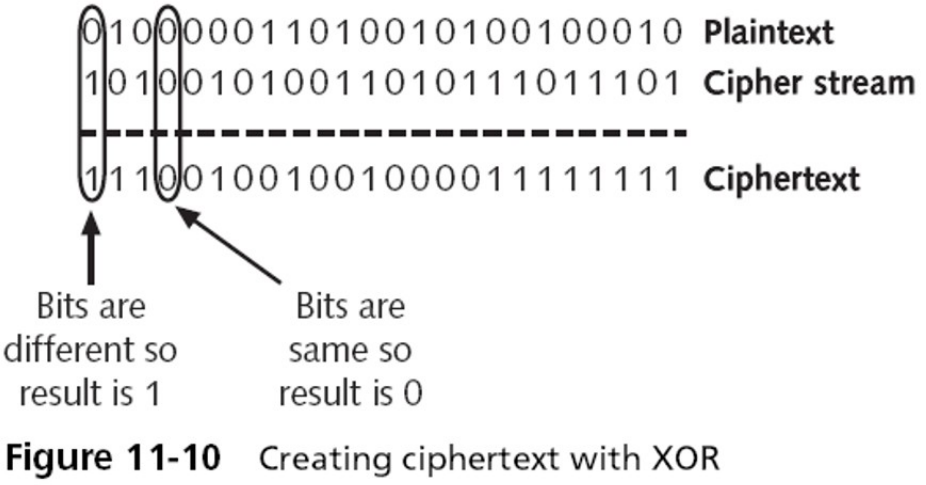


Figure 11-10 Creating ciphertext with XOR

Cifrado continuo

Cifrado por sustitución
Algoritmo de César

- Se realiza siempre la misma sustitución: 1ª letra por 4ª; 2ª letra por 5ª; 3ª letra por 6ª... Es decir, la A en el mensaje original pasaría a ser la D en el mensaje cifrado.
- La expresión matemática de este algoritmo es:

$$C = (m + 3) \bmod L$$

donde C es el mensaje cifrado, m es el menaje en claro, 3 sería la contraseña (que no es tal), L es el número de letras del alfabeto en cuestión. Esta expresión supone que cada letra esta asociada a un número (A=0, B=1, p. ej.).

Cifrado por sustitución
Algoritmo de César - Ejemplo

- Se desea cifrar el mensaje “SECRETO”
- Puede utilizarse una tabla para facilitar la conversión:

```
ABCDEFGHIJKLMNÑOPQRSTUVWXYZ
DEFGHIJKLMNÑOPQRSTUVWXYZABC
```

- El mensaje cifrado será “VHFUHWR”

- Es un algoritmo de cifrado **monoalfabético** porque a cada símbolo a cifrar le corresponde siempre el mismo símbolo cifrado.

Cifrado por sustitución
Cifrado de Vigenère

- Este es un ejemplo de cifrado polialfabético (la sustitución aplicable a cada carácter varía en función de la posición que ocupe en el mensaje en claro), en el que la clave es un secuencia de símbolos (una palabra; $K = \{k_0, k_1, \ldots , k_{d-1}\}$) y que se define en la siguiente expresión:

$$\mathbf{E_k\ (m_i) = m_i + k_{\ (i \bmod d)}\ (mod\ n)}$$

- donde m_i es el i-ésimo símbolo del texto a cifrar (mensaje en claro) y n es el número de letras del alfabeto.

Criptografía

Algoritmos de cifrado clásicos: Cifrado de Vigenère - Ejemplo

- Mensaje: “ESTO ES SECRETO”
- Clave: “CLAV EC LAVECLA”
- Cifrado: “GDTK IU DEXVGEO”

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

Cifrado por transposición

Otra técnica de cifrado consiste, en vez de sustituir símbolos, en realizar permutaciones, es decir, cambiar su lugar. (ubicación, orden)

- **Rail Fence:**
  - El texto se escribe en diagonal hacia abajo en “rieles” de una valla imaginaria hasta el último riel, luego se escribe en diagonal hacia arriba y así sucesivamente. Luego se toma el mensaje por filas.

```
t v o u g d l r u i n
  e e l e o e a e n o
```

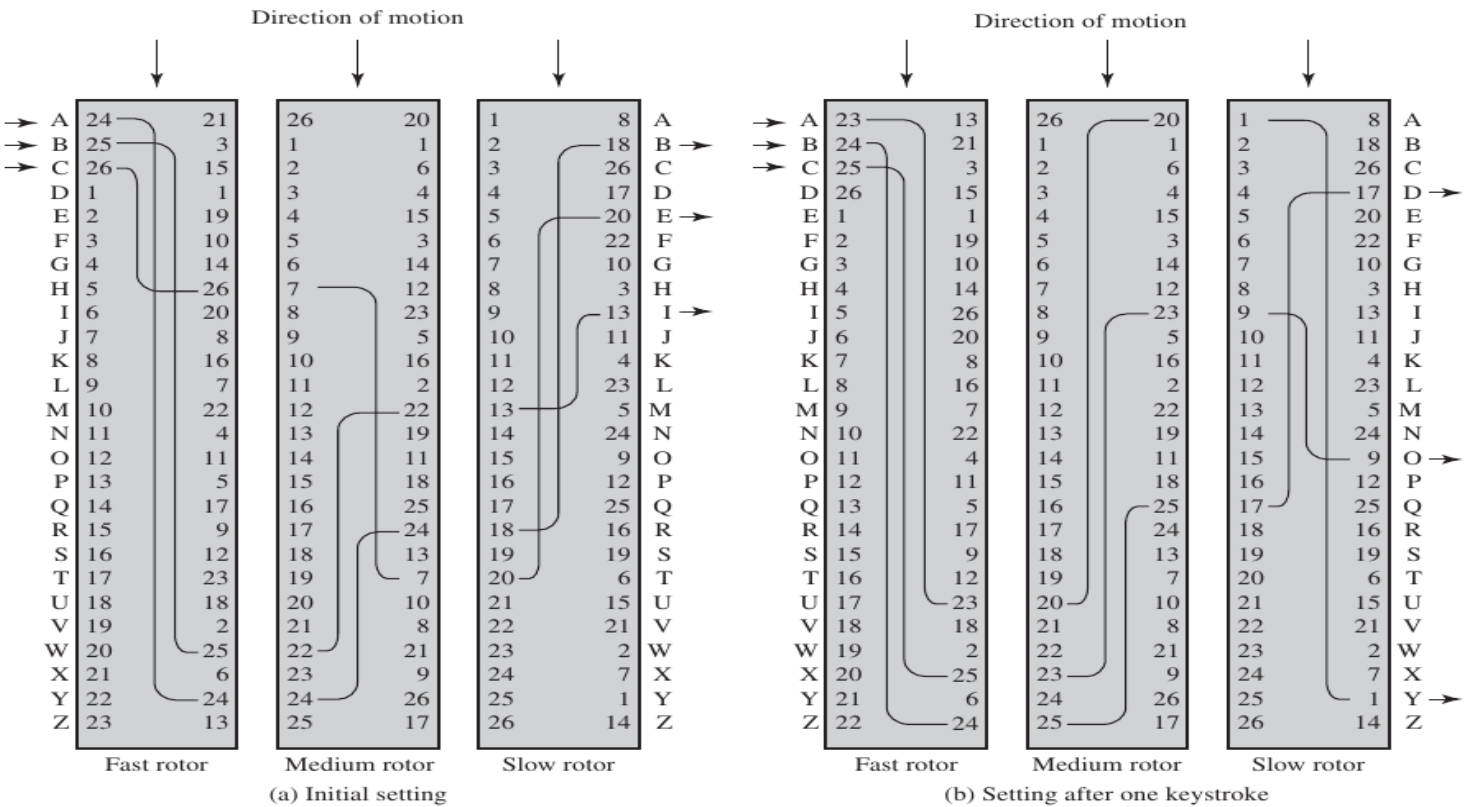
Mensaje → “te veo luego de la reunión”
← Rail Fence, Profundidad de 2
Texto cifrado → “tvougdlruineeleoeaeno”

- **Rotor Machine**
  - Compuesta por cilindros independientes con contactos eléctricos que implementan cada uno una sustitución monoalfabética.
  - Los cilindros giran a distinta velocidad, (como un odómetro*), logrando una sustitución polialfabética compleja.

*un “cuentakilómetros”

Criptografía

Rotor Machine



Enigma

Simulador: https://observablehq.com/@tmcw/enigma-machine

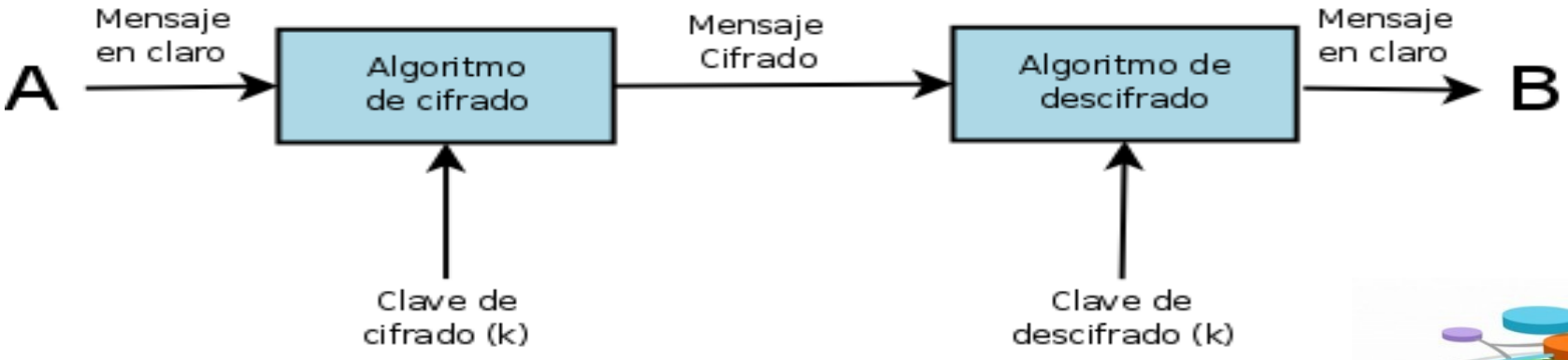
Criptografía simétrica (convencional, o de clave secreta)

- La criptografía simétrica se basa en la utilización de la misma clave para el cifrado y para el descifrado
- La robustez de un algoritmo de cifrado simétrico recae en el conocimiento de dicha clave.
- Ventajas: sencillez de implementación, rapidez y robustez.
- Desventajas: Administración de claves no escalable.

? ¿Qué servicio de seguridad puede garantizar?

Criptografía simétrica

- El emisor cifra el mensaje con la clave *k* y se lo envía al receptor. Este último, que conoce dicha clave, la utiliza para descifrar la información.



Criptografía simétrica – algoritmos:

Basados en Bloques	Basados en Stream
3DES (Triple-DES)	RC4
IDEA	Salsa20
Blowfish	ChaCha20
AES (Rijndael)	A5/1 - A5/2
CAST5	
Twofish	
Serpent	
Camellia	

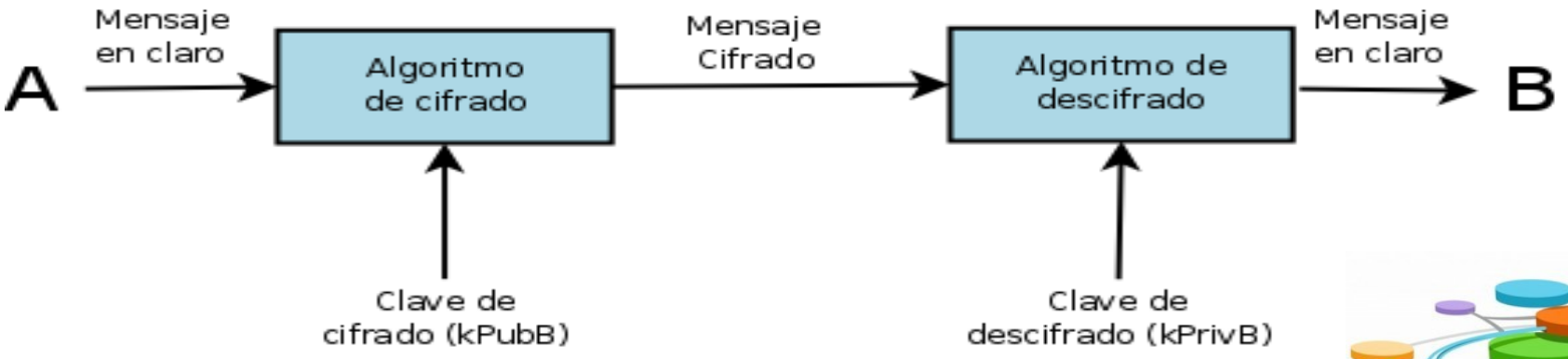
Criptografía asimétrica (clave pública)

- Se basa en la utilización de dos claves relacionadas, una para cifrar y otra para descifrar. (Denominadas clave pública y clave privada)
- La seguridad está basada en la dificultad de deducir una clave a partir del conocimiento de la otra. (la clave privada a partir de la clave pública)
- Ventajas: Mayor escalabilidad en la distribución de claves.
- Desventajas: Mayor tiempo de procesamiento. Necesidad de autenticar las claves públicas.

? ¿Qué servicio de seguridad puede garantizar?

Criptografía asimétrica

- El usuario A cifra un mensaje con la clave pública del usuario B (destinatario), éste para descifrarlo utiliza su clave secreta correspondiente, únicamente conocida por él.



Criptografía asimétrica

- Ejemplos de algoritmos de cifrado asimétrico son:
  - RSA (Rivest, Shamir y Adleman) 1977
  - DSA (Digital Signature Algorithm – Estandar FIPS) 1991
  - ECDSA (Elliptic Curve Digital Signature Algorithm)
  - ElGamal
  - Diffie-Hellman (intercambio de claves)
  - EdDSA (Edwards-curve Digital Signature Algorithm)
  - Ed25519

Funciones HASH

- Una función hash es una función computable que aplicada a un mensaje (m) de tamaño variable genera una representación de tamaño fijo del propio mensaje (H(m)).
- H(m) es mucho menor que m; por ejemplo, m puede tener una longitud de 1Mb, mientras que H(m) se puede reducir a 64 o 128 bits.
- Una función hash unidireccional es una función hash H de modo que para cualquier mensaje m es difícil encontrar un mensaje m' tal que H(m)=H(m'). Este tipo de función se denomina función resumen, y al valor H(m) se le suele llamar el resumen o digesto de m.

Funciones HASH

- Algunas de las funciones hash más utilizadas son:
  - MD5 (Message Digest, MD) que genera firmas (digestos o resúmenes) de 128 bits.
  - SHA-1 (Secure Hash Algorithm), genera firmas de 160 bits.
  - SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512).
  - RIPEMD-160, que genera firmas de 160 bits.
  - WHIRPOOL (firmas de 512 bits para mensajes menores a 2^256 bits)
  - SHA-3 (Keccak)

Autenticación de mensajes

- Procedimiento para verificar que el mensaje recibido ha sido generado por la supuesta fuente que lo envía, y que no ha sido modificado.

- Adicionalmente, puede verificarse la secuencia y tiempo oportuno. (Que no ha ocurrido alteración en el orden de los mensajes, retraso o retransmisión).

Código de Autenticación de Mensajes (MAC)

- Una función MAC es una función que aplicada a un mensaje (m) de tamaño variable y una clave (k) genera una representación de tamaño fijo del propio mensaje MAC=C_k(m).
- En resumen, es un mecanismo que provee autenticación e integridad a un mensaje.
- La clave secreta es compartida por emisor y receptor.
- Basado en cifrado simétrico por bloques. (Ej Data Authentication Algorithm)
- Basado en funciones hash (HMAC) o de cifrado (CMAC).
  - HMAC (RFC 2104):

```
MAC = H ( k xor opad || H ( k xor ipad || m ))
```

Donde H es una función Hash (MD5, SHA1, SHA256, SHA384, etc.)

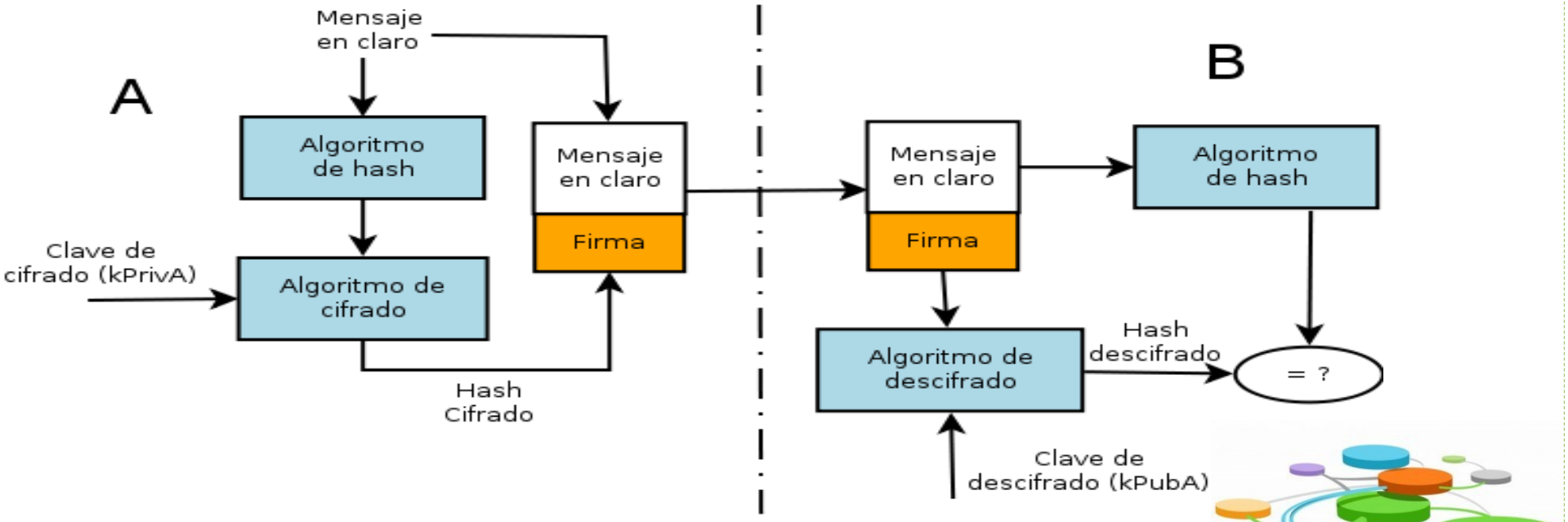
Firma digital

- Mecanismo de autenticación que permite al creador de un mensaje anexar un código que actúa como una firma, garantizando origen e integridad.

- Proceso de firmado:

  - El usuario A genera una huella digital H(m) del mensaje m y cifra dicha huella con su clave privada (kPrivA).
  - A continuación A envía al usuario B el mensaje sin cifrar (m) y su correspondiente resumen (H(m)) cifrado.
  - El usuario B obtiene la huella digital calculada por A utilizando la clave pública de A (kPubA) sobre el H(m) cifrado y a continuación genera la huella digital del mensaje enviado por el usuario A (H(m)').
  - B realiza una comparación de las dos huellas obtenidas. Si no coinciden (H(m) y H(m)') es que el mensaje o la huella enviada por A han sido modificados y por tanto la firma no es correcta.

Firma digital



Esteganografía

- Estudia los procedimientos encaminados a ocultar la existencia de un mensaje en lugar de ocultar su contenido.
- El objetivo de la esteganografía es ocultar el mensaje dentro de otro sin información importante, de forma que el atacante ni siquiera se entere de la existencia de dicha información oculta.
- No se trata de sustituir al cifrado convencional sino de complementarlo: ocultar un mensaje reduce las posibilidades de que sea descubierto; no obstante, si lo es, el que ese mensaje haya sido cifrado introduce un nivel adicional de seguridad.

Esteganografía - Ejemplos:

- Tinta invisible.
- Marcas de cualquier tipo sobre ciertos caracteres (desde pequeños pinchazos de alfiler hasta trazos a lápiz que marcan un mensaje oculto en un texto).
- Secuencia predefinida dentro de un texto.
- Afeitar la cabeza de un mensajero y tatuar en el cuero cabelludo el mensaje, dejando después que el crecimiento del pelo lo oculte.
- En imágenes digitales: sustituir el bit menos significativo de cada byte por los bits del mensaje que se desea ocultar.
- En archivos de audio, video, etc

Bibliografía

Cryptography and Network Security - Principles and Practice, Fifth Edition, William Stallings, Prentice Hall. 2011

http://www.argentina.gob.ar/jefatura/innovacion-publica/innovacion-administrativa/firma-digital