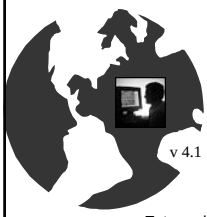
Capítulo 10
Introducción a la Cifra Moderna

Seguridad Informática y Criptografía



Material Docente de
Libre Distribución

Ultima actualización del archivo: 01/03/06
Este archivo tiene: 35 diapositivas

Dr. Jorge Ramió Aguirre
Universidad Politécnica de Madrid

Este archivo forma parte de un curso completo sobre Seguridad Informática y Criptografía. Se autoriza el uso, reproducción en computador y su impresión en papel, sólo con fines docentes y/o personales, respetando los créditos del autor. Queda prohibida su comercialización, excepto la edición en venta en el Departamento de Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España.

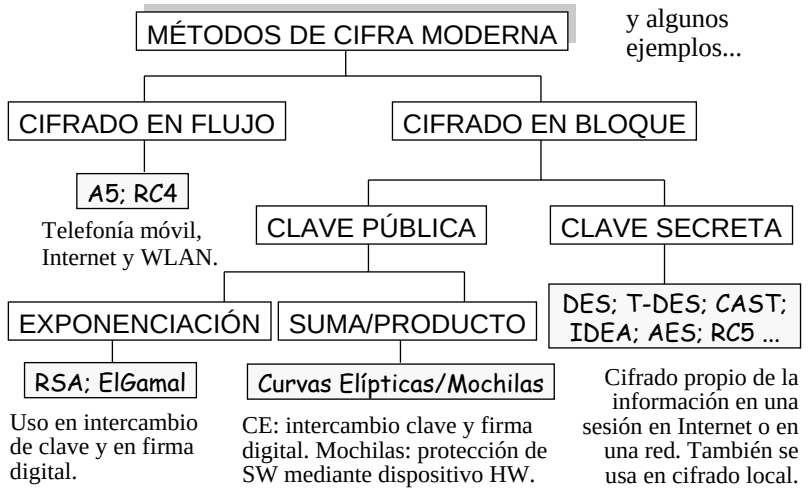
Conceptos elementales

Un par de ideas básicas

- Los criptosistemas modernos, cuya cifra en bits está orientada a todos los caracteres ASCII o ANSI, usan por lo general una operación algebraica en Z_n, un cuerpo finito, sin que necesariamente este módulo deba corresponder con el número de elementos del alfabeto o código utilizado. Es más, nunca coinciden: siempre será mucho mayor el cuerpo de trabajo que el alfabeto usado.
- Su fortaleza se debe basar en la imposibilidad computacional de descubrir una clave secreta única, en tanto que el algoritmo de cifra es (o al menos debería serlo) público.
- En la siguiente dirección web, encontrará un amplio compendio de sistemas de cifra y criptografía.

http://en.wikipedia.org/wiki/Category:Cryptography 

Clasificación de los criptosistemas



© Jorge Ramió Aguirre Madrid (España) 2006

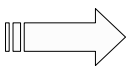
Introducción al cifrado de flujo

Usa el concepto de cifra propuesto por Vernam, que cumple con las ideas de Shannon sobre sistemas de cifra con 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).



Una duda: ¿Será posible satisfacer la condición a)?

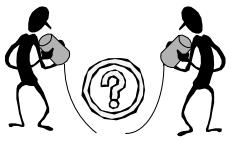
© Jorge Ramió Aguirre Madrid (España) 2006

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 (recuerde que aún no conoce 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?



© Jorge Ramió Aguirre Madrid (España) 2006

El concepto de semilla en un generador

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

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

© Jorge Ramió Aguirre Madrid (España) 2006

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:
  - Tener un período muy alto (ya no infinito)
  - Tener propiedades pseudoaleatorias (ya no aleatorias)

© Jorge Ramió Aguirre Madrid (España) 2006

Introducción a la cifra en bloque

El mensaje se agrupa en bloques, por lo general de 8 ó 16 bytes (64 ó 128 bits) 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), comercio electrónico (Triple DES) y el nuevo estándar (AES Rijndael).

© Jorge Ramió Aguirre Madrid (España) 2006

¿Qué tamaño de bloque usar?

Si el bloque fuese muy pequeño, por ejemplo uno o dos bytes, esto facilitaría un ataque por estadísticas del lenguaje. Se trataría de un cifrado por monogramas o digramas muy débil.

Pero si el bloque fuese muy grande, por ejemplo cientos de bytes, el sistema sería lento en el tratamiento del texto en claro y no sería bueno su rendimiento.

Los valores indicados de 64 y 128 bits son un término medio que satisface ambas condicionantes: es la típica situación de compromiso que tanto vemos en ingeniería.

© Jorge Ramió Aguirre Madrid (España) 2006

Tres debilidades en la cifra simétrica

a) Mala gestión de claves. Crece el número de claves secretas en una proporción igual a n^2 para un valor n grande de usuarios lo que imposibilita usarlo 👎.

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

c) No tiene firma digital. Aunque sí será posible autenticar el mensaje mediante una marca, no es posible firmar digitalmente el mensaje, al menos en un sentido amplio y sencillo 👎.

© Jorge Ramió Aguirre Madrid (España) 2006

¿Por qué usamos entonces clave secreta?

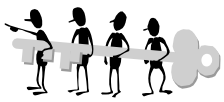
a) Mala gestión de claves 👎
b) Mala distribución de claves 👎
c) No permite firma digital 👎

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

Sí: la velocidad de cifra es muy alta 👍 y por ello se usará para realizar la función de cifra de la información. Además, con claves de sólo unas centenas de bits obtendremos una alta seguridad pues la no linealidad del algoritmo hace que en la práctica el único ataque factible sea por fuerza bruta.

© Jorge Ramió Aguirre Madrid (España) 2006

Cifrado asimétrico



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

© Jorge Ramió Aguirre Madrid (España) 2006

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. que lo que desean es atacar o criptoanalizar la cifra.

$f(M) = C$ es *siempre fácil.*

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

© Jorge Ramió Aguirre Madrid (España) 2006

Funciones con trampa más usadas

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 $\beta = \alpha^x \bmod n$
Cálculo inverso: logaritmo discreto $x = \log_\alpha \beta \bmod n$

© Jorge Ramió Aguirre Madrid (España) 2006

Otras funciones con trampa

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 $a = \sqrt{x} \bmod n$

© Jorge Ramió Aguirre Madrid (España) 2006

Cifrado con clave pública de destino

Origen — ESTOS SERÁN NUESTROS PROTAGONISTAS — Destino

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 n_B

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

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

Adela

Claves: e_A, n_A, d_A

e_A, n_A: públicas
d_A: privada

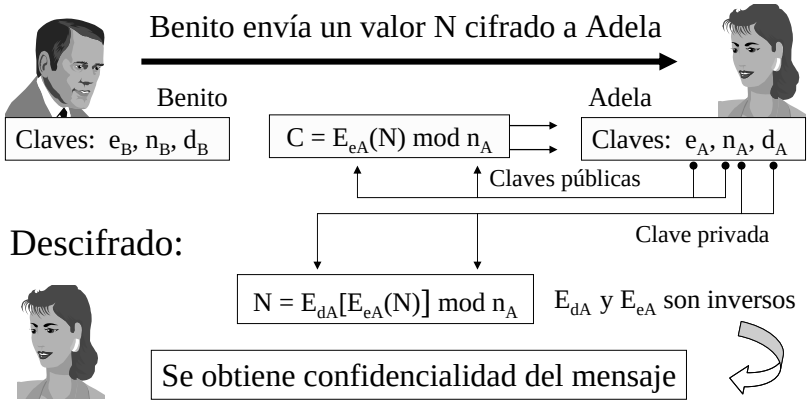
e_A y d_A son inversas dentro de un cuerpo n_A

¿A qué es mucho más lógico y familiar usar estos nombres y no Alice y Bob?

© Jorge Ramió Aguirre Madrid (España) 2006

Operación de cifra con clave de destino

Cifrado:



Descifrado:

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

E_{dA} y E_{eA} son inversos

Se obtiene confidencialidad del mensaje

© Jorge Ramió Aguirre Madrid (España) 2006

¿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.

© Jorge Ramió Aguirre Madrid (España) 2006

¿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 un par de claves entre dos usuarios... ⟶

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

© Jorge Ramió Aguirre Madrid (España) 2006

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 azul 🔒 y la envía a B.

2 B recibe la caja, la cierra con su llave roja 🔒 y envía a A la caja con las dos cerraduras 🔒 🔒.

3 A recibe la caja, quita su llave azul 🔓 y devuelve a B la caja sólo con la cerradura de roja 🔒.

4 B recibe la caja, quita su cerradura roja 🔓 y puede ver el mensaje M que A puso en su interior.

© Jorge Ramió Aguirre Madrid (España) 2006

¿Va 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.

Pero el usuario B no puede estar seguro si quien le ha enviado el mensaje M es el usuario A o un impostor. Por lo tanto el algoritmo así implementado no nos permite comprobar la autenticidad del emisor pues no detecta la suplantación de identidad. No obstante... →

Modificando un poco el algoritmo anterior, sí podremos asegurar tanto la integridad del mensaje como la autenticidad de emisor.

© Jorge Ramió Aguirre Madrid (España) 2006

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 n_B

Si ahora Benito realiza la operación de cifra con su clave privada d_B en el cuerpo n_B Adela 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.

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

Destino

Adela

Claves: e_A, n_A, d_A

e_A, n_A: públicas

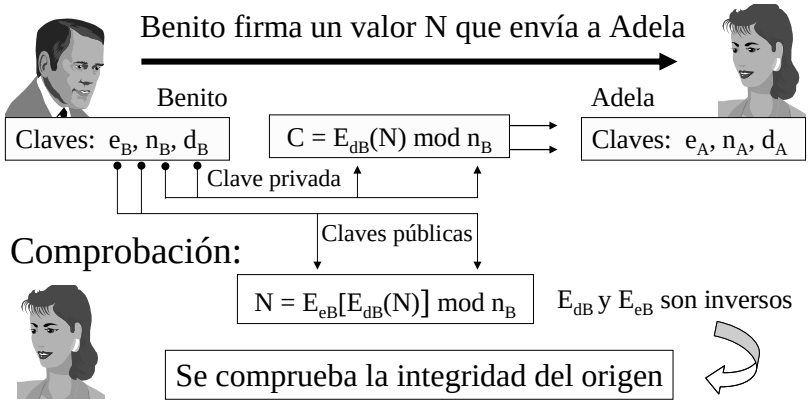
d_A: privada

e_A y d_A son inversas dentro de un cuerpo n_A

© Jorge Ramió Aguirre Madrid (España) 2006

Operación de cifra con clave de origen

Firma digital:



Comprobación:

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

E_{dB} y E_{eB} son inversos

Se comprueba la integridad del origen

© Jorge Ramió Aguirre Madrid (España) 2006

Uso de la criptografía asimétrica

- Estas dos operaciones de cifra son posibles debido a la característica intrínseca de los sistemas de clave pública: el uso de una clave privada (secreta) inversa de una pública.

  ¿Qué aplicación tendrán entonces los sistemas 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 (centenas de bits) del mensaje obtenido con una función hash.
- Observe que se hace hincapié en las “centenas de bits” dado que estos sistemas son muy lentos comparados con los simétricos.

© Jorge Ramió Aguirre Madrid (España) 2006

Comparativa: la gestión de claves

Gestión de claves

Clave Secreta	Clave Pública
Hay que memorizar un número muy alto de claves: $\rightarrow n^2$.	Sólo es necesario memorizar la clave privada del emisor.

En cuanto a la gestión de claves, serán mucho más eficientes los sistemas de cifra asimétricos pues los simétricos no permiten una gestión lógica y eficiente de estas claves: en los asimétricos sólo es necesario memorizar la frase o palabra de paso para acceder a la clave privada.

© Jorge Ramió Aguirre Madrid (España) 2006

Comparativa: el espacio de claves

Longitud y espacio de claves

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

≥ 128

En cuanto al espacio de claves, no son comparables los sistemas simétricos con los asimétricos. Para atacar un sistema asimétrico no se buscará en todo el espacio de claves como debería hacerse en los sistemas simétricos.

≥ 1.024

© Jorge Ramió Aguirre Madrid (España) 2006

Comparativa: la vida de las claves

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

Segundos o minutos

En cuanto a la vida de una clave, en los sistemas simétricos ésta es muchísimo menor que las usadas en los asimétricos. La clave de sesión es aleatoria, en cambio la asimétrica es propia del usuario.

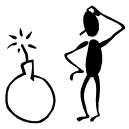
Meses o un año

© Jorge Ramió Aguirre Madrid (España) 2006

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! ... puede ser muy peligroso.

Lo mismo ocurrirá si usamos la cifra simétrica para proteger algún archivo o archivos en nuestro computador.

© Jorge Ramió Aguirre Madrid (España) 2006

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.

© Jorge Ramió Aguirre Madrid (España) 2006

Comparativa: la autenticación de emisor

Autenticación	
Clave Secreta	Clave Pública
Se puede autenticar el mensaje pero no al emisor de forma sencilla y eficiente.	Al haber una clave pública y otra privada, se podrá autenticar el mensaje y al emisor.

En cuanto a la autenticación, los sistemas simétricos tienen una autenticación más pesada y con una tercera parte de confianza. Los asimétricos permiten una firma digital verdadera, eficiente y sencilla, en donde la tercera parte de confianza es sólo presencial.

© Jorge Ramió Aguirre Madrid (España) 2006

Comparativa: la velocidad de cifra

Velocidad de cifra	
Clave Secreta	Clave Pública
La velocidad de cifra 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 HW

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

Cientos de K Bytes/seg en HW

© Jorge Ramió Aguirre Madrid (España) 2006

Resumen comparativo de estas cifras

Cifrado Simétrico	Cifrado Asimétrico
• Confidencialidad	• Confidencialidad
• Autenticación parcial	• Autenticación total
• Sin firma digital	• Con firma digital
• Claves:	• Claves:
– Longitud pequeña	– Longitud grande
– Vida corta (sesión)	– Vida larga
– Número elevado	– Número reducido
• Velocidad alta	• Velocidad baja

© Jorge Ramió Aguirre Madrid (España) 2006

Seguridad en la cifra simétrica y asimétrica

- La criptografía simétrica o de clave secreta usa una única clave para cifrar en emisión y descifrar en destino.
  - La seguridad del sistema reside entonces en cuán segura sea dicha clave.
- En la criptografía asimétrica cada usuario se crea un par de claves llamadas pública y privada, inversas entre sí dentro de un cuerpo finito, de forma que lo que hace una la otra lo deshace. Para cifrar se usa, por ejemplo, la clave pública de destino y para descifrar el destinatario hará uso de su clave privada.
  - La seguridad del sistema reside ahora en la dificultad computacional de encontrar la clave privada a partir de la clave pública.

Fin del capítulo

© Jorge Ramió Aguirre Madrid (España) 2006

Cuestiones y ejercicios (1 de 2)

1. En un sistema de cifra se usa un cuerpo de trabajo n. ¿Cómo es el tamaño de ese cuerpo comparado con el tamaño del alfabeto usado?
2. ¿Cómo se clasifican los criptosistemas en función del tratamiento que hacemos del mensaje a cifrar?
3. ¿Cómo se clasifican los criptosistemas en función de tipo de clave que se usa en ambos extremos, emisor y receptor?
4. ¿Por qué se dice que un sistema es simétrico y el otro asimétrico?
5. ¿Es posible cumplir 100% con la condición de cifrado de Vernam?
6. ¿Por qué en los cifradores de flujo se usa la misma función XOR en el extremo emisor y en el extremo receptor? ¿Son inversas aquí las claves usadas para cifrar y descifrar?
7. Nombre y comente algunas debilidades de los sistemas de cifra en bloque con clave secreta.

© Jorge Ramió Aguirre Madrid (España) 2006

Cuestiones y ejercicios (2 de 2)

8. Si ciframos un número con la clave pública del usuario receptor, ¿qué cree Ud. que estamos haciendo?
9. ¿Por qué decimos que en un sistema asimétrico la gestión de claves es mucho mejor que en un sistema simétrico?
10. Nos entregan un certificado digital (certificación de clave pública) de 512 bits. ¿Es hoy en día un valor adecuado? ¿Por qué sí o no?
11. ¿Por qué decimos que con un sistema asimétrico es muy fácil generar una firma digital en emisión y comprobarla en destino?
12. Compare los sistemas simétricos y asimétricos en cuanto a su velocidad de cifra.
13. ¿Qué es un cifrado híbrido? ¿Por qué y cómo se usa la cifra híbrida en el intercambio de información segura por ejemplo en Internet?
14. ¿Qué relación hay entre vida de una clave y principio de caducidad?

© Jorge Ramió Aguirre Madrid (España) 2006