HOJA

FECHA

Criptografía

Objetivos: - Confidencialidad
- Autenticidad
- Integridad de los datos
- No repudio

Confidencialidad: Es un servicio utilizado para mantener el contenido de la información para todos aquellos que estén autorizados.

Autenticidad: Comprobar de manera segura alguna característica sobre un objeto, como por ej su identidad, su origen.

Integridad de los datos: Cuando los datos no han sido alterados de una manera no autorizada desde su creación, transmisión o guardado por una fuente autorizada.

No repudio: Se trata de que una vez enviado un mensaje el emisor no pueda negar haber sido el autor del mismo.

⊙ **Criptosistema:** Es una quintupla (M, C, K, E, D)

M - se refiere a todos los mensajes sin encriptar

C - se refiere a todos los mensajes cifrados ó encriptados

K - Conj de todas las claves posibles

E - Transformacion que se le puede aplicar a todos los elementos de M y obtener C

D - Inversa de E

Luego: $\boxed{D_k(E_k(m)) = m}$

NOTA

Los Criptosistemas pueden ser: → Simétricos o clave privada: Clave K_{pr}

→ Asimétrico o clave publica: (K_{pu}, K_{pr})

⊙ Criptoanálisis: Consiste en comprometer la seguridad de un criptosistema ya sea decifrando un mensaje sin conocer la clave utilizada ó bien obteniendo la clave empleada para cifrar el mensaje.

- Brute force: Se tiene un criptograma y se prueba decifrarlo con todas las claves posibles K.

- Textos planos: Se eligen varios textos planos y se obtienen sus criptogramas. Deberá conocer el método de encriptación.

- Análisis de frecuencia: Se basa en estudiar las frecuencias en la que aparecen los simbolos en varios textos y luego se busca su ítem en los criptogramas.

⊙ Cifrado: reemplazar simbolos o grupos de simbolos por otros simbolos sin tener en cuenta la naturaleza linguistica de la fuente.

Criptografía Clasica: • Cifrado por sustitución: Se agarra ch x ch y reemplaza x bit por bit.

• Cifrado por transposición

- Cifrado por Sustitución → Monoalfabetico o sustitución simple

→ Homofónicos (un char en la fuente no va a ser reemplazado siempre por el mismo char))

→ Polialfabético.

NOTA

HOJA

FECHA

Cifrado de Vigemere (Siglo XVII)

$A = \{ \ldots \}$ q símbolos

clave $K = (k_1 k_2 \ldots k_j)$

$m = (m_1, m_2, \ldots, m_t)$

$\Phi_i = (m_i + k_i) \bmod q \quad 1 \le i \le t$

$\Phi_i^{-1} = (\Phi_i - k_i) \bmod q$

$E_k(m) = (\Phi_1, \Phi_2, \ldots, \Phi_t) = c$ (mensaje cifrado ó criptograma)

$D_k(c) = (\Phi_1^{-1}, \Phi_2^{-1}, \ldots, \Phi_t^{-1}) = m$

Vemos un ejemplo:

Sea $A = \{a, b, c, d, \ldots\}$ $q = 26$

Clave = "datos" $j = 5 \rightarrow K = (3, 0, 19, 14, 18)$

mensaje = "demostracion"

Luego:

m	3	4	12	14	18	19	17	0	2	8	14	13
K	3	0	19	14	18	3	0	19	14	18	3	0
c	6	4	5	2	10	22	17	17	16	26	17	13

$\rightarrow c = gefickwrfqm$

Desencriptado

c	6	4	5	
k	3	0	19	
m	3	4	12	4

$\rightarrow m =$ "DEM"...

D E M

Homofónico

$A = \{a, b\} \rightarrow H(a) = \{00, 10\}$

$H(b) = \{01, 11\}$

$m =$ "ab" $\rightarrow$ C_1: 0001 cifrado 1

C_2: 1001 cifrado 2

etc

NOTA

- Cifrado por Transposición de columnas

Clave = segunda (no se pueden repetir chars en la clave)

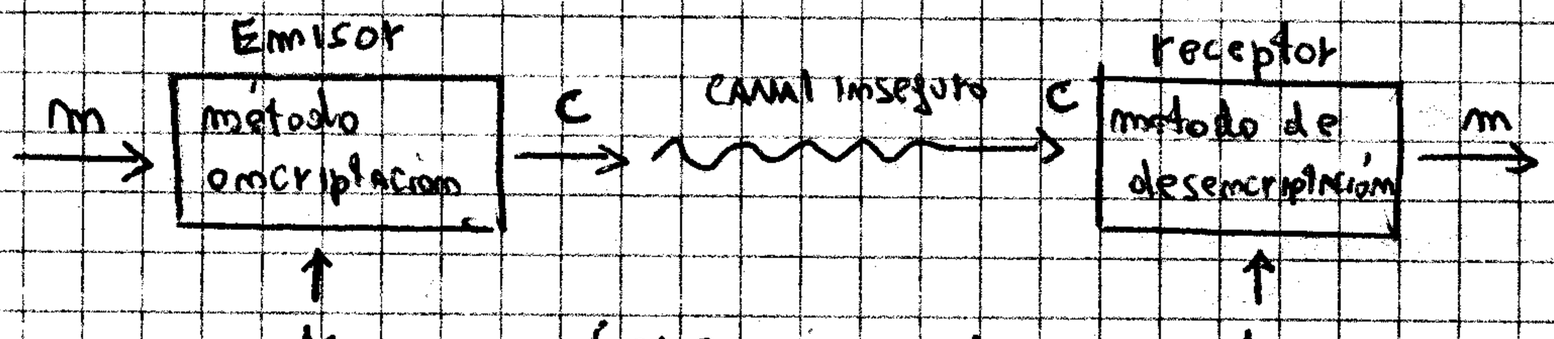
mensaje = establecen las siguientes características importantes

634752 1 → ordenamiento de las cols según orden de aparición, no posición de las cifras de la clave en el Alfabeto.

Segunda
establece
las
siguientes
características
importantes

C: estoiosLsmAtpesegseAt.....

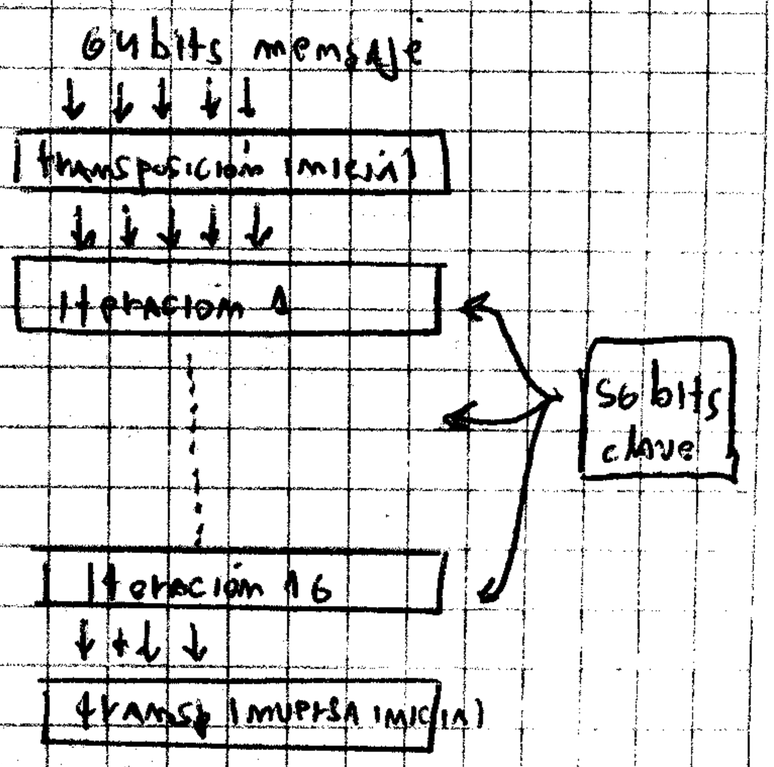
② Criptografía Simetrica (se usa solo Clave Privada)



(el Emisor no le envía la clave privada K por el canal, sino de otra forma como el DES)

DES

- 56 bits → longitud de la clave
- 64 bits → bloques de 64 bits del mensaje
- 19 etapas



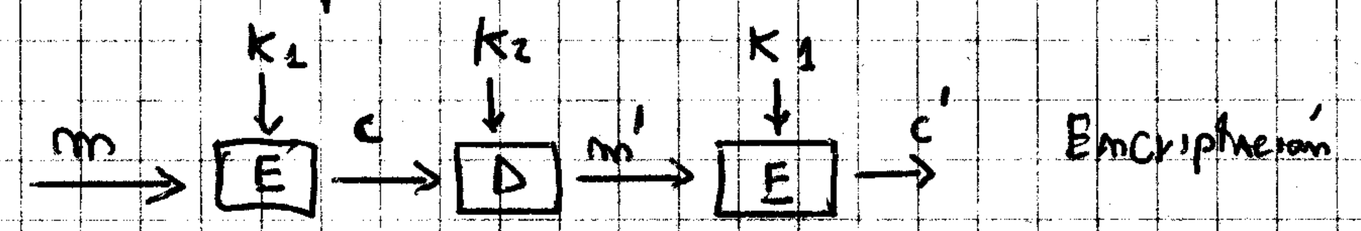
NOTA

HOJA

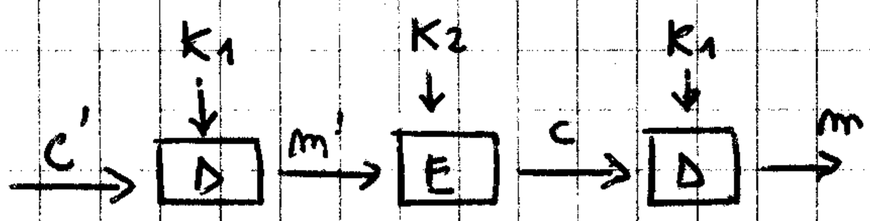
FECHA

TDES

(k_1, k_2) → claves privadas



Encriptación

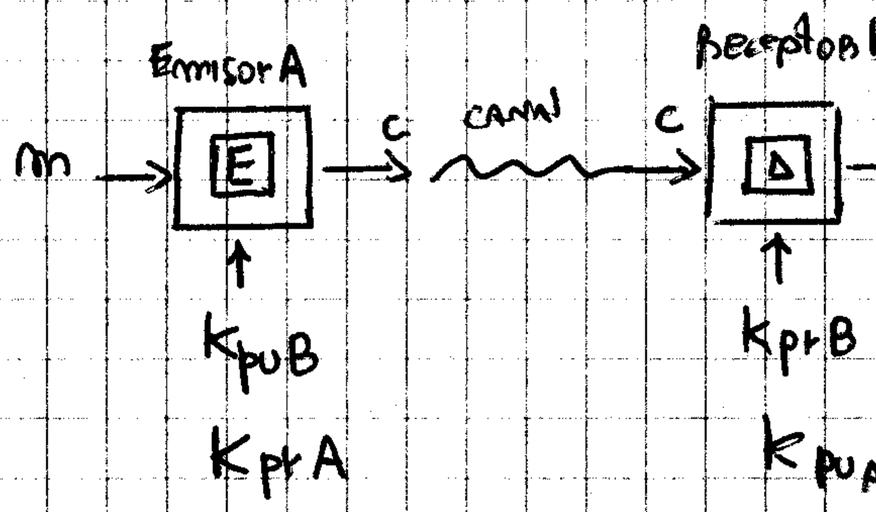


Desencriptación

② Criptografía Asimetrica

clave pública K_{pu}

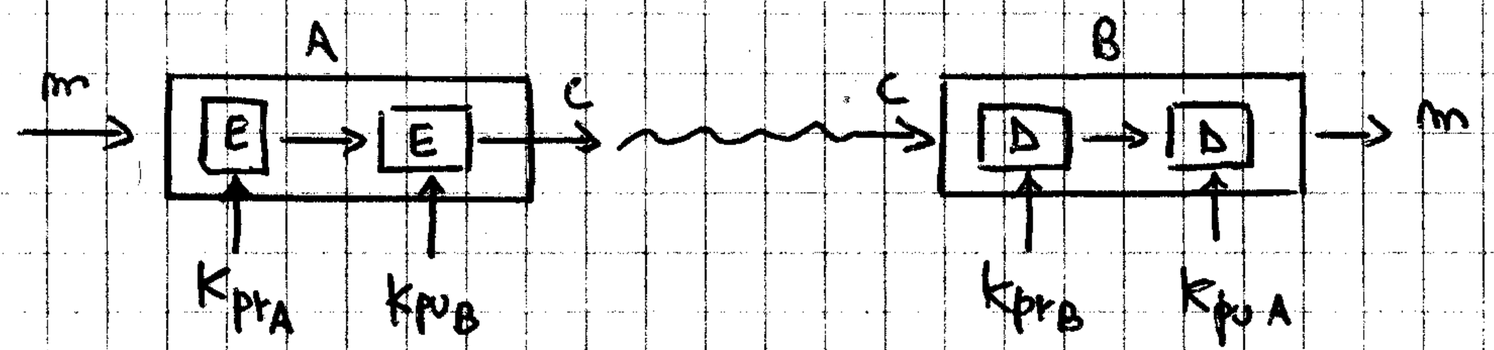
clave privada K_{pr}



(Así solo B puede descifrarlo)

(Así solo A pudo haberlo mandado)

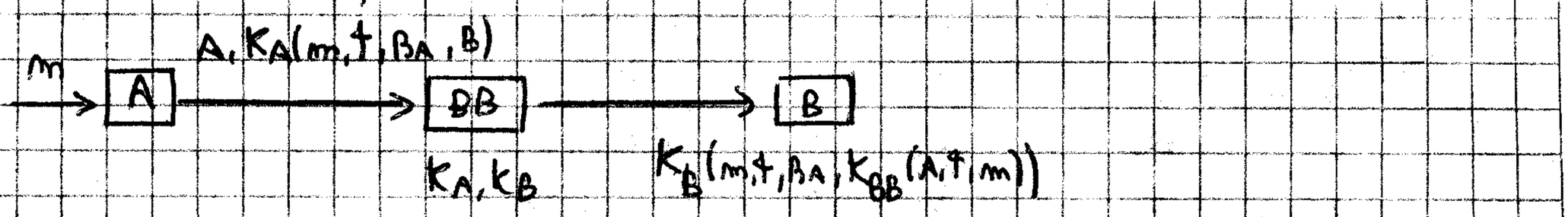
- Para garantizar tanto el emisor (Autenticidad) como el receptor (Confidencialidad), hago:



NOTA

Firma digital (simetrica)

BB - Big Brother : A y B deben transportar personalmente su clave privada a BB.



NOTA