Compresión y Criptografía de Datos

Coordinación de Ciencias Computacionales
May – Jul 2003

Dra. Claudia Feregrino

Contenido

1. Introducción
2. Tipos de criptosistemas
   1. Criptosistemas simétricos
   2. Criptosistemas asimétricos
3. Sistema de cifrado
4. Secreto de un sistema criptográfico
5. Criptosistemas clásicos
6. Criptosistemas modernos

Las dos últimas décadas

- 80s - uso de PC comienza a ser común.
  - Preocupación por integridad de los datos.
- 90s proliferan los ataques a sistemas informáticos
  - aparecen los virus, conciencia del peligro que acecha como usuarios de PCs y equipos conectados a Internet.
- Fines de los 90s - las amenazas se generalizan.
  - Se toma en serio la seguridad: década de los 00s

¿Qué hay de nuevo en los 00s?

- Principalmente por el uso de Internet, el tema de la protección de la información se transforma en una necesidad y con ello se populariza la terminología técnica asociada a la criptología:
  - Cifrado, descifrado, criptoanálisis, firma digital.
  - Autoridades de Certificación, comercio electrónico.
- Ya no sólo se transmiten estas enseñanzas en las universidades. El usuario final desea saber, por ejemplo, qué significa ***firmar*** un e-mail.
- Productos futuros: Seguridad añadida

Seguridad Física vs Seguridad Lógica

- El estudio de la seguridad informática puede plantearse desde dos enfoques:
  - Seguridad Física: protección del sistema ante las amenazas físicas, planes de contingencia, control de acceso físico, políticas de backups, etc.
  - Seguridad Lógica: protección de la información en su propio medio mediante el enmascaramiento de la misma usando técnicas de criptografía.

¿Encriptar o cifrar?

- Cifra o cifrado:
  - Técnica que, en general, protege o autentica a un documento o usuario al aplicar un algoritmo criptográfico. Sin conocer una clave específica, no será posible descifrarlo o recuperarlo.
- Por influencia del inglés: encriptar.
  - No existe, ...*¿Meter a alguien dentro de una cripta?*

Criptografía

Kriptós – “esconder”
Ghaphein – “escribir”

Rama de las Matemáticas -*y en la actualidad de la Informática y Redes de Cómputo*- que hace uso de métodos y técnicas matemáticas para cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves.

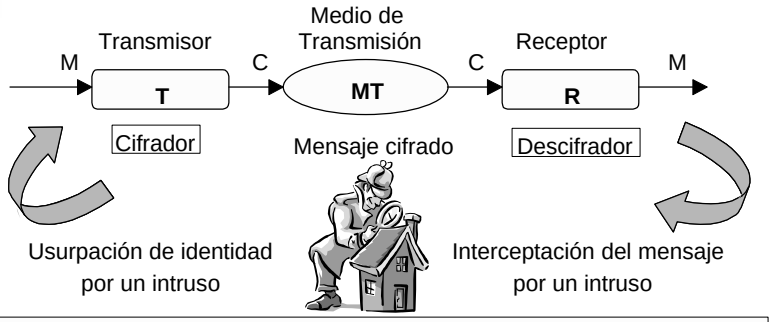
Los criptosistemas permiten establecer cuatro aspectos fundamentales de la seguridad informática:

- Confidencialidad,
- Integridad,
- Autenticación y
- No repudio de emisor y receptor.

¿Porqué usarla?

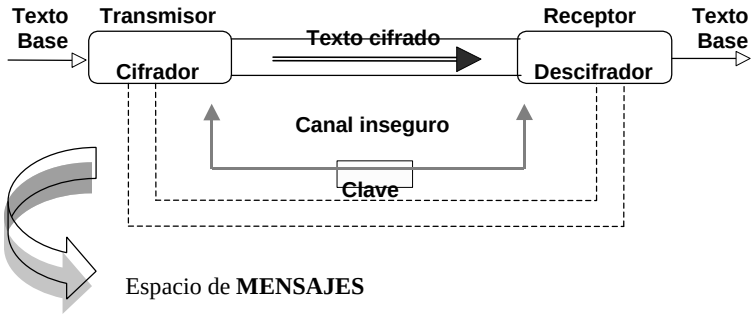
- El delito informático parece ser un “buen negocio”:
- Objeto Pequeño: la información está almacenada en “contenedores pequeños”: no es necesario un camión para robar el banco, joyas, dinero, ...
- Contacto Físico: no existe contacto físico en la mayoría de los casos. Se asegura el anonimato y la integridad física del delincuente.
- Alto Valor: el objeto codiciado tiene un alto valor. El contenido (los datos) vale mucho más que el soporte que los almacena (disquete, disco compacto, ...).
- Unica solución: el uso de técnicas criptográficas.

Sistema de cifradp



Sea cual sea el medio de transmisión (enlace, red telefónica, red de datos, disco magnético, disco óptico, etc.) éste por definición es **INSEGURO.**

Esquema de un criptosistema



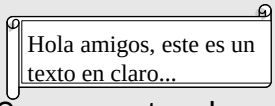
Espacio de **MENSAJES**

Espacio de **TEXTOS CIFRADOS**

Espacio de **CLAVES**

Transformaciones de **CIFRADO y DESCIFRADO**

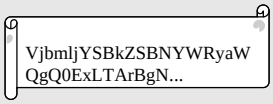
Espacio de mensajes M



$M = \{m_1, m_2, \ldots, m_n\}$

- Componentes de un mensaje inteligible (bits, bytes, pixeles, signos, caracteres, etc.) que provienen de un alfabeto.
- El lenguaje tiene unas reglas sintácticas y semánticas.
- En algunos casos y para los sistemas de cifra clásicos la longitud del alfabeto indicará el módulo en el cual se trabaja. En los modernos, no guarda relación.
- Habrá mensajes con sentido y mensajes sin sentido.

Espacio de textos cifrados C



$C = \{c_1, c_2, \ldots, c_n\}$

- Normalmente el alfabeto es el mismo que el utilizado para crear el mensaje en claro.
- Supondremos que el espacio de los textos cifrados C y el espacio de los mensaje M (con y sin sentido) tienen igual magnitud.
- En este caso, a diferencia del espacio de mensajes M, serán válidos todo tipo de criptogramas.

Espacio de claves K

$K = \{k_1, k_2, \ldots, k_n\}$

- Si el espacio de claves K es tan grande como el de los mensajes M, se obtendrá un criptosistema con secreto perfecto.
- Se supone que es un conjunto altamente aleatorio de caracteres, palabras, bits, bytes, etc., en función del sistema de cifra. Al menos una de las claves en un criptosistema se guardará en secreto.

Transformaciones de cifrado E_k

$E_k: M \rightarrow C \qquad k \in K$

- E_k es una aplicación con una clave k, que está en el espacio de claves K, sobre el mensaje M y que lo transforma en el criptograma C.
- Es el algoritmo de cifra. Sólo en algunos sistemas clásicos el algoritmo es secreto. Por lo general será de dominio público y su código fuente estará disponible en Internet.

Transformaciones de descifrado D_k

$D_k: C \rightarrow M \qquad k \in K$

- D_k es una aplicación con una clave k, que está en el espacio de claves K, sobre el criptograma C y que lo transforma en el texto en claro M.
- Se usa el concepto de inverso. D_k será la operación inversa de E_k o bien -que es lo más común- se usa la misma transformación E_k para descifrar pero con una clave k' que es la inversa de k dentro de un cuerpo.

Requisitos de un criptosistema

- Algoritmo de cifrado/descifrado rápido y fiable.
- Posibilidad de transmitir ficheros por una línea de datos, almacenarlos o transferirlos.
- No debe existir retardo debido al cifrado o descifrado.
- La seguridad del sistema deberá residir solamente en el secreto de una clave y no de las funciones de cifra.
- La fortaleza del sistema se entenderá como la *imposibilidad computacional* de romper la cifra o encontrar la clave secreta.

Recomendaciones de Bacon

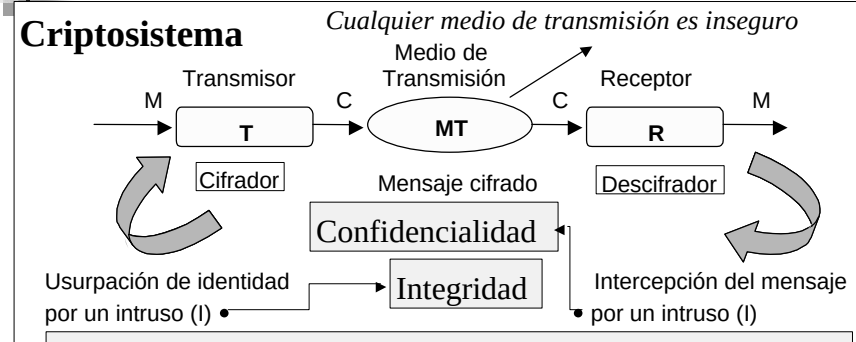
- Filósofo y estadista inglés del siglo XVI
  - Dado un texto en claro M y un algoritmo de cifra E_k, el cálculo de $E_k(M)$ y su inversa debe ser *sencillo*.
  - Será *imposible* encontrar el texto en claro M a partir del criptograma C si se desconoce la función de descifrado D_k.
  - El criptograma deberá contener caracteres distribuidos para que su *apariencia* sea inocente y no dé pistas a un intruso.

Recomendaciones de Kerckhoffs

- Profesor holandés en París del siglo XIX
  - $\mathbf{K_1}$: El sistema debe ser en la *práctica imposible* de criptoanalizar.
  - $\mathbf{K_2}$: Las limitaciones del sistema no deben plantear *dificultades* a sus usuarios.
  - $\mathbf{K_3}$: Método de elección de claves *fácil* de recordar.
  - $\mathbf{K_4}$: Transmisión del texto cifrado por *telégrafo*.
  - $\mathbf{K_5}$: El criptógrafo debe ser *portable*.
  - $\mathbf{K_6}$: No debe existir una larga lista de *reglas* de uso.

Confidencialidad e Integridad

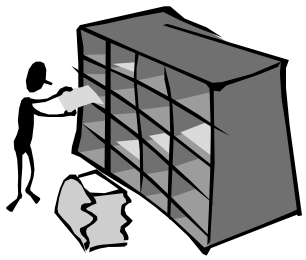
Criptosistema



Estos dos principios de la seguridad informática, el de la confidencialidad y la integridad, (además de la disponibilidad y el no repudio) serán muy importantes en un sistema de intercambio de información segura a través de Internet.

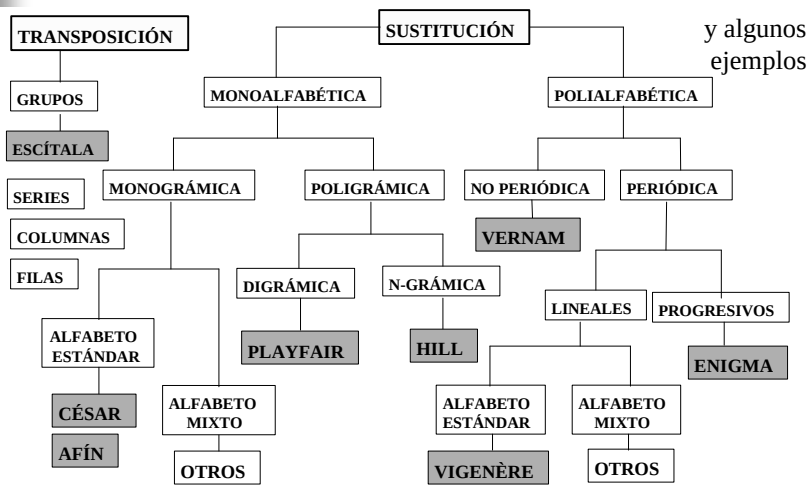
Clasificación de los criptosistemas

- Sistemas de cifra: clásicos vs modernos
  - Clasificación histórica y cultural.
- Sistemas de cifra: en bloque vs en flujo
  - Clasificación de acuerdo a cómo se produce la cifra.



- Sistemas de clave: secreta vs pública
  - Clasificación de acuerdo a la cifra usando una única clave secreta o bien sistemas con dos claves, una de ellas pública y la otra privada.

Clasificación de los criptosistemas clásicos



Hitos históricos de la criptografía

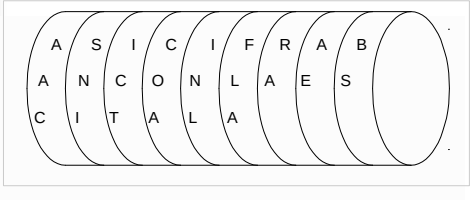
- La criptografía clásica abarca desde tiempos inmemoriales hasta la mitad del siglo XX.
- El punto de inflexión en esta clasificación la marcan tres hechos relevantes:
  - En el año 1948 se publica el estudio de Claude Shannon sobre la Teoría de la Información.
  - En 1974 aparece el estándar de cifra DES.
  - En el año 1976 se publica el estudio realizado por W. Diffie y M. Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifra, denominado cifrado con clave pública.

CIFRADO DIGITAL

El cifrador de la escítala

- La escítala era usada en el siglo V a.C. por el pueblo griego lacedemonios. Consistía en un bastón en el que se enrollaba una cinta y luego se escribía en ella el mensaje de forma longitudinal.
- Al desenrollar la cinta, las letras aparecían sin orden alguno.
- La única posibilidad de deshacer esta cifra pasaba por enrollar dicha cinta en un bastón con el mismo diámetro que el usado en el extremo emisor y leer el mensaje de forma longitudinal.

Método de cifra de la escítala



Se trata de un sistema de cifra por transposición

El texto en claro es:

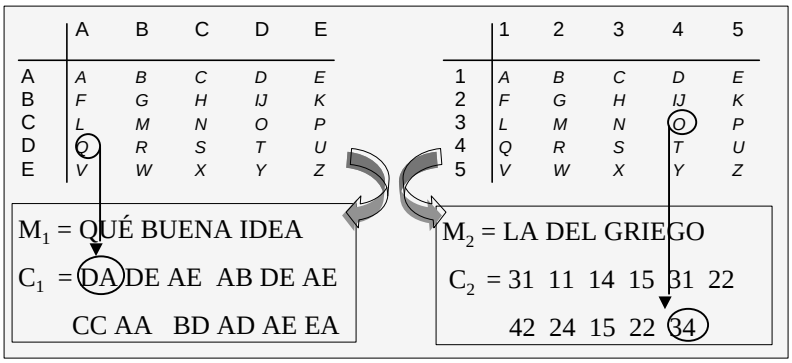
M = ASI CIFRABAN CON LA ESCITALA

El texto cifrado o criptograma será:

C = AAC SNI ICT COA INL FLA RA AE BS

El cifrador de Polybios

Es el cifrador por sustitución de caracteres más antiguo que se conoce (siglo II a.C.) pero duplica el tamaño.



El cifrador del César

En el siglo I a.C., Julio César presenta este cifrador cuyo algoritmo consiste en el desplazamiento de tres espacios hacia la derecha de los caracteres del texto en claro. Es un cifrador por sustitución en el que las operaciones se realizan módulo *n*, siendo *n* igual al número de elementos del alfabeto (latín).

M_i	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
C_i	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

Alfabeto de cifrado del César para castellano mod 27

Ejemplo de cifra con cifrador del César

M_i	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
C_i	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

M = **E**L P**A**TIO D**E** MI C**A**S**A** **E**S P**A**RTICUL**A**R

C = **H**Ñ S**D**WLR G**H** OL F**D**V**D** **H**V S**D**UWLFXÑ**D**U

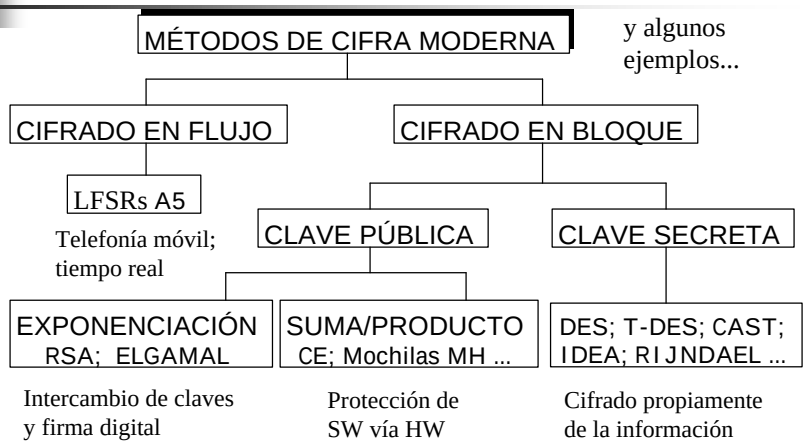
Cada letra se cifrará siempre igual. Es una gran debilidad y hace que este sistema sea muy vulnerable y fácil de atacar simplemente usando las estadísticas del lenguaje.

Tipos de Criptosistemas

Clasificación

- Según el tratamiento del mensaje:
  - Cifrado en bloque (DES, IDEA, RSA: 64 - 128 bits)
  - Cifrado en flujo (A5) cifrado bit a bit
- Según el tipo de claves se dividen en:
  - Cifrado con clave secreta **Sistemas simétricos**
  - Cifrado con clave pública **Sistemas asimétricos**

Clasificación de los criptosistemas



Cifrado en bloque y en flujo

- **CIFRADO EN BLOQUE**:
  - El mismo algoritmo de cifra se aplica a un bloque de información (grupo de caracteres, número de bytes, etc.) repetidas veces, usando la misma clave.
- **CIFRADO EN FLUJO**:
  - El algoritmo de cifra se aplica a un elemento de información (carácter, bit) mediante un flujo de clave en teoría aleatoria y mayor que el mensaje.

Comparativa cifrado en bloque v/s flujo

CIFRADO EN BLOQUE

Ventajas:

- Alta difusión de los elementos en el criptograma.
- Inmune: imposible introducir bloques extraños sin detectarlo.

Desventajas:

* Baja velocidad de cifrado al tener que leer el bloque.
* Propenso a errores de cifra. Un error se propagará a todo el bloque.

CIFRADO EN FLUJO

Ventajas:

- Alta velocidad de cifra al no tener en cuenta otros elementos.
- Resistente a errores. Cifra independiente de cada elemento.

Desventajas:

* Baja difusión de elementos en el criptograma.
* Vulnerable. Pueden alterarse los elementos por separado.

Introducción al cifrado de flujo

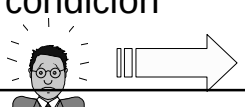
Usa el concepto de cifra propuesto por Vernam, que cumple con las ideas de Shannon sobre sistemas de cifra secreto perfecto, esto es:

a) El espacio de las claves es igual o mayor que el espacio de los mensajes.

b) Las claves deben ser equiprobables.

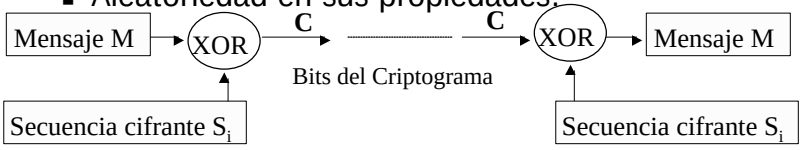
c) La secuencia de clave se usa una sola vez y luego se destruye (sistema *one-time pad*).

DUDA: ¿Es posible satisfacer la condición **a)**?



Técnica de cifra en flujo

- ✓ El mensaje en claro se leerá bit a bit.
- ✓ Se realizará una operación de cifra, normalmente la función XOR, con una secuencia cifrante de bits S_i que debe cumplir ciertas condiciones:
  - Un período muy alto.
  - Aleatoriedad en sus propiedades.



Criptosistemas simétricos y asimétricos

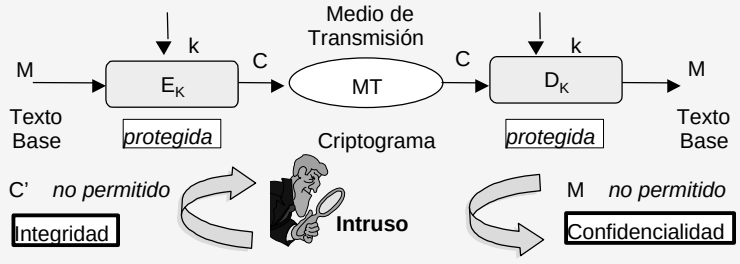
- Criptosistemas simétricos:
  - Existirá una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra por lo que la seguridad reside en mantener dicha clave en secreto.
- Criptosistemas asimétricos:

Cada usuario crea dos claves, una *privada* y otra *pública*, inversas dentro de un cuerpo finito.

- Cifra en tx con una clave, descifra en rx con la clave inversa.
- La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública. Para ello usan funciones matemáticas de un solo sentido con trampa.

Criptosistemas simétricos

Cifrado con criptosistemas de clave secreta



La confidencialidad y la integridad se lograrán si se protegen las claves en el cifrado y en el descifrado. Es decir, se obtienen *simultáneamente* si se protege la clave secreta.

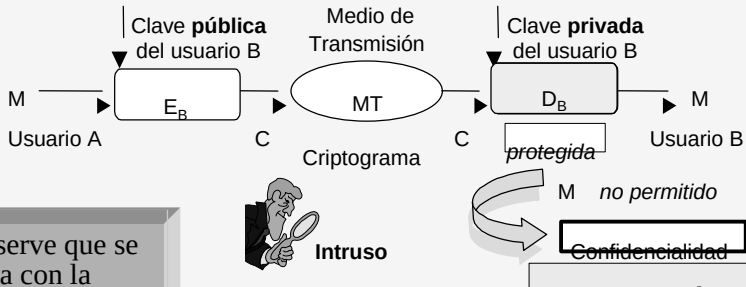
DES, TDES, IDEA, CAST, RIJNDAEL

Criptosistemas asimétricos (1)

Cifrado con clave pública del receptor

Intercambio de claves RSA

Intercambio: RSA y DH



Observe que se cifra con la clave pública del destinatario.

Las claves de E_B y D_B son "inversas"

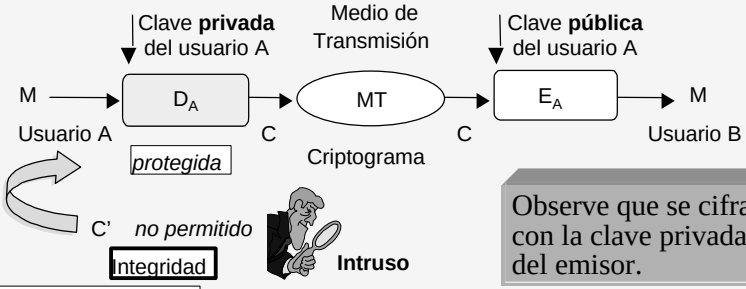
Un sistema similar es el intercambio de clave de Diffie y Hellman DH

Criptosistemas asimétricos (2)

Cifrado con clave privada del emisor

Firma digital RSA

Firmas: RSA y DSS



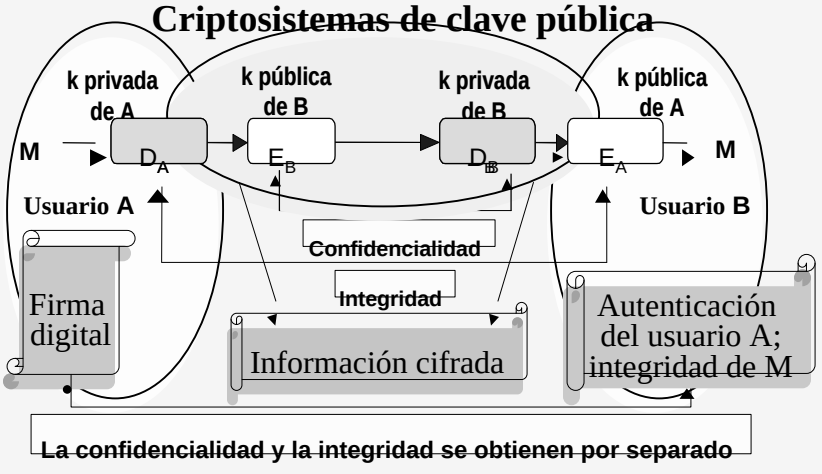
Observe que se cifra con la clave privada del emisor.

Se firma sobre un hash H(M) del mensaje, por ejemplo MD5 o SHA-1

Las claves de E_A y D_A son "inversas"

La firma DSS está basada en el algoritmo de cifra de El Gamal

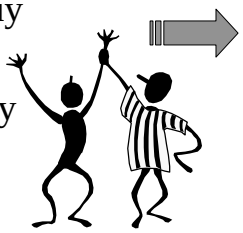
Tipos de cifra con sistemas asimétricos



¿Qué usar, simétricos o asimétricos?

Los sistemas de clave pública son muy lentos pero tienen firma digital.

Los sistemas de clave secreta son muy rápidos pero no tienen firma digital.



¿Qué hacer?

Cifrado de la información:
Sistemas de clave secreta
Firma e intercambio de clave de sesión:
Sistemas de clave pública

La solución híbrida

¿Es entonces la clave pública la solución?

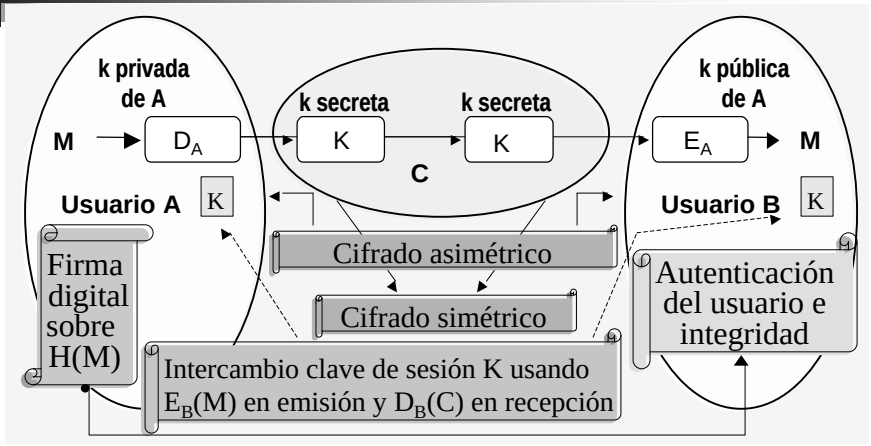
NO

- Tendrá como inconveniente principal (debido a las funciones de cifra empleadas) una tasa o velocidad de cifra mucho <u>más baja</u> que la de los criptosistemas de clave secreta.

¿Solución?

Sistemas de cifra híbridos

Sistema híbrido de cifra y firma



Fortaleza: tipos de ataques

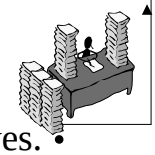
Conociendo el algoritmo de cifra, el criptoanalista intentará romper la cifra:

1. Contando únicamente con el criptograma.
2. Contando con texto en claro conocido.
3. Eligiendo un texto en claro.
4. A partir de texto cifrado elegido.

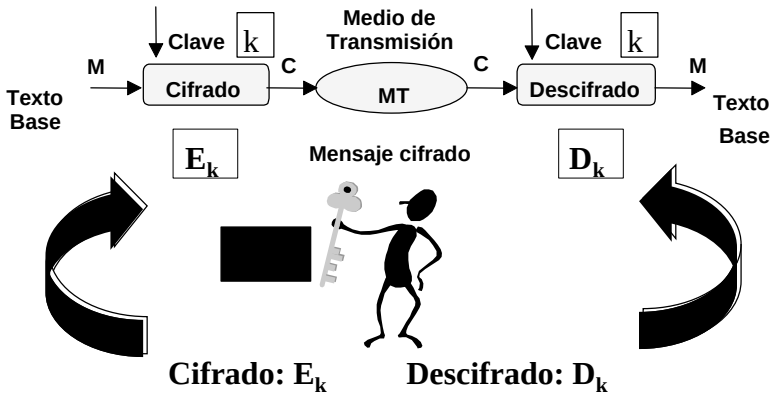
ATAQUE POR FUERZA BRUTA

5. Buscando combinaciones de claves.

Mayor trabajo



Criptosistemas de clave secreta



Funciones y operaciones de cifra

- C = E(M)
- M = D(C)
- M = D(E(M))

E: Cifrado del mensaje M

D: Descifrado del criptograma C

Las operaciones D y E son inversas o bien lo son las claves que intervienen. Esto último es lo más normal, con los inversos dentro de un cuerpo finito. Por lo tanto, se recupera el mensaje en claro.

Si se usa una clave k:

- C = E(k,M) o E_k(M)
- M = D(k, E(k,M))
- M = D(k_D, E(k_E,M))

En este caso los algoritmos E y D son iguales

Secreto en un sistema criptográfico

Shannon midió el secreto de un criptosistema como la incertidumbre del mensaje en claro conocido el criptograma recibido:

Mensajes $M = \{M_1, M_2, \ldots, M_3\}$ $\sum_M p(M) = 1$

Criptogramas $C = \{C_1, C_2, \ldots, C_3\}$ $\sum_C p(C) = 1$

Claves $K = \{K_1, K_2, \ldots, K_3\}$ $\sum_K p(K) = 1$

¿Cuando tendrá nuestro sistema un secreto perfecto?

Definiciones previas secreto criptográfico

- **p(M)**: Probabilidad de enviar un mensaje M. Si hay n mensajes M_i equiprobables, $p(M_i) = 1/n$.
- **p(C)**: Probabilidad de recibir un criptograma C. Si cada uno de los n criptogramas recibidos C_i es equiprobable, $p(C_i) = 1/n$.
- $\mathbf{p_M(C)}$: Probabilidad de que, a partir de un texto en claro M_i, se obtenga un criptograma C_i.
- $\mathbf{p_C(M)}$: Probabilidad de que, una vez recibido un criptograma C_i, éste provenga de un texto claro M_i.

Secreto criptográfico perfecto (1)

Un sistema tiene secreto perfecto si el conocimiento del texto cifrado no proporciona ninguna información acerca del mensaje. Es decir, cuando la probabilidad de acierto al recibir el elemento *i* +1 es la misma que en el estado *i*.

Secreto perfecto $\Rightarrow$ $\mathbf{p(M) = p_C(M)}$

La probabilidad **p** de enviar un mensaje **M** con texto en claro **p(M)** o ***probabilidad a priori*** será igual a la probabilidad **p** de que, conocido un criptograma **C**, éste se corresponda a un mensaje **M** cifrado con la clave **K**. Esta última (***probabilidad a posteriori***) es $\mathbf{p_C(M)}$.

Secreto criptográfico perfecto (2)

La probabilidad **p** de recibir un texto cifrado **C** al cifrar un mensaje **M** usando una clave **K** será $\mathbf{p_M(C)}$. Luego, M debe haberse cifrado con alguna clave K:

$$\mathbf{p_M(C)} = \sum_{\mathbf{K}} \mathbf{p(K)} \quad \text{donde } E_K(M) = C$$

$$\exists\, k_j \,/\, E_{kj}(M_i) = C_i$$

Habrá una condición necesaria y suficiente que se explica en la siguiente diapositiva.

Secreto criptográfico perfecto (3)

La condición necesaria y suficiente del secreto perfecto es que para cualquier valor de M se cumpla que la probabilidad de recibir **C**, resultado de la cifra de un mensaje **M** con una clave **K**, sea la misma que recibir el criptograma **C**, resultado de la cifra de otro mensaje **M'** distinto, cifrado con otra clave.

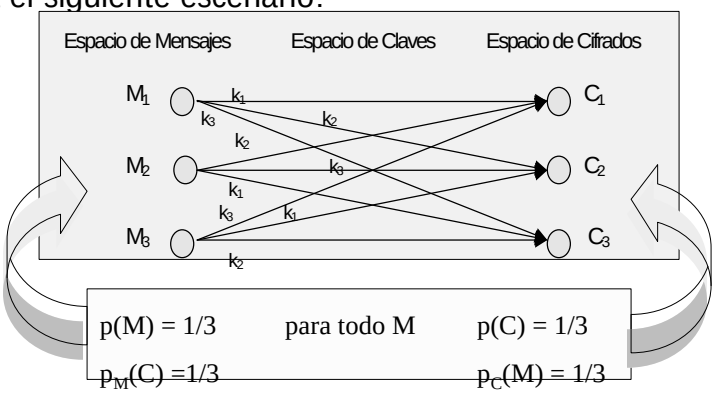
$$p_M(C) = p(C)$$

para todo valor de M

Veamos algunos ejemplos

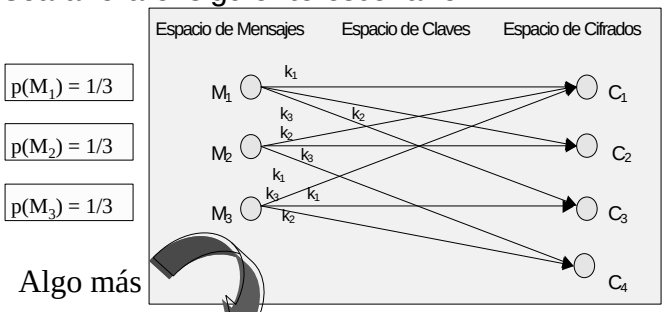
Cifrador con secreto perfecto

Sea el siguiente escenario:



Cifrador sin secreto perfecto (1)

Sea ahora el siguiente escenario:



$p(M_1) = 1/3$

$p(M_2) = 1/3$

$p(M_3) = 1/3$

$p(C_1) = 3/9$

$p(C_2) = 2/9$

$p(C_3) = 2/9$

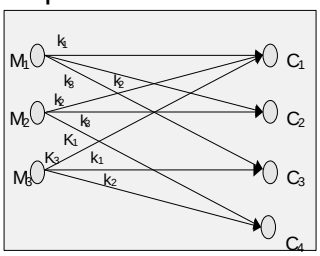
$p(C_4) = 2/9$

Algo más

¿Probabilidad de que un mensaje M_i se convierta en un criptograma C_i: $[P_{Mi}(C_i)]$ y que un criptograma C_i sea el resultado de la cifra de un mensaje M_i: $[P_{Ci}(M_i)]$?

Cifrador sin secreto perfecto (2)

Esquema anterior:



$p_{C1}(M_1) = 1/3$	$p_{C1}(M_2) = 1/3$	$p_{C1}(M_3) = 1/3$
$p_{C2}(M_1) = 1/2$	$p_{C2}(M_2) = 1/2$	$p_{C2}(M_3) = 0$
$p_{C3}(M_1) = 1/2$	$p_{C3}(M_2) = 0$	$p_{C3}(M_3) = 1/2$
$p_{C4}(M_1) = 0$	$p_{C4}(M_2) = 1/2$	$p_{C4}(M_3) = 1/2$

$p_{M1}(C_1) = 1/3$	$p_{M1}(C_2) = 1/3$	$p_{M1}(C_3) = 1/3$	$p_{M1}(C_4) = 0$
$p_{M2}(C_1) = 1/3$	$p_{M2}(C_2) = 1/3$	$p_{M2}(C_3) = 0$	$p_{M2}(C_4) = 1/3$
$p_{M3}(C_1) = 1/3$	$p_{M3}(C_2) = 0$	$p_{M3}(C_3) = 1/3$	$p_{M3}(C_4) = 1/3$

Difusión y confusión

Para lograr un mayor secreto en las operaciones de cifra Shannon propuso dos técnicas:

Difusión: Transformación sobre el texto en claro con objeto de dispersar las propiedades estadísticas del lenguaje sobre todo el criptograma.

TRANSPOSICIONES O PERMUTACIONES

Confusión: Transformación sobre el texto en claro con objeto de mezclar los elementos de éste, aumentando la complejidad de la dependencia funcional entre clave y criptograma.

SUSTITUCIONES

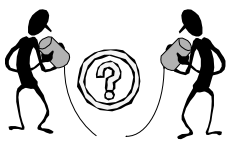
Ambas técnicas serán usadas en todos los sistemas clásicos y también en el DES

Espacio de claves y del mensaje

¿Espacio de Claves ≥ Espacio de Mensajes?

1) La secuencia de bits de la clave deberá enviarse al destinatario a través de un canal que sabemos es inseguro (aún no conocemos el protocolo de intercambio de clave de Diffie y Hellman).
2) Si la secuencia es “infinita”, desbordaríamos la capacidad del canal de comunicaciones.

¿Qué solución damos a este problema?



El concepto de semilla

Si por el canal supuestamente seguro enviamos esa clave tan larga ... ¿por qué entonces no enviamos directamente el mensaje en claro y *nos dejamos de historias*? ☺

La solución está en generar una secuencia de tipo pseudoaleatoria con un algoritmo determinístico a partir de una semilla de sólo unas centenas de bits. Podremos generar así secuencias con períodos del orden de 2^n, un valor ciertamente muy alto. Esta semilla es la que se envía al receptor mediante un sistema de cifra de clave pública y un algoritmo de intercambio de clave y no sobrecargamos el canal.

Introducción a la cifra en bloque

El mensaje se agrupa en bloques, normalmente de 8 bytes, antes de aplicar el algoritmo de cifra a cada bloque de forma independiente con la misma clave.

Cifrado con Clave Secreta

Hay algunos algoritmos muy conocidos por su uso en aplicaciones bancarias (DES), correo electrónico (IDEA, CAST) y en comercio electrónico (T-DES).

No obstante, tienen tres puntos débiles.

Debilidades de la cifra con clave secreta

a) Mala gestión de claves. Crece el número de claves secretas en un orden igual a n^2 para un valor n grande de usuarios 👎.

b) Mala distribución de claves. No existe posibilidad de enviar, de forma segura, una clave a través de un medio inseguro 👎.

c) No tiene firma digital. Aunque sí será posible autenticar el mensaje mediante una marca, no es posible firmar digitalmente el mensaje 👎.

¿Por qué usamos clave secreta?

a) Mala gestión de claves 👎.
b) Mala distribución de claves 👎.
c) No tiene firma digital 👎.

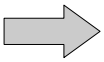
¿Tiene algo de bueno la cifra en bloque con clave secreta?

Sí: la velocidad de cifra es muy alta 👍

Cifrado en bloque con clave pública

Cifrado con Clave Pública

- Comienza a ser ampliamente conocido a través de su aplicación en los sistemas de correo electrónico seguro (PGP y PEM) al permitir incluir una firma digital adjunta al documento o e-mail enviado.
- Cada usuario tiene dos claves, una secreta o privada y otra pública, inversas dentro de un cuerpo.
- Usan las funciones unidireccionales con trampa.



Funciones unidireccionales con trampa

Son funciones matemáticas de un solo sentido (*one-way functions*) y que nos permiten usar la función en sentido directo o de cálculo fácil para cifrar y descifrar (usuarios legítimos) y fuerza el sentido inverso o de cálculo difícil para aquellos (impostores, hackers, etc.) si lo que se desea es atacar o criptoanalizar la cifra.

$f(M) = C$ *siempre es fácil.*

$f^{-1}(C) = M$ *es difícil salvo si se tiene la trampa.*

Funciones con trampa típicas (1)

Problema de la factorización

Cálculo Directo: Producto de dos primos grandes **p*q = n**
Cálculo Inverso: Factorización de número grande **n = p*q**

Problema del logaritmo discreto

Cálculo Directo: Exponenciación discreta **$b = a^x \bmod n$**
Cálculo Inverso: Logaritmo discreto **$x = \log_a b \bmod n$**

Funciones con trampa típicas (2)

Problema de la mochila

Cálculo Directo: Sumar elementos de mochila con trampa
Cálculo Inverso: Sumar elementos de mochila sin trampa

Problema de la raíz discreta

Cálculo Directo: Cuadrado discreto **$x = a*a \bmod n$**
Cálculo Inverso: Raíz cuadrada discreta **$n = \sqrt{a} \bmod n$**

Cifrado con clave pública de destino

NUESTROS PROTAGONISTAS

Benito

Adelaida

Claves: e_B, n_B, d_B

e_B, n_B: públicas

d_B: privada

e_B y d_B son inversas dentro de un cuerpo Z

Si Benito realiza la operación con las claves públicas de Adelaida (e_A, n_A), la información que se transmite mantiene la confidencialidad: sólo ella puede verla.

$C = E_{eA}(M) \bmod n_A$

Claves: e_A, n_A, d_A

e_A, n_A: públicas

d_A: privada

e_A y d_A son inversas dentro de un cuerpo Z

Operación de cifra con clave de destino

Cifrado:

Benito envía un mensaje M a Adelaida

Benito

Claves: e_B, n_B, d_B

$C = E_{eA}(M) \bmod n_A$

Adelaida

Claves: e_A, n_A, d_A

Claves públicas

Descifrado:

Clave privada

$M = E_{dA}[E_{eA}(M)] \bmod n_A$

E_{dA} y E_{eA} son inversos

Recupera el texto en claro: *confidencialidad*

¿Y si usamos la clave pública de origen?

Si en vez de utilizar la clave pública de destino, el emisor usa su propia clave pública, la cifra no tiene sentido bajo el punto de vista de sistemas de clave pública ya que sólo él o ella sería capaz de descifrar el criptograma (deshacer la operación de cifra) con su propia clave privada.

Esto podría usarse para cifrar de forma local uno o varios ficheros, por ejemplo, pero para ello ya están los sistemas de clave secreta, mucho más rápidos y, por tanto, más eficientes.

¿Y si usamos la clave privada de origen?

Si ahora el emisor usa su clave privada en la cifra sobre el mensaje, se obtiene una firma digital que le autentica como emisor ante el destinatario y, además, a este último le permitirá comprobar la integridad del mensaje.

Veamos antes un ejemplo de algoritmo que usa dos claves

Obviamente, el emisor nunca podrá realizar la cifra del mensaje M con la clave privada del receptor.

El algoritmo del mensaje en la caja

PROTOCOLO: A envía a B un mensaje M

1. A pone el mensaje M en la caja, la cierra con su llave y la envía a B.
2. B recibe la caja, la cierra con su llave y envía a A la caja con las dos cerraduras.
3. A recibe la caja, quita su llave y devuelve a B la caja sólo con la cerradura de B.
4. B recibe la caja, quita su cerradura y puede ver el mensaje M que A puso en el interior de la caja.

¿Todo bien en el algoritmo de la caja?

Durante la transmisión, el mensaje está protegido de cualquier intruso por lo que existe integridad del mensaje y hay protección contra una ataque pasivo.

El usuario B no puede estar seguro si quien le ha enviado el mensaje M es el usuario A o un impostor. El algoritmo no permite comprobar la autenticidad del emisor pues no detecta suplantación de identidad.

Una ligera modificación del algoritmo anterior nos permitirá cumplir estos dos aspectos de la seguridad informática

Cifrado con clave privada del origen

origen

Benito

Claves: e_B, n_B, d_B

e_B, n_B: públicas

d_B: privada

e_B y d_B son inversas dentro de un cuerpo Z

Si ahora Benito realiza la operación de cifra con su clave privada d_B en el cuerpo n_B Adelaida será capaz de comprobar esa cifra ya que posee (entre otras) la clave pública de Benito. Comprueba así tanto la autenticidad del mensaje como del autor.

$C = E_{dB}(M) \bmod n_B$

destino

Adelaida

Claves: e_A, n_A, d_A

e_A, n_A: públicas

d_A: privada

e_A y d_A son inversas dentro de un cuerpo Z

Operación de cifra con clave de origen

Cifrado:

Benito firma un mensaje M a Adelaida

Benito

Claves: e_B, n_B, d_B

$C = E_{dB}(M) \bmod n_B$

Adelaida

Claves: e_A, n_A, d_A

Clave privada

Claves públicas

Descifrado:

$M = E_{eB}[E_{dB}(M)] \bmod n_B$

E_{dB} y E_{eB} son inversos

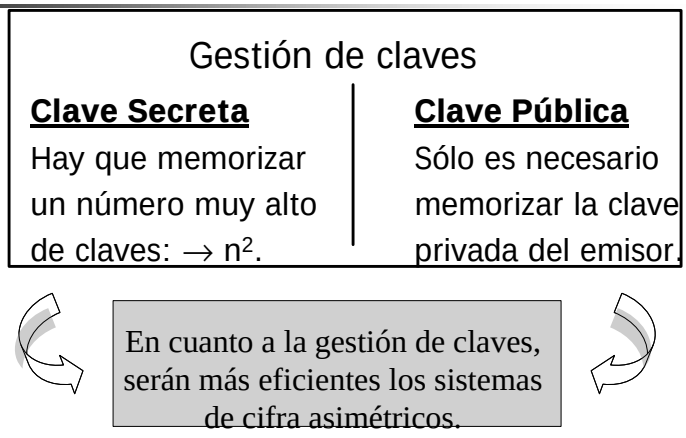
Se comprueba la *integridad* del origen

Uso de la criptografía asimétrica

¿Qué aplicación tendrán entonces los sistema de criptografía de clave pública o asimétrica?

- Usando la clave pública del destino se hará el intercambio de claves de sesión de una cifra con sistemas simétricos (decenas a centenas de bits).
- Usando la clave privada de origen, se firmará digitalmente un resumen (decenas a centenas de bits) del mensaje obtenido con una función hash.

Gestión de claves



Espacio de claves

Longitud y espacio de claves

Clave Secreta	**Clave Pública**
Debido al tipo de cifrador usado, la clave será del orden de la ***centena*** de bits.	Por el algoritmo usado en la cifra, la clave será del orden de los ***miles*** de bits.

^{3} **128**

En cuanto al espacio de claves, no son comparables los sistemas simétricos con los asimétricos.

^{3} **1024**

Vida de la claves

Vida de una clave

Clave Secreta	**Clave Pública**
La duración es muy corta. Normalmente se usa como una clave de sesión.	La duración de la clave pública, que la entrega y gestiona un tercero, suele ser larga.

Segundos, minutos

En cuanto a la vida de una clave, en los sistemas simétricos ésta es muchísimo menor que la de las usadas en los asimétricos.

Meses, años

Vida de la clave y principio de caducidad

Si en un sistema de clave secreta, ésta se usa como clave de una sesión que dura muy poco tiempo...

y en este tiempo es imposible romperla...

¿para qué preocuparse entonces?

La confidencialidad de la información tiene una *caducidad*. Si durante este tiempo alguien puede tener el criptograma e intentar un ataque por fuerza bruta, obtendrá la clave (*que es lo menos importante*) ...

¡**pero también el mensaje secreto**!

El problema de la autenticación

Condiciones de la autenticidad:

a) El usuario **A** deberá protegerse ante mensajes dirigidos a **B** que un tercer usuario desconocido **C** introduce por éste. Es la suplantación de identidad o problema de la autenticación del emisor.

b) El usuario **A** deberá protegerse ante mensajes falsificados por **B** que asegura haberlos recibido firmados por **A**. Es la falsificación de documento o problema de la autenticación del mensaje.

Autenticación de origen y destino

Autenticación	
Clave Secreta	**Clave Pública**
Sólo será posible autenticar el mensaje con una marca pero no al emisor.	Al haber una clave pública y otra privada, se podrá autenticar el mensaje y al emisor.

En cuanto a la autenticación, los sistemas asimétricos -a diferencia de los simétricos- permiten una firma digital.

Velocidad de cifra

Velocidad de cifra	
Clave Secreta	**Clave Pública**
La velocidad del cifrado es muy alta. Es el algoritmo de cifra del mensaje.	La velocidad de cifra es muy baja. Se usa para el intercambio de clave y la firma digital.

Cientos de M Bytes/seg

En cuanto a la velocidad de cifra, los sistemas simétricos son de 100 a 1.000 veces más rápidos que los asimétricos.

Cientos de K Bytes/seg

Resumen cifra simétrica v/s asimétrica

Cifrado Simétrico

- Confidencialidad
- Autenticación parcial
- Sin firma digital
- Claves:
  - Longitud pequeña
  - Vida corta
  - Número elevado
- Velocidad alta

Cifrado Asimétrico

- Confidencialidad
- Autenticación total
- Con firma digital
- Claves:
  - Longitud grande
  - Vida larga
  - Número reducido
- Velocidad baja

- Información tomada del curso de criptografía de Jorge Ramió Aguirre.