Introducción a la Criptologia

Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx

Definición y componentes

- *Criptología*.- Ciencia que estudia los aspectos y contenidos de información en condiciones de secrecía.
- Del griego: *criptos* oculto y *logos* tratado
- La Criptología se divide en:
  - *Criptografía.*
  - *Criptoanálisis.*

Criptografía

- Es el *arte* de construir códigos secretos.
- Es el conjunto de técnicas o procedimientos que alteran los símbolos de información sin alterar el contenido, convirtiendo a la información modificada en un conjunto de símbolos sin contenido para las partes que no disponen de las técnicas.

Lámina 3 Dr. Roberto Gómez C.

Criptoanálisis

- Metodologías y técnicas que permiten recuperar la información que ha sido previamente tratada por un procedimiento criptográfico, sin conocer *"a priori"* la técnica utilizada para la criptografia.

Lámina 4 Dr. Roberto Gómez C.

Esteganografía??

- Area similar a la de criptología.
- Viene del griego stegos (ocultar).
- Conjunto de técnicas que nos permiten ocultar o camuflar cualquier tipo de datos.
- La información puede esconderse de cualquier forma
  - esconder documentos electrónicos dentro de imagenes.
  - aprovechar campos no usados de los paquetes de protocolos de redes.

Lámina 5 Dr. Roberto Gómez C.

Ejemplo esteganografía: imagen original

- Imagen original: foto de una casa.
- Imagen con mapas: imagen que esconde información.

Lámina 6 Dr. Roberto Gómez C.

Ejemplo esteganografía: imagen original

Lámina 7 Dr. Roberto Gómez C.

Ejemplo: imagen con marcas

Lámina 8 Dr. Roberto Gómez C.

Ejemplo: información oculta

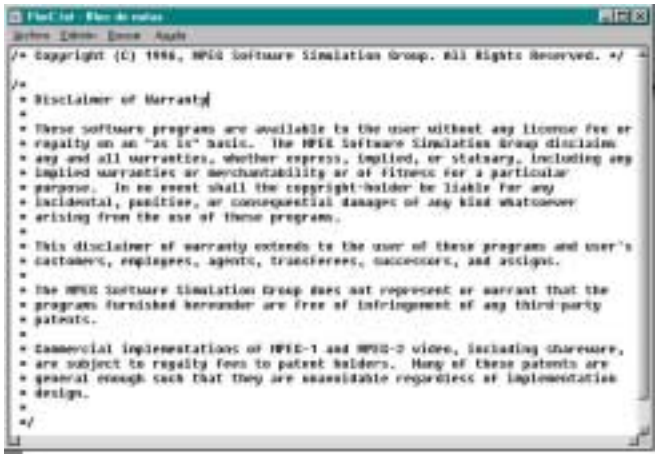


Lámina 9 Dr. Roberto Gómez C.

Comparando las imagenes

Lámina 10 Dr. Roberto Gómez C.

Esteganografía en textos

- Se usan técnicas mas complejas como el "Null Cipher", un ejemplo son los siguientes mensajes

  Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday.

- Si tomamos la tercera letra de cada palabra diría

  Send Lawyers, Guns, and Money.

Lámina 11 Dr. Roberto Gómez C.

Criptosistemas

- Es el conjunto de procedimiento que garantizan la seguridad de la información y utilizan técnicas criptográficas.
- El termino en inglés es cipher.
- El elemento fundamental de un Criptosistema es la *"llave"*.
- En algunas referencias a la llave se le conoce como *clave*.

Lámina 12 Dr. Roberto Gómez C.

Proceso encripción/decripción

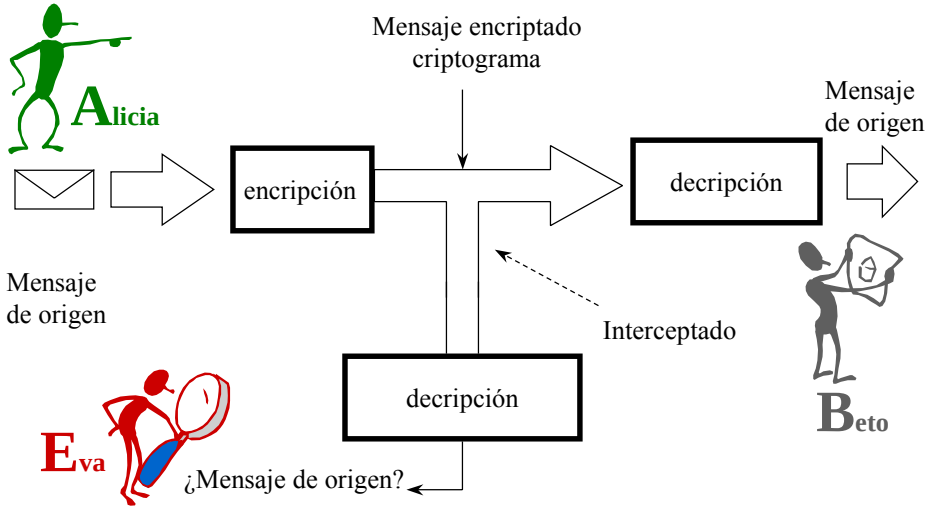


Lámina 13 Dr. Roberto Gómez C.

Objetivos criptografía

- Mantener la confidencialidad del mensaje
  - la información contenida en el mensaje permanezca secreta
- Garantizar la autenticidad tanto del mensaje como del par remitente/destinatario
  - el mensaje recibido ha de ser realmente el enviado
  - el remitente y destinatario han de ser realmente quienes dicen ser y no remitentes y/o destinatarios fraudulentos

Lámina 14 Dr. Roberto Gómez C.

Clasificación seguridad criptográfica

- Seguridad incondicional (teórica).
  - sistema seguro frente a un atacante con tiempo y recursos computacionales ilimitados.
- Seguridad computacional (práctica).
  - el sistema es seguro frente a un atacante con tiempo y recursos computacionales limitados.
- Seguridad probable.
  - no se puede demostrar su integridad, pero el sistema no ha sido violado.

Lámina 15 Dr. Roberto Gómez C.

- Seguridad condicional.
  - todos los demás sistemas, seguros en tanto que el enemigo carece de medios para atacarlos.

Lámina 16 Dr. Roberto Gómez C.

Criptografía y seguridad

- En la práctica la seguridad que ofrece un criptosistema consiste en mostrar que *"cualquier ataque que tiene una probabilidad de romper la llave requiere de una cantidad infinita de computación"*.
- Un sistema criptográfico se dice *inseguro* cuando los contenidos de encripción pueden ser descifrados en un tiempo polinomial.

Lámina 17 Dr. Roberto Gómez C.

Obscuridad vs Seguridad

Si guardo en una caja fuerte una carta, **escondo** la caja en **algún** lugar de Nueva York, y luego les pido que lean la carta, eso **no es seguridad**: es **obscuridad**.

Si por otra parte, guardo en una caja fuerte una carta, **les doy las especificaciones** de la caja, y cientos de cajas fuertes con sus combinaciones para que ustedes y analistas **expertos revisen el mecanismo** de seguridad; y aún así **no pueden** abrir la caja fuerte y leer la carta, eso es **seguridad**."

Principio de Kerchkhoffs

Lámina 18 Dr. Roberto Gómez C.

Procedimientos clásicos de encripción

- Primeros metodos criptograficos
  - epoca romana hasta siglo XX
- Basados en dos técnicas
  - transposición
  - substitución

Lámina 19 Dr. Roberto Gómez C.

La transposición

- Principio:
  - "barajar" los símbolos del mensaje original colocandolos en un orden distinto, de manera que el criptograma contenga los mismos elementos del texto claro, pero colocados de tal forma que resulten incomprensibles.
- Ejemplos
  - La escítala lacedemonia (skytale staff).
  - La técnica "rail fence".
  - Transposición en reversa.

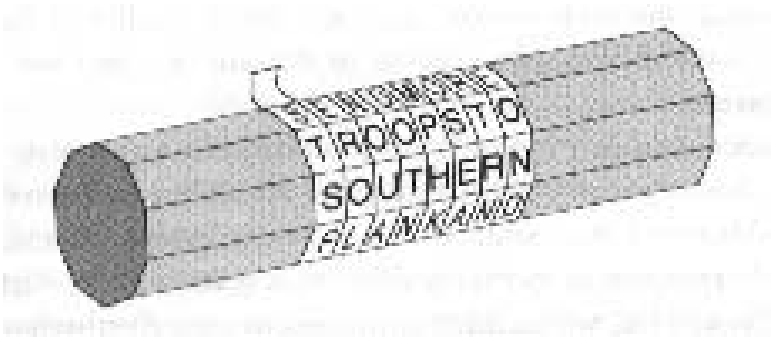
Lámina 20 Dr. Roberto Gómez C.

La escítala lacedemonia

- Dos varas idénticas, alrededor de una de ellas se envolvía una tira de pergamino.
- Mensaje se escribía a lo largo del bastón, se retiraba la cinta y se enviaba.
- El destinatario poseía la segunda vara,
- La cinta por si sola, no era mas que una sucesión de símbolos de alfabeto griego colocados en un orden ininteligible.

Lámina 21 Dr. Roberto Gómez C.

Otro ejemplo skytale



Mensaje: SENDMORETROOPSTOSOUTHERNFLANKAND…
Criptograma: STSFEROLNOUADOTNMPHKOSEARTRNEOND

Lámina 22 Dr. Roberto Gómez C.

La técnica "rail fence"

- El texto claro es escrito hacia abajo como una secuencia de diagonales y es leído como una secuencia de renglones.

hola → **h l**
o a

- Por ejemplo:
  - texto claro: meet me after the toga party
  - con un rail fence de profundidad 2, la encripción da como resultado:

m e m a t r h t g p r y
e t e f e t e o a a t

  - criptograma: **mematrhtgpryetefeteoaat**

Lámina 23 Dr. Roberto Gómez C.

La substitución

- Principio:
  - establecer correspondencia entre las letras del alfabeto en el que está escrito el mensaje original y los elementos de otro conjunto que puede ser el mismo o distinto alfabeto.
- Ejemplos
  - Encriptado de Cesar (siglo I a.C.).
  - Encriptado de Vigenére (1586).

Lámina 24 Dr. Roberto Gómez C.

Criptosistema de Adventures Dancing Men

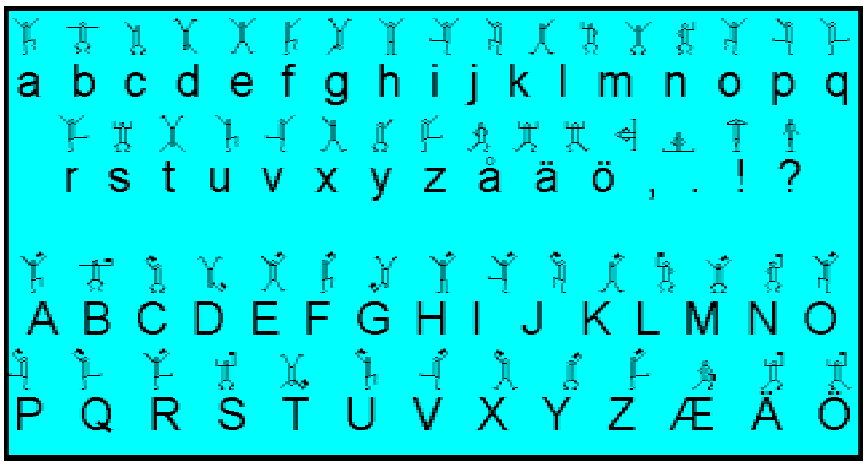


Lámina 25 Dr. Roberto Gómez C.

Encriptado de Cesar

- Sustituye primera letra del alfabeto A, por la cuarta D; la segunda, B, por la quinta E, etc.
- Termino matemático: $\mathbf{Y_i = X_i \oplus Z_i \pmod{26}}$
- Recuperación mensaje
  - se suma nuevamente símbolo a símbolo el criptograma con la inversa de la llave modulo 26
- Desventaja
  - frecuencia de aparición de cada letra en el texto claro se refleja en el criptograma

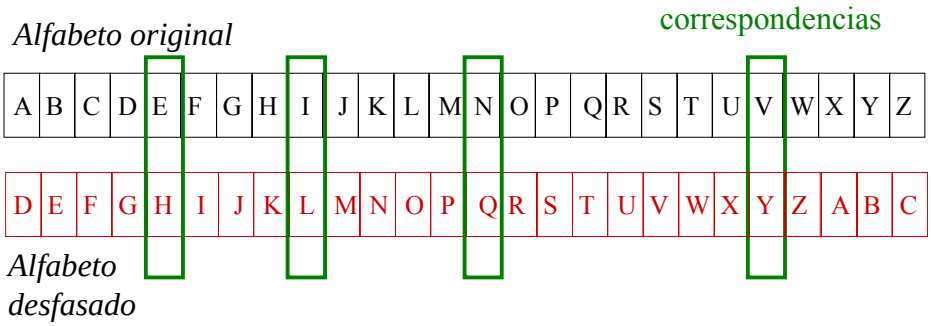
Lámina 26 Dr. Roberto Gómez C.

Ejemplo criptosistema Cesar

- Es del tipo de criptosistemas monoalfabeticos.
- El mensaje a enviar es:
  - VENI VIDI VICI
- El alfabeto estara desplazado hasta la letra D, por lo que
  - Llave: D

Lámina 27 Dr. Roberto Gómez C.

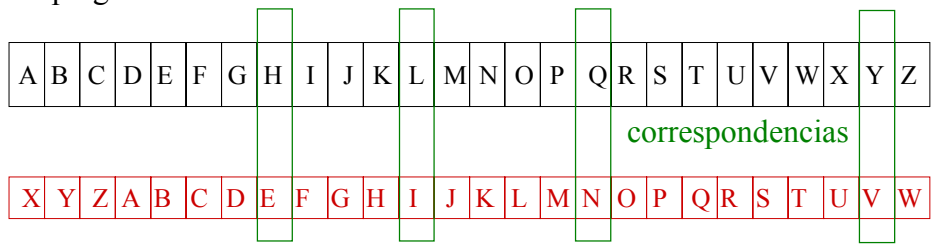
Encriptando el mensaje



Mensaje:	VENI	VIDI	VICI
Llave:	DDDD	DDDD	DDDD
Criptograma:	YHQL	YLGL	YLFL

Lámina 28 Dr. Roberto Gómez C.

Recuperando el mensaje



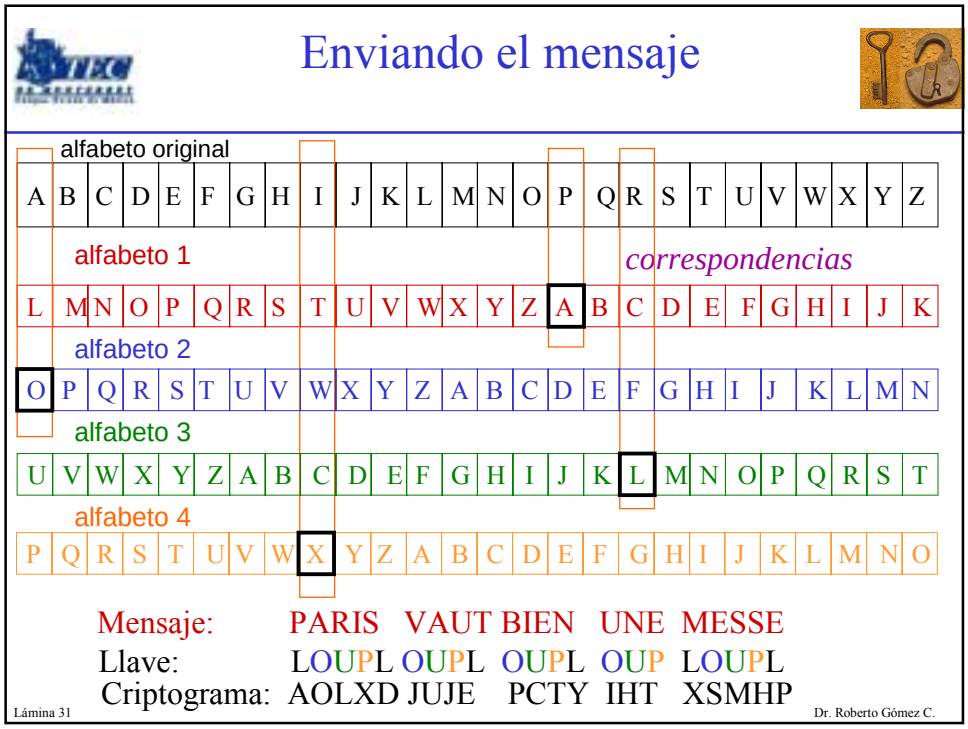
Criptograma:	YHQL	YLGL	YLFL
Llave:	DDDD	DDDD	DDDD
Mensaje:	VENI	VIDI	VICI

Lámina 29
Dr. Roberto Gómez C.

Encriptado de Vigenére

- Generalización del anterior
- La llave toma sucesivamente diferentes valores (criptosistema polifalfabético)
- Termino matemático: $Y_i = X_i \oplus Z_i \pmod{26}$
- Una misma letra en el texto claro le pueden corresponder diferentes letras en el texto cifrado
- Recuperación mensaje es análoga al procedimiento de Cesar
- Ejemplo:
  - Mensaje a enviar: PARIS VAUT BIEN UNE MESSE

Lámina 30
Dr. Roberto Gómez C.


Enviando el mensaje
alfabeto original
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
alfabeto 1
correspondencias
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
alfabeto 2
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
alfabeto 3
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
alfabeto 4
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
Mensaje: PARIS VAUT BIEN UNE MESSE
Llave: LOUPL OUPL OUPL OUP LOUPL
Criptograma: AOLXD JUJE PCTY IHT XSMHP
Lámina 31
Dr. Roberto Gómez C.


Recuperando el mensaje
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
criptograma
correspondencias
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
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
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
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
Criptograma: AOLXD JUJE PCTY IHT XSMHP
Llave: LOUPL OUPL OUPL OUP LOUPL
Mensaje: PARIS VAUT BIEN UNE MESSE
Lámina 32
Dr. Roberto Gómez C.

- Se dice que el método Kasiski (1863) consiguió romperlo.
- En realidad fue Charles Babbage

http://www.math.temple.edu/~renault/cryptology/vigenere.html

Lámina 33 Dr. Roberto Gómez C.

One time pad

- No consiste de una serie de palabras sino una gran serie de letras elegidas al azar
- Propone utilizar este conjunto de letras como parte de un criptosistema de Vigenere
- Principio funcionamiento:
  - Primer paso: conseguir un bloque (pad) de hojas
  - Cada hoja contiene una llave única en forma de lineas de secuencias aleatorias de letras.
  - Dos copias bloque: una para emisor y otra para receptor.
  - Para encriptar el emisor aplica el criptosistema de Vigenere con la primera hoja del bloque como llave.

Lámina 34 Dr. Roberto Gómez C.

Principio funcionamiento

- El receptor puede decriptar usando el mismo cripsistema y con la misma llave.
- Una vez que el mensaje fue encriptado, enviado, recibido y decriptado con éxito, la hoja que se usó como llave se destruye.
- Cuando el siguiente mensaje se va a enviar, la siguiente llave del bloque es usada
  - la cual es subsecuentemente destruida y asi se continua
- Debido a que cada llave es usada una sola vez, el sistema se conoce como onetime pad

Lámina 35 Dr. Roberto Gómez C.

Ejemplo one time pad

Hoja 1	Hoja 2	Hoja 3
P L M O E	O I W V H	J A B P R
Z Q K J Z	P I Q Z E	M F E C F
L R T E A	T S E B L	L G U X D
V C R C B	C Y R U P	D A G M R
Y N N R B	D U V N M	Z K W Y I

Llave: P L M O E Z Q K J Z L R T E A V C R C B Y
Texto claro: a t t a c k t h e v a l l e y a t d a w n
Criptograma: P E F O G J J R N UL C E I Y V V U C X L

Lámina 36 Dr. Roberto Gómez C.

Otros criptosistemas clásicos

- Pigpen
- Redefence
- Nihilist
- Grilla
- El criptosistema de Bacon
- El Polybius square
- Checker board
- Atbash
- Los nomenclators
- Porta
- Playfair
- Grandpre
- Beale
- Criptosistema ADFGVX

Lámina 37 Dr. Roberto Gómez C.

Máquinas criptograficas

- Los discos de encriptamiento
- El cilindro de Jefferson
  - el dispositivo M-94
- La máquina enigma
- La máquina de Lorenz
- La Bomba
- La máquina Coloussus

Lámina 38 Dr. Roberto Gómez C.

Imagenes máquinas criptográficas




Lámina 39
Dr. Roberto Gómez C.

Otras imagenes

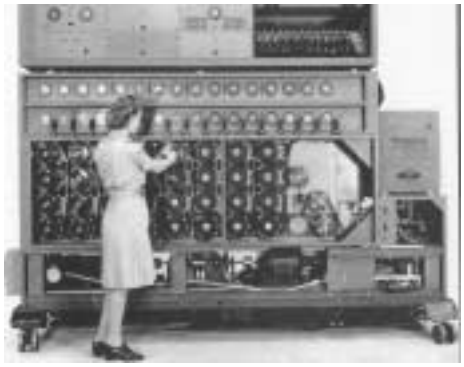


Lámina 40
Dr. Roberto Gómez C.

Encriptando con una computadora

- La computadora *"maneja"* números en lugar de letras
  - solo números binarios (digitos binarios = bits)

a = 1100001
! = 0100001
& = 0100110

- La encripción se realiza bajo mismo principio de substitución y transposición
  - elementos del mensaje son substituidos por otros elementos, o sus posiciones son intercambiadas o ambas

Lámina 41 Dr. Roberto Gómez C.

Encripción por computadora

- Convertir mensaje a ASCII

Texto claro:
HELLO = 1001000 1000101 1001100 1001100 1001111

- Transposición: intercambiar las letras en un orden predeterminado

Texto claro:
HELLO = 1001000100010110011001001100111111
Criptograma:
LHOEL = 1001100100100010011111000101100110 0

- La transposición puede darse a nivel de bits

Letra original: 1001000 **Letra encriptada: 0010010**

Lámina 42 Dr. Roberto Gómez C.

Utilizando una llave

- Es posible utilizar una llave para transformar los bits.
- Por ejemplo supongamos el uso de la llave DAVID.

DAVID = 1000100 1000001 1010110 1001001 1000100

- Para encriptar/decriptar sumamos la llave al mensaje original, (suma binaria: xor)

Texto claro:	**HELLO**
Texto ASCII:	**1001000100010110011001001001001111**
Llave:	**1000100100000110101101001001100010 0**
Criptograma:	**0001100000010000110100000101000101 1**

Lámina 43 Dr. Roberto Gómez C.

Encriptado Vernam

- Representa el caso límite del cifrado de Vigenere
- Emplea alfabeto binario
- Operación aritmética es suma modulo 2
- llave: secuencia binaria aleatoria de la misma longitud que el texto claro, solo se usa una vez
- Ejemplo:

Mensaje:	00011	01111	01101	00101	10011	01111
Llave:	11011	00101	01011	00110	10110	10101
Criptograma:	11000	01010	00110	00011	00101	11010

Lámina 44 Dr. Roberto Gómez C.

Aplicación encriptado Vernan

- Ofrece máximas garantías de seguridad
  - cumple con las condiciones de secrecia perfecta definidas por Shanon
- Inconveniente: requiere un dígito de llave secreta por cada dígito de texto claro
- Reservado para condiciones de máxima seguridad, pero mínima información a proteger
- Teléfono rojo usaba Vernan
- Vernam pensaba usarla para aplicaciones comerciales
  - problema: tamaño llave (igual que el mensaje)

Lámina 45 Dr. Roberto Gómez C.

Métodos Criptográficos

- Métodos Simétricos
  - llave encriptado coincide con la de descifrado
  - la llave tiene que permanecer secreta
  - emisor y receptor se han puesto de acuerdo previamente o existe un centro de distribución de llaves
- Métodos asimétrico
  - llave encriptado es diferente a la de descriptado
  - llave encriptado es conocida por el público, mientras que la de decriptado solo por el usuario

Lámina 46 Dr. Roberto Gómez C.

Sinónimos métodos

- Los métodos simétricos son propios de la criptografía clásica o criptografía de llave secreta
- Los métodos asimétricos corresponden a la criptografía de la llave pública, introducida por Diffie y Hellman en 1976

Lámina 47 Dr. Roberto Gómez C.

Algoritmos encripción de llave secreta

Características principales

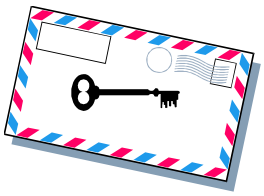


Lámina 48 Dr. Roberto Gómez C.

Características encripción llave secreta

- Algoritmos que ofrecen confidencialidad casi perfecta
- Cada entidad debe asegurar a la otra parte que mantendrá en secreto la llave compartida
- Útil en redes donde el número de usuarios es reducido
- Debe existir un administrador encargado de la generación, asignación y almacenamiento de las llaves

Lámina 49
Dr. Roberto Gómez C.

Esquema general encripción llave secreta

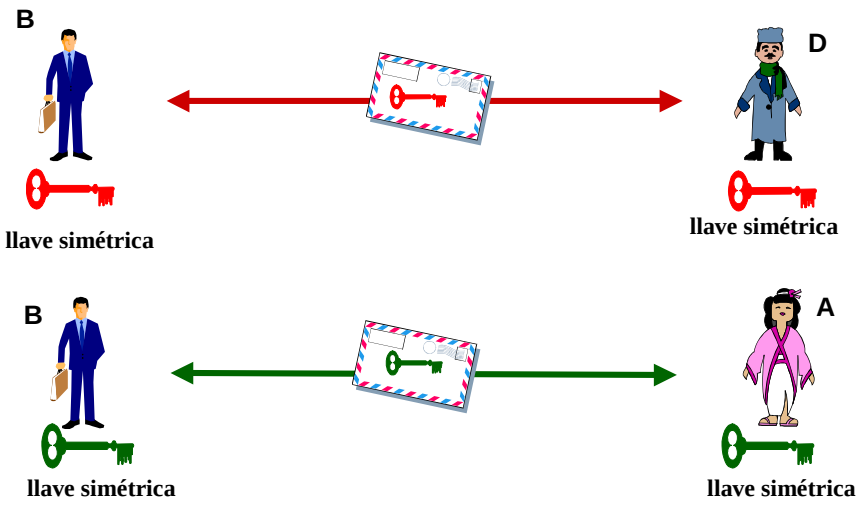


Lámina 50
Dr. Roberto Gómez C.

Encripción llave secreta

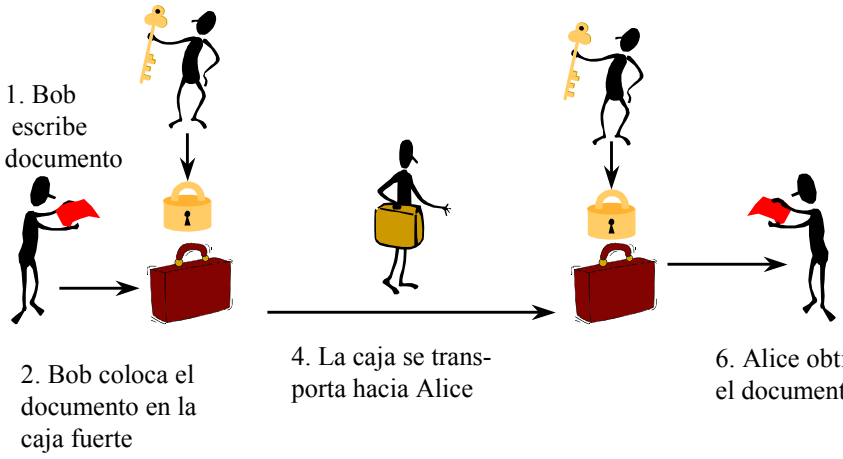


Lámina 51 Dr. Roberto Gómez C.

Clasificación métodos encripción simetricos

- Encripción en flujo

- Encripción en bloques

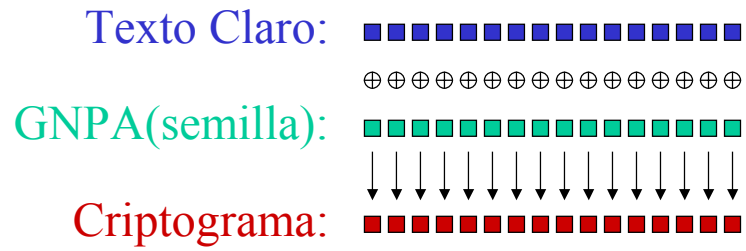
Lámina 52 Dr. Roberto Gómez C.

Encriptado en flujo

- En inglés: stream ciphers.
- Usa la llave como semilla de un generador de números pseudo-aleatorio.
- El resultado del generador es una secuencia de bits.
- La secuencia se suma módulo 2 con el texto claro (emisión) o con el criptograma (recepción)

Lámina 53 Dr. Roberto Gómez C.

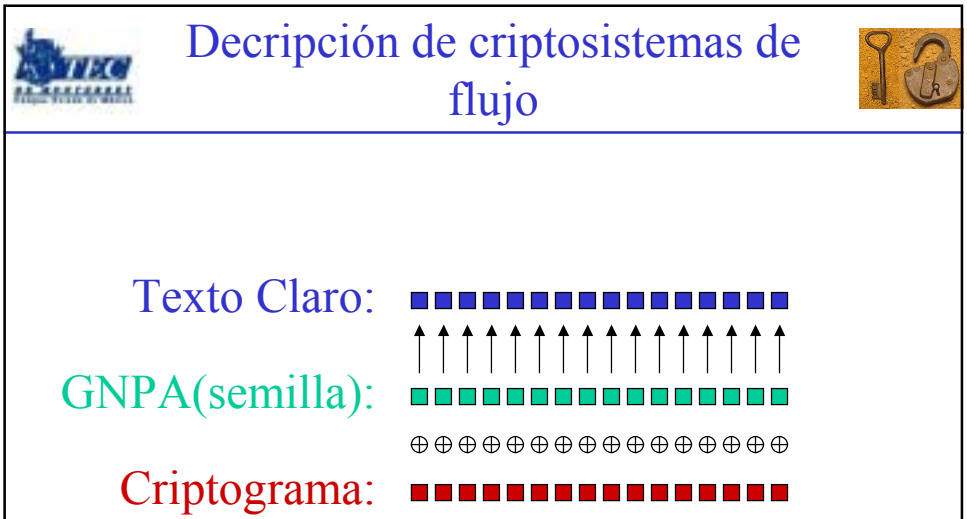
Encripción de criptosistemas de flujo



GNPA: Generador Números Pseudo-Aleatorios

Lámina 54 Dr. Roberto Gómez C.

Decripción de criptosistemas de flujo



GNPA: Generador Números Pseudo-Aleatorios

Lámina 55 Dr. Roberto Gómez C.

Ejemplo envío/recepción

Mensaje a enviar: HOLA
HOLA = 10010001000101100110010011111

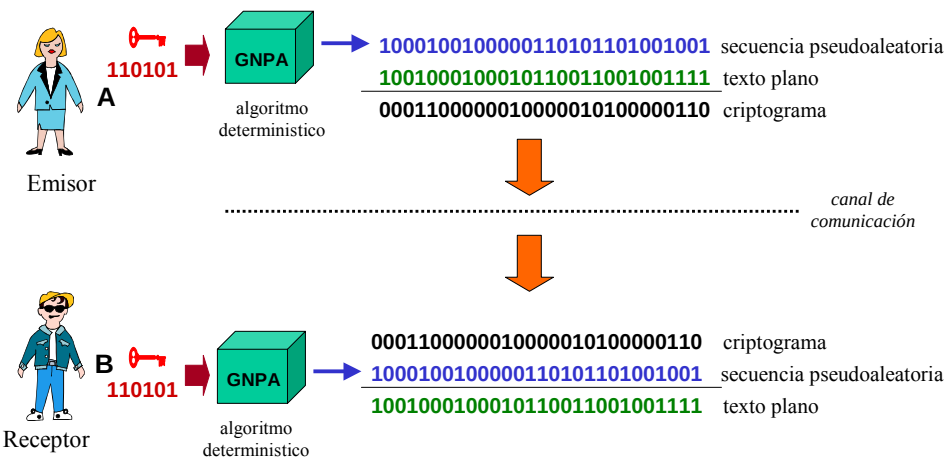


Lámina 56 Dr. Roberto Gómez C.

Generadores pseudoaleatorios

- Son algoritmos determinísticos que a partir de una llave corta (128 bits), conocida por emisor y receptor, generan simultáneamente una determinada secuencia de la longitud deseada.
- Estas secuencias nunca podrán ser autenticas secuencias aleatorias
- Son secuencias periódicas que deben ser lo más semejantes a una secuencia aleatoria
  - Período
  - Distribución unos y ceros
  - Imprevisibilidad
  - Facilidad implementación

Lámina 57 Dr. Roberto Gómez C.

Métodos generación secuencias pseudoaleatorias

- Generadores basados en congruencias lineales
- Registros de desplazamiento realimentados
- Registros de desplazamiento realimentados no linealmente (NLFSR)
- Registros de desplazamientos realimentados linealmente (LFSR)

Lámina 58 Dr. Roberto Gómez C.

Feedback Shift Registers

- Usados en criptología y teoría de códigos
- Basados en registros de corrimiento, que han servido a la criptología militar.
- Están constituidos de dos partes:
  - registro de corrimiento: secuencia de bits
  - función de retroalimentación
- Cuando se necesita un bit, todos los bits del registro de corrimiento son desplazados un bit a la derecha.
- El nuevo bit de la izquierda es calculado con la función de retroalimentación.

Lámina 59 Dr. Roberto Gómez C.

Esquema general Feedback Shift Registers

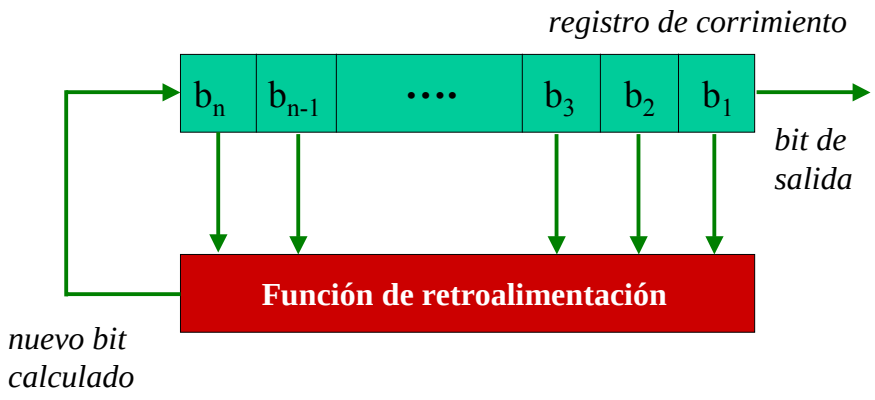


Lámina 60 Dr. Roberto Gómez C.

Registros de desplazamientos realimentados linealmente

- LFSR: Linear Feedback Shift Register
- El más simple tipo de FSR es el linear feedback shift register LSFR.
- La función de retroalimentación es un XOR de algunos bits en el registro.
  - el conjunto de estos bits se le denomida tap register (secuencia de entrada)

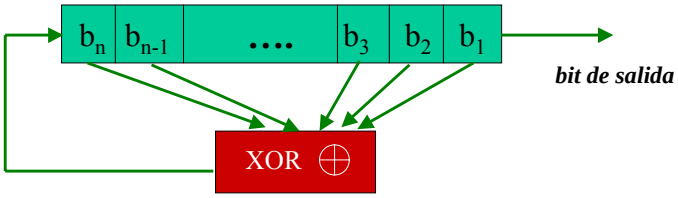
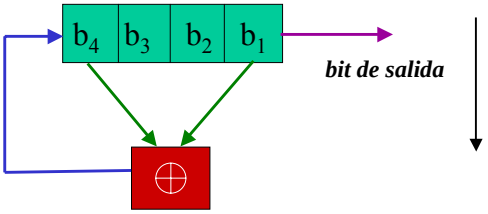


Lámina 61 Dr. Roberto Gómez C.

Ejemplo LSFR

- LFSR con bits de secuencia de entrada: b_4 b_1
- LFSR es inicializado con el valor 1111



1111	1001
0111	1001
1011	0100
0101	0010
1010	0001
1101	1000
0110	1100
0011	1110

- La secuencia de salida es: **1 1 1 1 0 1 0 1 1 0 0 1 0 0 0 ...**

Lámina 62 Dr. Roberto Gómez C.

El generador RC4

- RC4 es un criptograma de llave de tamaño variable desarrollado en 1987 por Ron Rivest para la RSA.
- Durante siete años su implementación fue privada.
- En septiembre 1994, alguien lo puso en la lista de correo Cypherpunks anonimamente.
- Lectores con copias legales de RC4 confirmaron su compatibilidad.
- RSA intento *poner de nuevo al genio en la botella*, pero fue muy tarde.

Lámina 63 Dr. Roberto Gómez C.

Código RC4

Inicialización

```
S[0..255] = 0,1,…,255
K[0..255] = Key,Key,Key,…
for i = 0 to 255
    j = (j + S[i] + K[i]) mod 256
    swap S[i] and S[j]
```

Lámina 64 Dr. Roberto Gómez C.

Código RC4

Iteración (produciendo un byte al azar)

i = (i + 1) mod 256

j = (j + S[i]) mod 256

swap S[i] and S[j]

t = (S[i] + S[j]) mod 256

Output S[t]

Lámina 65 Dr. Roberto Gómez C.

Otros generadores pseudo-aleatorios

- El generador Blum-Blum-Shub
- Algoritmo ANSI X9.17
- FIPS 186
- Algoritmo Micali-Schnorr

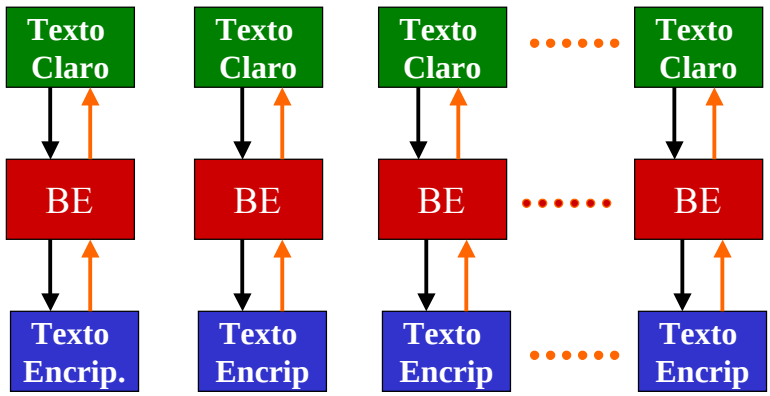
Lámina 66 Dr. Roberto Gómez C.

Métodos de encripción en bloque

- Se encripta el mensaje original agrupando los símbolos en grupos (bloques) de dos o más elementos
- Modos operación de encripción en bloque:
  - ECB: Electronic Code Book
  - CBC: Cipher Block Chaining

Lámina 67 Dr. Roberto Gómez C.

Esquema ECB de encripción / decripción en bloque



ECB: Electronic Code Book

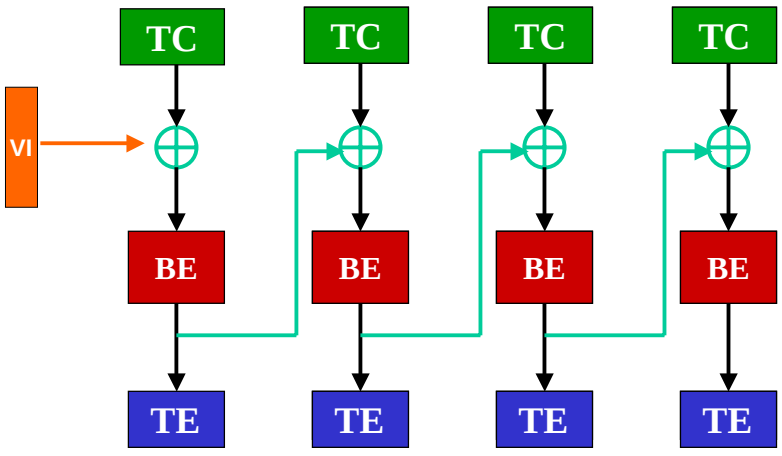
Lámina 68 Dr. Roberto Gómez C.

Problemas de ECB

- Bloques identicos me dan salidas idénticas
- Se pueden encontrar patrones en los datos por parte de un observador externo
- Solución:
  - "barajear" los datos antes de que entren al bloque de encripción (BC)

Lámina 69 Dr. Roberto Gómez C.

Cipher Block Chaining (CBC) Encripción



VI: Vector Inicialización aleatorio TC: Texto Claro TE: Texto Encriptado

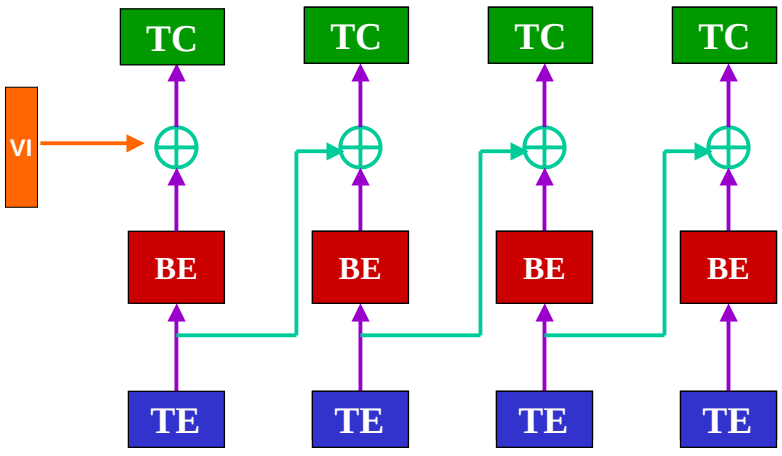
Lámina 70 Dr. Roberto Gómez C.

Comentarios sobre CBC

- Solución problema de bloques iguales me da salidas iguales
- Como decriptar:
  - se invierten las flechas
- Desventaja:
  - difícil si se tiene que encriptar/decriptar toda la información
  - no es posible decriptar solo una parte

Lámina 71 Dr. Roberto Gómez C.

Cipher Block Chaining (CBC) Decripción



VI: Vector Inicialización aleatorio TC: Texto Claro TE: Texto Encriptado

Lámina 72 Dr. Roberto Gómez C.

¿Cómo construir un block cipher?

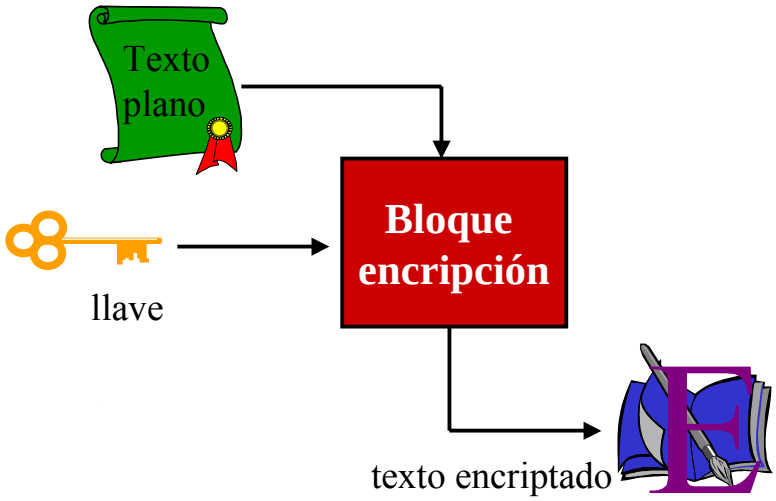


Lámina 73 Dr. Roberto Gómez C.

Los criptosistemas de Feistel

- Criptosistemas en los que el bloque de datos se divide en dos mitades y en cada vuelta de encriptación se trabaja alternadamente, con una de las mitades
- Ejemplos:
  - LUCIFER
  - DES
  - LOKI
  - FEAL

Lámina 74 Dr. Roberto Gómez C.

Barajeando los datos de entrada

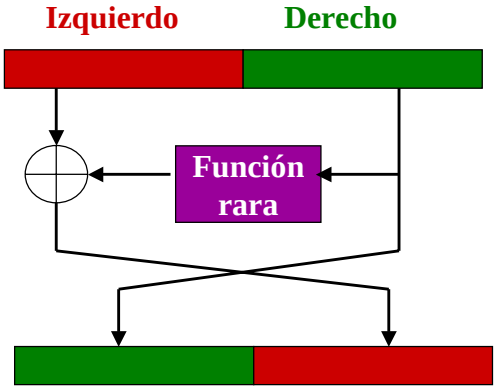


Lámina 75 Dr. Roberto Gómez C.

Repitiendo

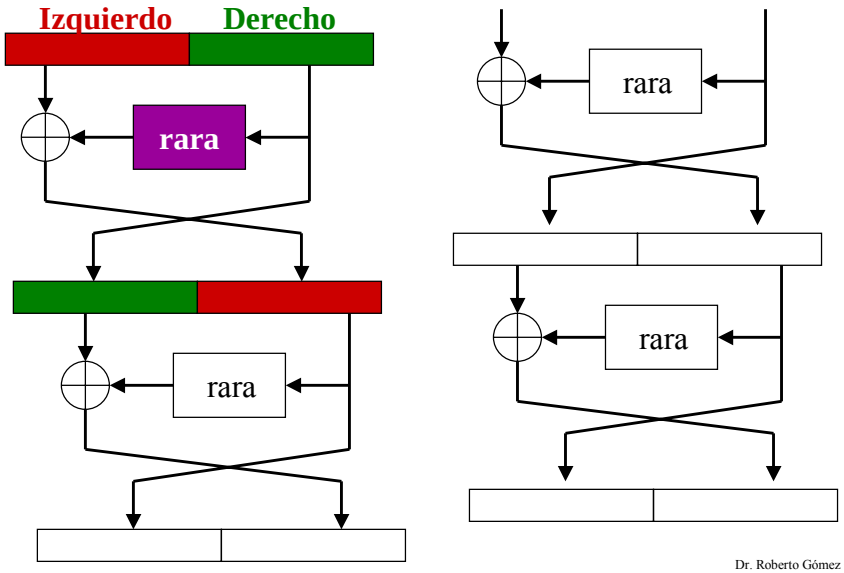


Lámina 76 Dr. Roberto Gómez C.

Comentarios

- Tipicamente los criptosistemas de Feistel son iterados unas 16 veces
- Otra opción es que la función rara cambie en cada iteración:
  - usar sub-llaves diferentes en cada turno
- Cada iteración debil puede construir un Fiestel más fuerte

Lámina 77 Dr. Roberto Gómez C.

DES: ejemplo de encripción simétrica

- Data Encryption Standard
- Nació en 1974 en IBM
- Propuesto a raíz de una petición de la NIST (National Institute of Standards and Technology, USA) en 1972 y 1974.
- Inspirado de sistema LUCIFER de IBM.
- Aprobado y modificado por la NSA (National Security Agency, USA)
- NSA impuso la longitud de la llave

Lámina 78 Dr. Roberto Gómez C.

Características de DES

- Algoritmo cifrado en bloque y simétrico
- Longitud bloque: 64 bits
- Longitud llave: 56 bits, por lo que existen 2^{56} = 7.2 x 10^{16} llaves diferentes
- Norma exige que DES se implemente mediante un circuito integrado
- En 1981 ANSI adopto el DES con el nombre de Data Encryption Algorithm
  - no exige chip y puede ser programado

Lámina 79 Dr. Roberto Gómez C.

Esquema general DES

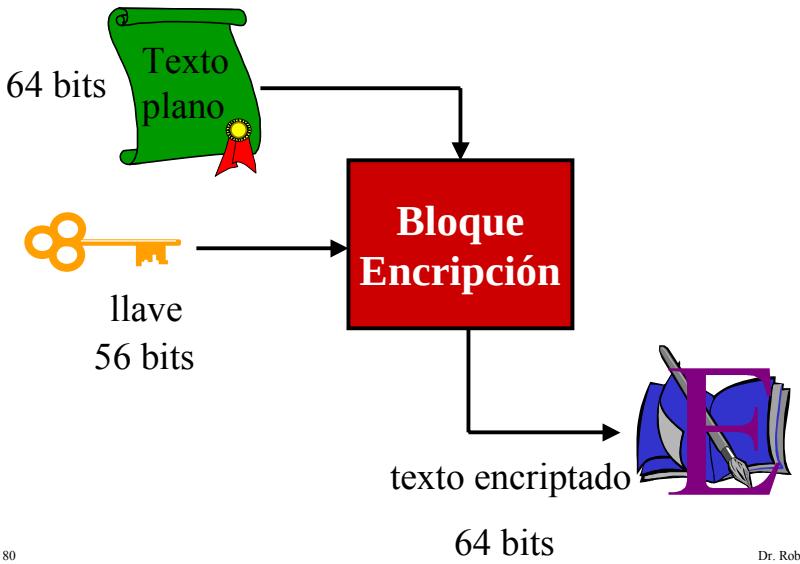


Lámina 80 Dr. Roberto Gómez C.

Las iteraciones en DES

- Se trata de 16 iteraciones tipo Feistel

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

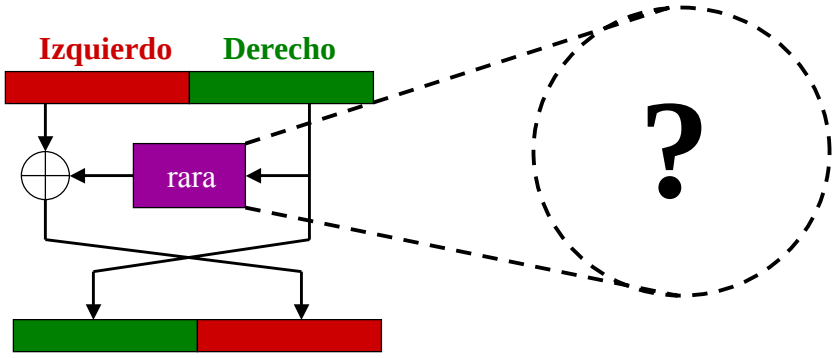


Lámina 81
Dr. Roberto Gómez C.

Esquema función rara

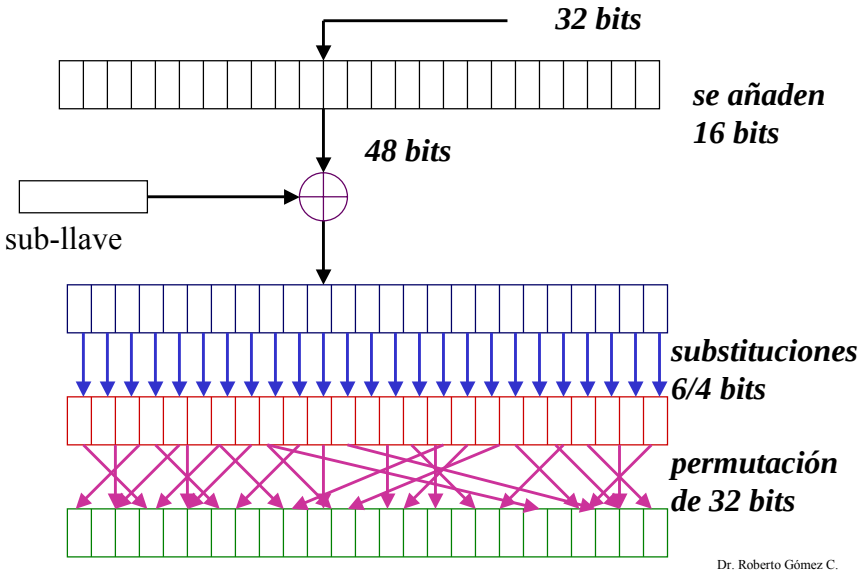


Lámina 82
Dr. Roberto Gómez C.

Esquema de una iteración en DES

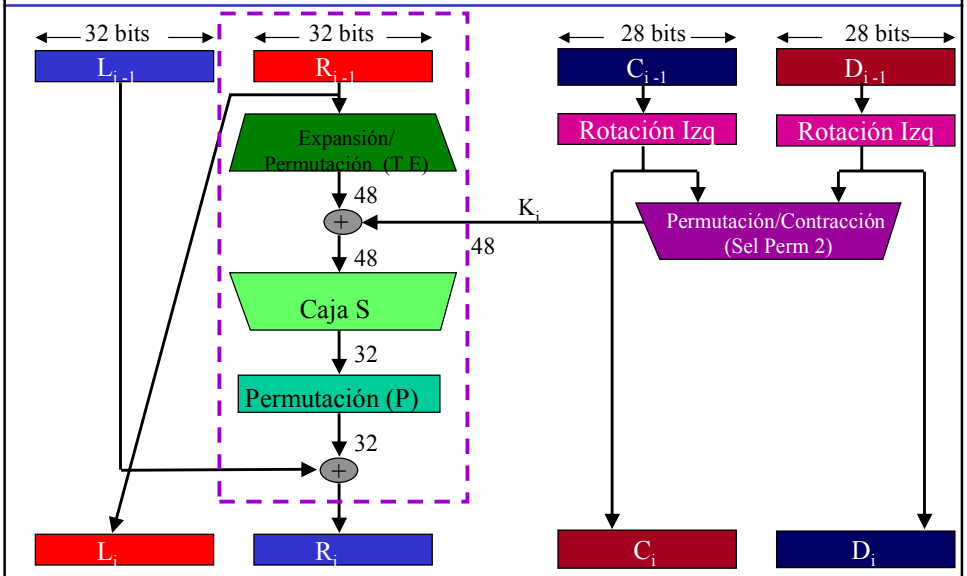


Lámina 83 Dr. Roberto Gómez C.

El proceso de decriptado

- El proceso de decriptado es en esencia el mismo que el de encriptado.
- La regla es la siguiente:
  - usar el texto cifrado como entrada a DES,
  - usar la llave K_i en orden inverso.

Lámina 84 Dr. Roberto Gómez C.

Encripción/decripción en DES

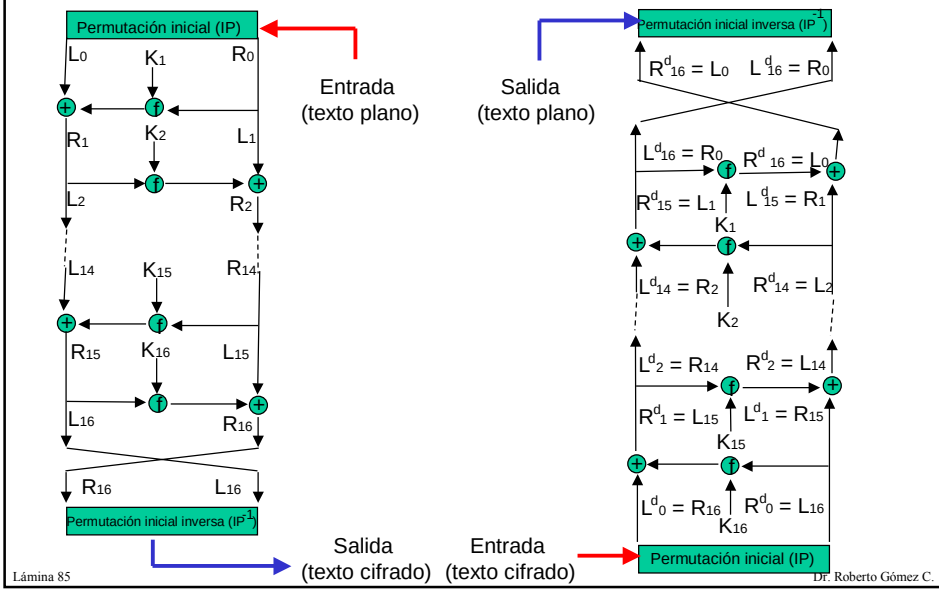


Lámina 85
Dr. Roberto Gómez C.

¿Qué es MiniDES?

- Versión reducida de DES
- Objetivo académico
- Palabra entrada

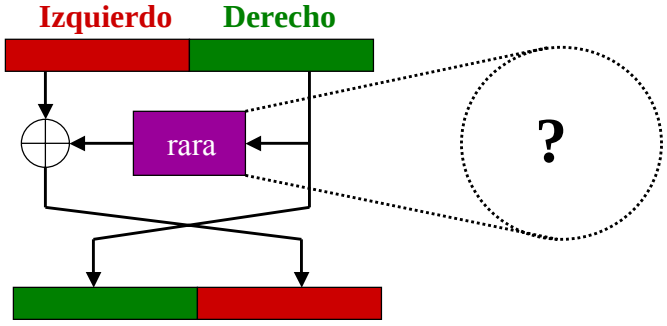


Lámina 86
Dr. Roberto Gómez C.

Esquema de una interación en MiniDES

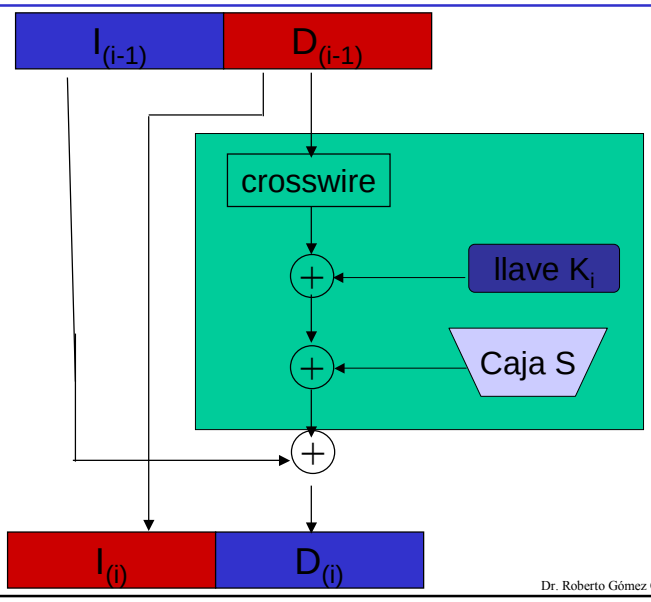
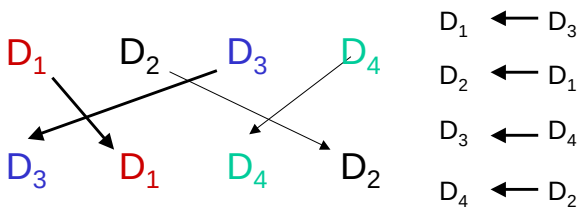


Lámina 87 Dr. Roberto Gómez C.

Pasos dentro de MiniDES

- Crosswire (intercambiar bits de la parte derecha)



- Suma binaria con la llave K_i

$$D = D \oplus Ki$$

Lámina 88 Dr. Roberto Gómez C.

Pasos dentro de MiniDES

- Suma binaria con la caja S

$$D = D \oplus S_{box}(D)$$

	00	01	10	11
00	A	0	C	8
01	5	B	3	2
10	1	9	E	4
11	7	6	F	D

columna: valor bits D_2 y D_3
renglón: valor bits D_1 y D_4

Lámina 89 Dr. Roberto Gómez C.

Pasos dentro de MiniDES

- Suma binaria e intercambio

$$D = D \oplus I$$
$$I = D$$

- Repetir lo anterior el número de llaves
- Al final intercambiar la parte izquierda con la parte derecha

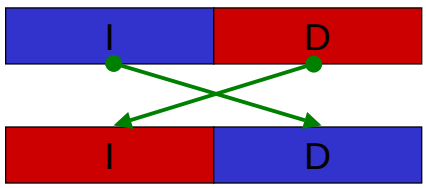


Lámina 90 Dr. Roberto Gómez C.

Ejemplo (caracteristicas)

- Tamaño palabra: 8 bits
- Palabra a codificar: $C5_{16}$
- En binario: **1100 0101**
- Tamaño llaves 4 bits
- Número de llaves: 3
  - Valor K_1: 0110
  - Valor K_2: 1100
  - Valor K_3: 0111

Lámina 91 Dr. Roberto Gómez C.

El efecto avalancha

- Una propiedad deseable de cualquier algoritmo de encriptado es que un pequeño cambio en el texto original (un bit) o en la llave produzca un cambio significante en el texto encriptado.
- DES exhibe un efecto avalancha bastante fuerte.

Lámina 92 Dr. Roberto Gómez C.

Efecto de avalancha en DES

a) Cambio en texto plano		b) Cambio en llave	
Iteración	Número de bits que difieren	Iteración	Número de bits que difieren
0	1	0	0
1	6	1	2
2	21	2	14
3	35	3	28
4	39	4	32
5	34	5	30
6	32	6	32
7	31	7	35
8	29	8	34
9	42	9	40
10	44	10	38
11	32	11	31
12	30	12	33
13	30	13	28
14	26	14	26
15	29	15	34
16	34	16	35

Lámina 93
Dr. Roberto Gómez C.

Preocupaciones sobre DES

- Llave de 56 bits = $2^{56} \sim 7.2 \times 10^{16}$ llaves posibles.
- Una máquina capaz de realizar un encriptado de DES por microsegundo necesitaría más de 1000 años para romper el cifrado.
- Con el procesamiento paralelo o dispositivos dedicados podríamos alcanzar 1 millón de encriptados por microsegundo. (Costo?????),

Lámina 94
Dr. Roberto Gómez C.

The DES Key Search Project

- Una máquina construida por Cryptography Research, Advanced Wireless Technologies, y EFF lleva a cabo una busqueda rápida de la llave de DES.
- El proyecto de *busqueda de llave de DES* desarrolló hardware y software especializado para buscar 90 billones de llaves por segundo, calculando la llave y ganando el reto RSA DES, después de una busqueda de 56 horas.
- Referencia:
  - http://www.cryptography.com/des/despictures/index.html

Lámina 95 Dr. Roberto Gómez C.

Detalles de la máquina

- Cada chip procesa dos criptogramas y contiene un vector de 256 bits que especifica cuales bytes pueden aparecer en el texto claro.
- La máquina se encuentra albergada en seis gabinetes reciclados SUN-2 y consiste de 27 tarjetas de circuitos que contienen más de 1800 chips
  - cada chip contiene 24 unidades de busqueda que independientemente, recorren un rango de llaves, filtrando aquellas que no pasan el criterio de busqueda para los criptogramas.

Lámina 96 Dr. Roberto Gómez C.

Imagenes de la máquina

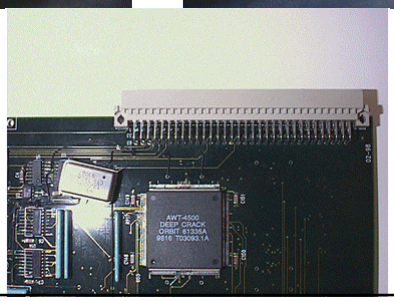


Lámina 97
Dr. Roberto Gómez C.

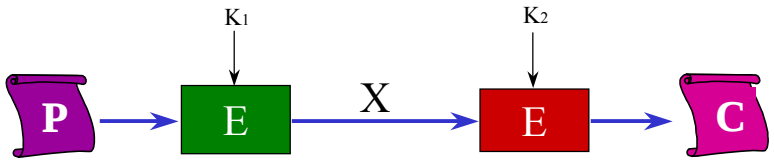
Mejoras a DES

- Debido a las vulnerabilidades que presenta DES contra ataques de fuerza bruta, se han buscado alternativas.
- Una de esta es realizar un múltiple encriptado con DES usando más de una llave.

Lámina 98
Dr. Roberto Gómez C.

Doble DES

Encriptado



Decriptado

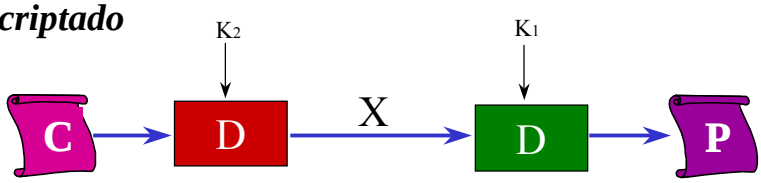
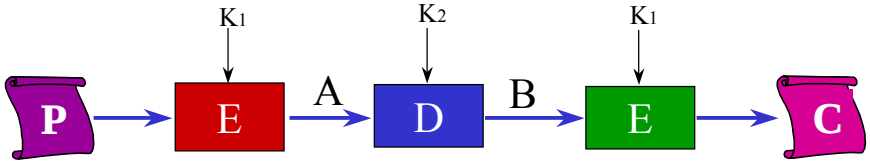


Lámina 99 Dr. Roberto Gómez C.

Triple DES

Encriptado



Decriptado

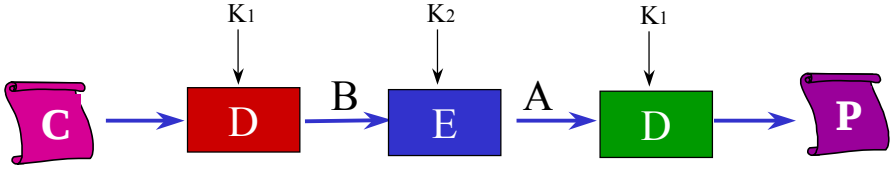


Lámina 100 Dr. Roberto Gómez C.

Substituto DES: AES

- En 1997 la NIST anuncia el substituto de DES: AES (Advanced Encryption Standard)
- Referencia: http://csrc.nist.gov/encryption/aes/
- Candidatos (al 20-abril- 2000):
  - MARS (IBM)
  - RC6 (Laboratorios RSA)
  - **Rijndael (J. Daemen y V. Rijmen) !!!! (2.10.2000)**
  - Serpent (R. Anderson, E.Biham, L.Knudsen)
  - Twofish (B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson)

Lámina 101 Dr. Roberto Gómez C.

Características

- Rijndael es una iteración de bloque cifrado con un tamaño de bloque y llave variable.
- La llave puede tener un tamaño de 128,192 o 256.
- No usa otros componentes criptograficos.
- No tiene partes obscuras y cosas dificiles de entender entre operaciones aritméticas.
- No deja espacio suficiente para esconder un trapdoor.
- Modo encripción en bloque ECB.

Lámina 102 Dr. Roberto Gómez C.

AES vs DES

- DES:
  - la iteración de tranformación esta basada en Feistel (en cada iteración se aplica Feistel)
  - el mismo algoritmo sirve para encriptar como para decriptar, invirtiendo el orden de las subllaves que se obtienen a partir de la llave de encripción
- AES
  - la iteración de tranformación esta compuesta por capas
  - capas formadas por funciones reversibles
  - para descifrar basta con aplicar las funciones inversas de cada capa, en el orden contrario

Lámina 103 Dr. Roberto Gómez C.

Funcionamiento Rijndael

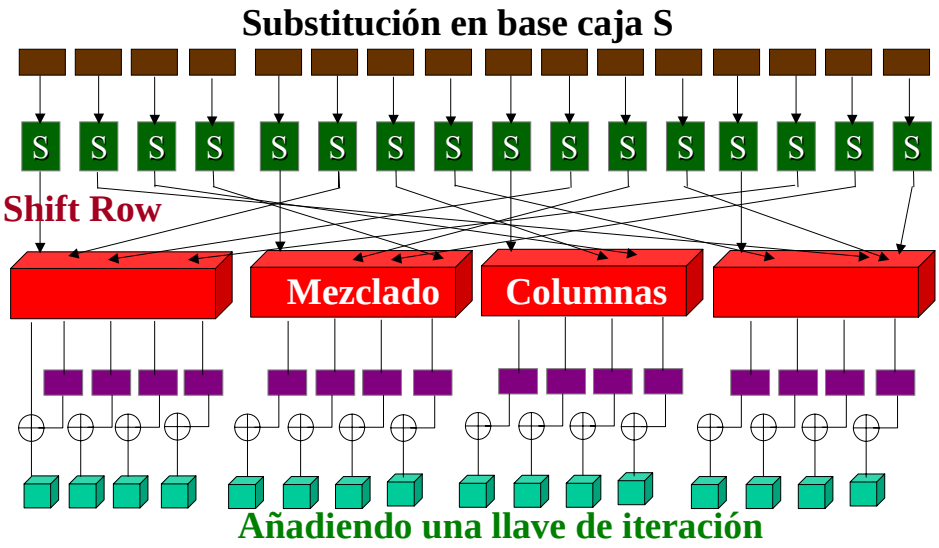


Lámina 104 Dr. Roberto Gómez C.

Usando encripción en bloques para encripción en flujo

- Permite usar un esquema de encripción en bloque para una encripción en flujo.
- Con una encripción en flujo se elimina el requisito de añadir bits para completar el tamaño del bloque
- Permite que la encripción opere en tiempo real.
  - si se transmite un caracter cada caracter puede ser encriptado antes de su transmisión
- Dos formas de hacerlo:
  - CFB: Cipher Feedback Mode
  - OFB: Output Feedback Mode

Lámina 105 Dr. Roberto Gómez C.

Encripción en modo CFB

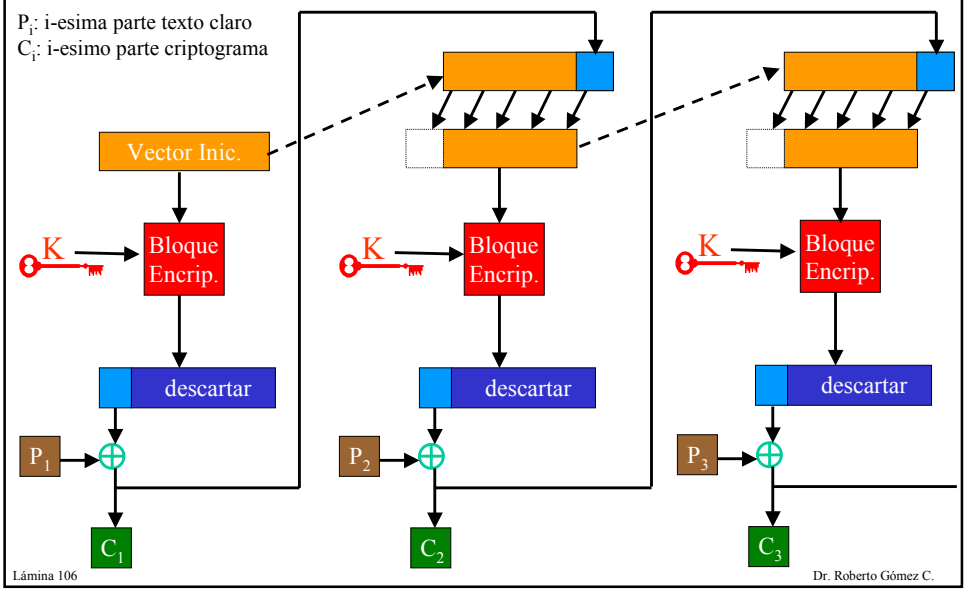
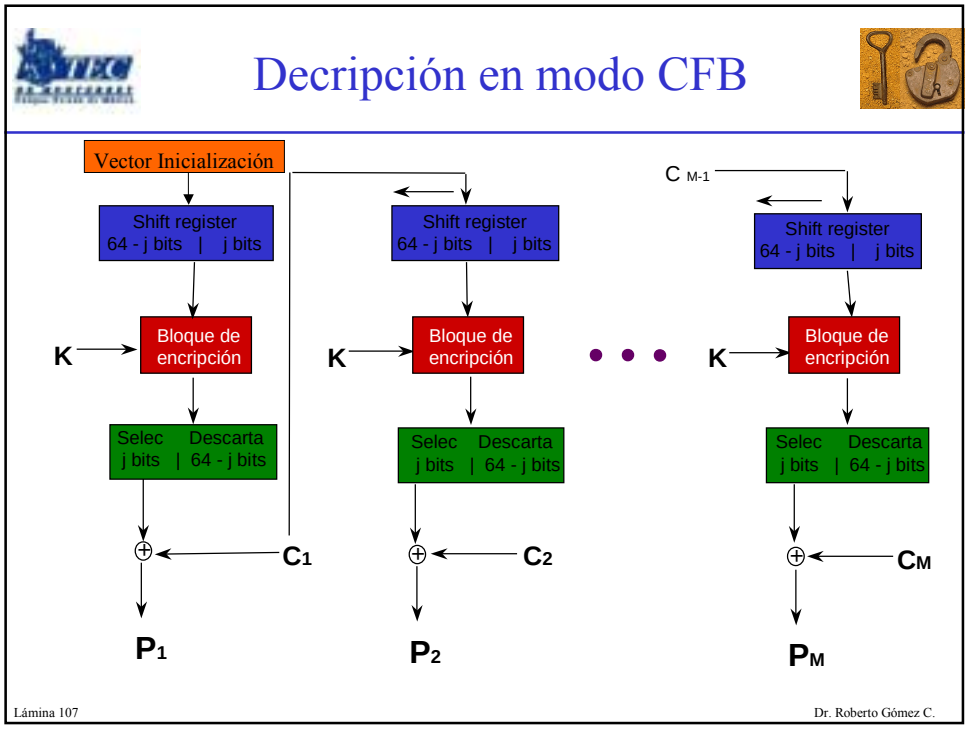
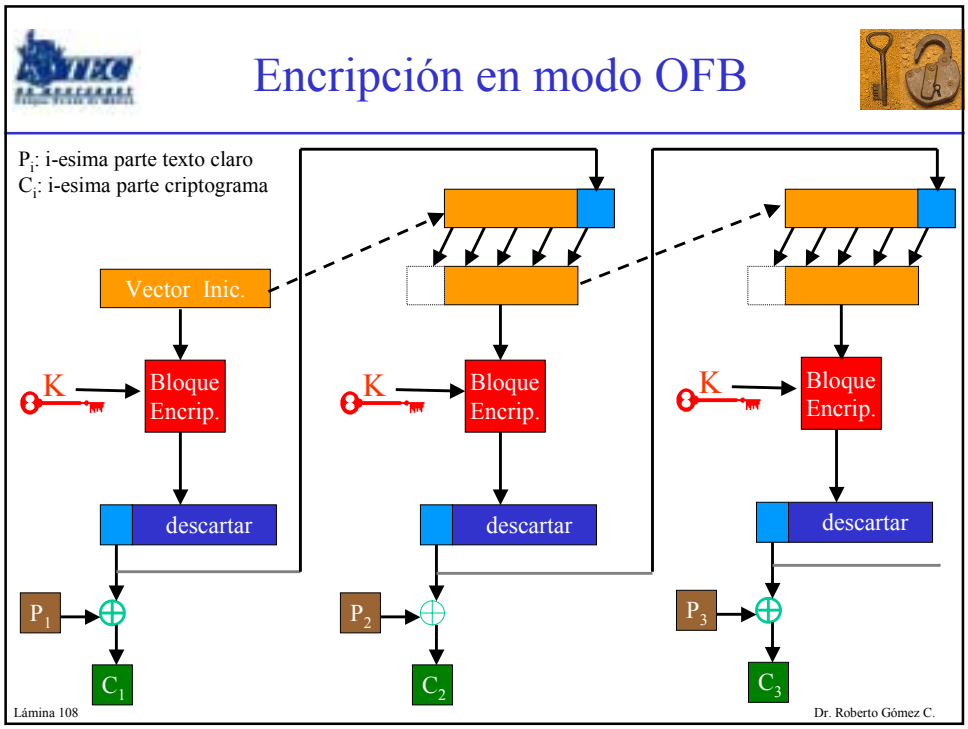


Lámina 106 Dr. Roberto Gómez C.


Decripción en modo CFB
Vector Inicialización
Shift register
64 - j bits | j bits
Bloque de encripción
K
Selec j bits | Descarta 64 - j bits
C1
P1
C2
P2
C M-1
CM
PM
Lámina 107
Dr. Roberto Gómez C.


Encripción en modo OFB
Pi: i-esima parte texto claro
Ci: i-esima parte criptograma
Vector Inic.
K
Bloque Encrip.
descartar
P1
C1
P2
C2
P3
C3
Lámina 108
Dr. Roberto Gómez C.

Decripción en modo OFB

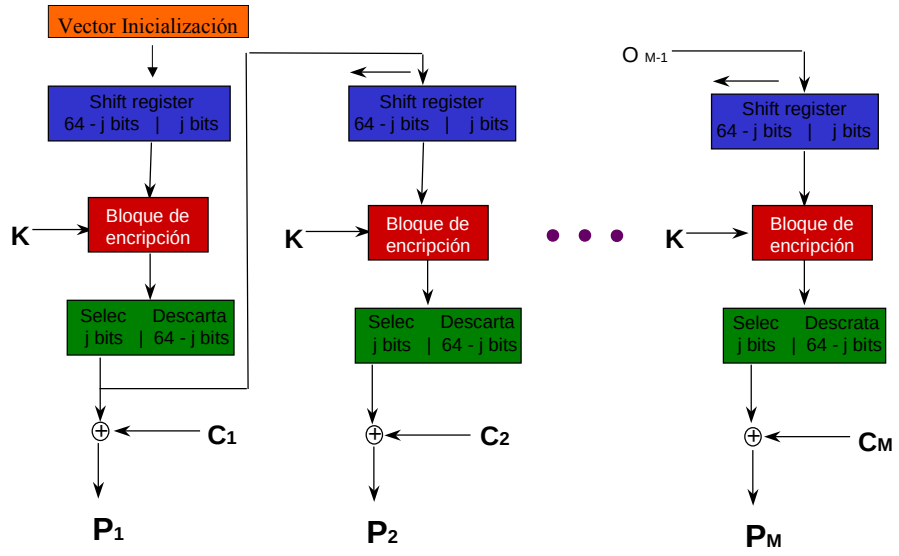


Lámina 109 Dr. Roberto Gómez C.

Otros algoritmos llave simétrica

- Twofish
- Blowfish
- IDEA
- RC2, RC4 y RC5
- NewDES
- Feal
- SKIPJACK
- MMB
- GOST
- CRAB 342
- CAST
- SAFER
- 3-WAY
- FEAL
- REDOC
- LOKI
- MADRYGA
- Lucifer
- Khufu and Khafre
- CA-1.1

Lámina 110 Dr. Roberto Gómez C.

Desventajas llave secreta

- Distribución de llaves
  - usuarios tienen que seleccionar llave en secreto antes de empezar a comunicarse
- Manejo de llaves
  - red de n usuarios, cada pareja debe tener su llave secreta particular, i.e. n(n-1)/2 llaves
- Sin firma digital
  - no hay posibilidad , en general, de firmar digitalmente los mensajes

Lámina 111 Dr. Roberto Gómez C.

Criptosistemas de llave pública

Características y ejemplos

Lámina 112 Dr. Roberto Gómez C.

Background

- Concepto de llave pública fue inventado por Whitfield Diffie y Martin Hellman e independientemente por Ralph Merkle.
- Contribución fue que las llaves pueden presentarse en pares.
- Concepto presentado en 1976 por Diffie y Hellman.
- Desde 1976 varios algoritmos han sido propuestos, muchos de estos son considerados seguros, pero son impracticos.
- Algunos solo son buenos para distribución de llaves.

Lámina 113 Dr. Roberto Gómez C.

Background

- Otros solo son buenos para encripción.
- Algunos más solo son buenos para firmas digitales.
- Solo tres algoritmos son buenos para encripción y firmas digitales:
  - RSA,
  - ElGamal
  - Rabin.
- Los tres algoritmos son más lentos que los algoritmos simétricos.

Lámina 114 Dr. Roberto Gómez C.

Criptograma llave pública (asimétrico)

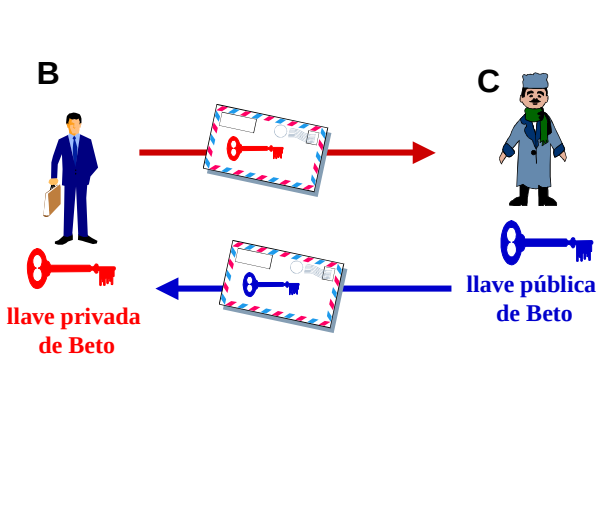


Lámina 115
Dr. Roberto Gómez C.

Encripción llave pública

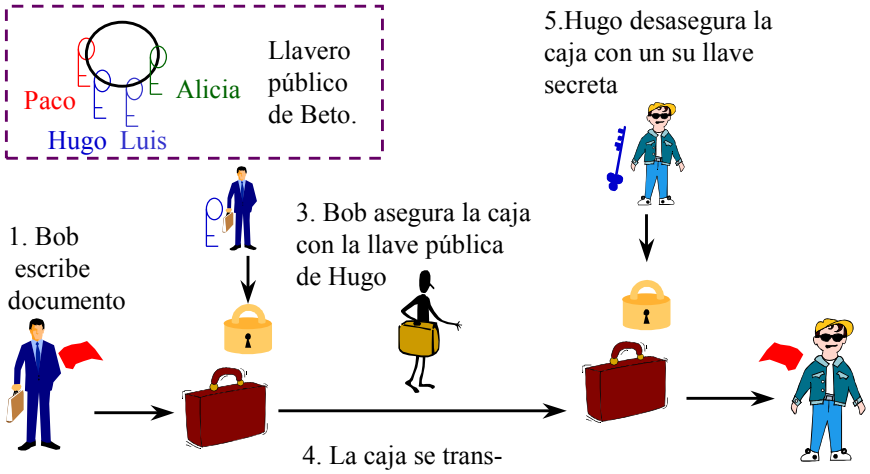


Lámina 116
Dr. Roberto Gómez C.

Criptosistema Diffie Hellman

Criptosistema intercambio llaves

Lámina 117 Dr. Roberto Gómez C.

Diffie-Hellman

- Primer algoritmo de llave pública (1976)
  - Williamson del CESG[1] UK, publica un esquema identico unos meses antes en documento clasificado
  - asegura que descubrió dicho algoritmo varios años antes
- Varios productos comerciales utilizan este técnica de intercambio de llaves.
- Propósito del algoritmo
  - permitir que dos usuarios intercambien una llave de forma segura
  - algoritmo limitado al intercambio de llaves
- Basado dificultad para calcular logaritmos discretos

Lámina 118 1: Communications-Electronic Security Group Dr. Roberto Gómez C.

Algoritmo de Diffie-Hellman

1. Los dos usuarios A y B seleccionan públicamente un grupo multiplicativo finito, G, de orden n y un elemento de G
2. A genera un número aleatorio X_a, calcula Y_a en G y transmite este elemento a B
3. B genera un número aleatorio X_b, calcula Y_b en G y transmite este elemento a A
4. A recibe Y_b y calcula $(Y_b)^{Xa}$ en G
5. B recibe Y_a y calcula $(Y_a)^{Xb}$ en G

Lámina 119 Dr. Roberto Gómez C.

Esquema Diffie Hellman

Elementos globales públicos: q (numero primo) y α $(\alpha < q)$

Selecciona val. priv: X_A $(X_A < q)$

Calcula valor pub: $Y_A = \alpha^{X_A} \bmod q$

Y_A

Selecciona val. priv: X_B $(X_B < q)$

Calcula valor pub: $Y_B = \alpha^{X_B} \bmod q$

Y_B

Generando llave secreta A

$K = (Y_B)^{X_A} \bmod q$

Generando llave secreta B

$K = (Y_A)^{X_B} \bmod q$

Lámina 120 Dr. Roberto Gómez C.

Ejemplo Diffie Hellman

Elementos globales públicos: $q = 53 \quad \alpha = 2 \; (2 < 53)$

A

La llave de A y B es 21

B

Selecciona val. priv: $X_A = 29 \; (29 < 53)$

Calcula valor pub: $Y_A = 2^{29} \bmod 53$

$= 45 \mod 53$

$Y_A \; (45)$

Selecciona val. priv: $X_B = 19 \quad (19 < 53)$

Calcula valor pub: $Y_B = 2^{19} \bmod 53$

$= 12 \bmod 53$

$Y_B \; (12)$

Generando llave secreta A

$K = 12^{29} \bmod 53 = 21 \bmod 53$

Generando llave secreta B

$K = 45^{19} \bmod 53 = 21 \bmod 53$

Lámina 121 Dr. Roberto Gómez C.

Comentarios ejemplo

- La clave privada o la información secreta que comparten ahora A y B es 21
- Un escucha, S, conoce del protocolo anterior:
  - Z_{53}^* , 2, 45 y 12
  - no puede conocer que la información secreta compartida por A y B es 21

Lámina 122 Dr. Roberto Gómez C.

Aritmética Modular

- Utiliza enteros no negativos
- Realiza operaciones aritméticas ordinarias (suma, multiplicación).
- Reemplaza su resultado con el residuo cuando se divide entre n.
- El resultado es modulo n o *mod n*.

Lámina 123 Dr. Roberto Gómez C.

Ejemplo suma modular

- 5 + 5 = 10 mod 10 = 0
- 3 + 9 = 12 mod 10 = 2
- 2 + 2 = 4 mod 10 = 4
- 9 + 9 = 18 mod 10 = 8

Lámina 124 Dr. Roberto Gómez C.

Tabla suma modular

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Lámina 125 Dr. Roberto Gómez C.

Encripción usando suma modular

- Suma modulo 10 puede usarse como esquema de encripción de dígitos.
- Encripción:
  digito + <constante> mod 10
- Se mapea cada dígito decimal a uno diferente de tal forma que es reversible.
- La constante es la llave secreta
- Decripción:
  digito - <constante> mod 10
  si el resultado es menor a cero => sumar 10

Lámina 126 Dr. Roberto Gómez C.

Ejemplo encripción suma modular

- Llave secreta: 5
- Encripción:
  - 7 + 5 = 12 mod 10 = 2
  - 8 + 5 = 13 mod 10 = 3
  - 3 + 5 = 8 mod 10 = 8
- Decripción:
  - 2 - 5 = -3 + 10 = 7
  - 3 - 5 = -2 + 10 = 8
  - 8 - 5 = 3

Lámina 127 Dr. Roberto Gómez C.

Encripción con inversa aditiva de x

- Aritmética regular:
  - substraer x puede hacerse sumando -x
- Inversa aditiva de x
  - número que se le tiene que semar a x para obtener 0
- Por ejemplo:
  - inversa aditiva de 4 es 6
  - artimética mod 10: 4 + 6 = 10 mod 10 = 0
- Si la llave secreta es 4:
  - para encriptar se añade 4 mod 10
  - para decriptar se añade 6 mod 10

Lámina 128 Dr. Roberto Gómez C.

Ejemplo encripción inversa aditiva

- Llave encripción: 4
- Encripción:
  - 7 + 4 mod 10 = 11 mod 10 = 1
  - 8 + 4 mod 10 = 12 mod 10 = 2
  - 3 + 4 mod 10 = 7 mod 10 = 7
- Decripción:
  - 1 + 6 mod 10 = 7 mod 10 = 7
  - 2 + 6 mod 10 = 8 mod 10 = 8
  - 7 + 6 mod 10 = 13 mod 10 = 3

Llave encripción: 4

Llave decripción: 6

¿Es posible decriptar si solo se conoce la llave de encripción?

Lámina 129 Dr. Roberto Gómez C.

Encripción con multiplicación modular

- Multiplicación modular: mismo principio que la suma:
  - 7 * 4 mod 10 = 8
  - 3 * 9 mod 10 = 7
  - 2 * 2 mod 10 = 4
  - 9 * 9 mod 10 = 1
- Diferencia:
  - no es posible aplicar el mismo principio de encripción que en la suma

Lámina 130 Dr. Roberto Gómez C.

Tabla multiplicación modular

*	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Lámina 131 Dr. Roberto Gómez C.

¿Cómo decriptar?

- Inverso multiplicativo
  - aritmética normal: inverso de x es: $x^{-1} = 1/x$
  - número por el cual se debe multiplicar x para obtener el valor de 1: *número fraccionario*
  - en aritmética modular solo hay enteros
- Entonces:
  - los números {1,3,7,9} tiene inversos multiplicativos, por lo que son los que se van a usar como llaves

Lámina 132 Dr. Roberto Gómez C.

¿Por qué no usar el 5 y el 8?

Encriptando con 5

- 1 * 5 mod 10 = 5
- 2 * 5 mod 10 = 0
- 3 * 5 mod 10 = 5
- 4 * 5 mod 10 = 0
- 5 * 5 mod 10 = 5
- 6 * 5 mod 10 = 0
- 7 * 5 mod 10 = 5
- 8 * 5 mod 10 = 0
- 9 * 5 mod 10 = 5

Encriptando con 8

- 1 * 8 mod 10 = 8
- 2 * 8 mod 10 = 6
- 3 * 8 mod 10 = 4
- 4 * 8 mod 10 = 2
- 5 * 8 mod 10 = 0
- 6 * 8 mod 10 = 8
- 7 * 8 mod 10 = 6
- 8 * 8 mod 10 = 4
- 9 * 8 mod 10 = 2

Lámina 133 Dr. Roberto Gómez C.

¿Y el resto de los números?

*	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

- Se debe escoger con cuidado el multiplicador
- La llave puede ser 1,3,7 o 9 ya que realizan substitución uno a uno de los dígitos
- Problema: **¿Cómo decriptar?**

Lámina 134 Dr. Roberto Gómez C.

Ejemplos inversos multiplicativos

- Ejemplo 1:
  - 7 es el inverso multiplicativo de 3

    3 x 7 mod 10 = 21 mod 10 = 1
  - Entonces: encripción con 3 y decripción con 7

Encripción	Decripción
7 * 3 mod 10 = 1	1 * 7 mod 10 = 7
8 * 3 mod 10 = 4	4 * 7 mod 10 = 8
3 * 3 mod 10 = 9	9 * 7 mod 10 = 3

Lámina 135 Dr. Roberto Gómez C.

Otro ejemplo

- Ejemplo 2:
  - 9 es su propio inverso multiplicativo

    9 x 9 mod 10 = 81 mod 10 = 1
  - Entonces: encripción con 9 y decripción con 9

Encripción	Decripción
7 * 9 mod 10 = 3	3 * 9 mod 10 = 7
8 * 9 mod 10 = 2	2 * 9 mod 10 = 8
3 * 9 mod 10 = 7	7 * 9 mod 10 = 3

Lámina 136 Dr. Roberto Gómez C.

En general

- Criptograma:
  - se puede modificar la información a través de un algoritmo y revertir el proceso para obtener la información original.
- Una multiplicación mod n por un número x es un criptograma ya que:
  - se puede multiplicar por x para encriptar
  - se puede multiplicar por x^{-1} para decriptar

Lámina 137 Dr. Roberto Gómez C.

Primera observación

- No es tan simple encontar un inverso multiplicativo mod n, especialmente si n es muy grande,
- Si n = 100 digitos
  - no es lógico realizar una busqueda de fuerza bruta para encontrar un inverso multiplicativo
- Algoritmo ecludiano (mcd: max. com. div)
  - permite encontrar inversos mod n, dado x y n encuentra y tal que:

    x * y mod n = 1 (si existe)

Lámina 138 Dr. Roberto Gómez C.

Segunda observación

- ¿Por qué los números {1,3,7,9} son los únicos que tienen inversos multiplicativos?
  - respuesta: son relativamente primos a 10.
- Relativamente primos a 10:
  - significa que no comparte ningún factor común aparte de 1
  - el entero más largo que divide 9 y 10 es 1
  - el entero más largo que divide 7 y 10 es 1
  - el entero más largo que divide 3 y 10 es 1
  - el entero más largo que divide 1 y 10 es 1

Lámina 139 Dr. Roberto Gómez C.

- En constraste 6, 2, 4, 5 y 8 son primos en 10 ya que:
  - 2 divide a 6 y 10, i.e. mcd(6,10) = 2
  - 2 divide a 2 y 10, i.e. mcd(6,10) = 2
  - 2 divide a 4 y 10, i.e. mcd(6,10) = 2
  - 5 divide a 5 y 10, i.e. mcd(6,10) = 2
  - 2 divide a 8 y 10, i.e. mcd(6,10) = 2
- Conclusión
  - cuando se trabaja con aritmetica mod n, todos los números relativos primos a n tienen multiplicativos inversos y los otros números no.

$$\exists \text{ inverso } a^{-1} \text{ en mod n} \quad \textit{ssi} \quad \text{mcd } (a, n) = 1$$

Lámina 140 Dr. Roberto Gómez C.

El mcd y la criptografía

- En criptografía muchas veces nos interesará encontrar el máximo común denominador mcd entre dos números a y b.
- Para la existencia de inversos en un cuerpo n, la base a y el módulo n deberán ser primos entre sí
  - es decir mcd (a, n) = 1
- Algoritmo de Euclides
  - a) Si x divide a a y b $\Rightarrow$ $a = x * a'$ y $b = x * b'$
  - b) Por lo tanto: $a - k * b = x * a' - k * x * b'$
    $a - k * b = x (a' - k * b')$
  - c) Entonces se concluye que x divide a $(a - k * b)$

Lámina 141 Dr. Roberto Gómez C.

La función totient de Euler

- ¿Cuantos números a n pueden ser relativamente primos a n?
  - Respuesta: función totient $\Phi(n)$
  - to = total tient = quotient (cociente)
- Si n es primo:
  $\Phi(n) = n - 1$
  existen n-1 números relativamente primos a n
- Si n es un producto de dos números primos (p y q) $\Phi(n) = \Phi(pq) = \Phi(p) \times \Phi(q)$
  $\Phi(n) = (p-1)(q-1)$
  existen (p-1)(q-1) números relativamente primos a n

n	Φ(n)
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

Lámina 142 Dr. Roberto Gómez C.

Teorema de Euler

Dice que si mcd (a,n) = 1 $\Rightarrow$ $a^{\phi(n)} \bmod n = 1$

Ahora igualamos $a*x \bmod n = 1$ y $a^{\phi(n)} \bmod n = 1$

$\therefore \quad a^{\phi(n)} * a^{-1} \bmod n = x \bmod n$

$\therefore \quad x = a^{\phi(n)-1} \bmod n$

El valor x será el inverso de a en el cuerpo n

Nota: Observe que se ha ***dividido*** por a en el cálculo anterior. Esto se puede hacer porque mcd (a, n) = 1 y por lo tanto hay un único valor inverso en el cuerpo n que lo permite.

Lámina 143 Dr. Roberto Gómez C.

Criptosistema RSA

- Primera realización del modelo de Diffie-Hellman
- Realizado por Rivest, Shamir y Adleman en 1977 y publicado por primero vez en 1978
  - se dice que un método casi idéntico fue creado por Clifford Cocks en1973
- Basado en una operaciones con números primos
- Podría considerarse un criptosistema de bloque
  - texto claro y criptograma son enteros entre 0 y n-1 para algún valor de n

Lámina 144 Dr. Roberto Gómez C.

El algoritmo RSA

- Dos etapas
  - la creación de las llaves
  - la encripción/decripción del mensaje
- Algoritmo general

1. Cada usuario elige un grupo $n = p*q$ (pueden ser distintos).
2. Los valores p y q no se hacen públicos.
3. Cada usuario calcula $\phi(n) = (p-1)(q-1)$.
4. Cada usuario elige una clave pública e que sea parte del cuerpo n y que cumpla: $mcd [e, \phi(n)] = 1$.
5. Cada usuario calcula la clave privada $d = inv [e,\phi(n)]$.
6. Se hace público el grupo n y la clave e.
7. Se guarda en secreto la clave d.

Podrían destruirse ahora p, q y $\phi(n)$.

Lámina 145 Dr. Roberto Gómez C.

Ejemplo generación llaves en RSA

Beto genera su par de llaves

- Usuario elige dos números primos: $p_b = 281$ y $q_b=167$
- calcula $n_b = 281*167 = 46927$
- Orden grupo: $\Phi(46927) = 280\times166 = 46480$
- B elige número $e_b=39423$ y comprueba que:

  $mcd(39423,46480)=1$
- B determina el inverso de 39423 módulo 46480, el cual es $d_b=26767$
- Por lo que la llave pública de B es

  $(n_b, e_b) = (46927, 39423)$
- Mantiene en secreto el resto de los valores

Lámina 146 Dr. Roberto Gómez C.

Ejemplo encripción/decripción RSA

- Mensaje a encriptar: M=48
- Grupo n = 91 = 7∗13
- $\phi(n) = \phi(7*13) = (7-1)(13-1) = 72$
- Elegimos e = 5 pues mcd (5,72) = 1
- Se calcula el inverso de e: d = inv(5,72) = 29
- Para encriptar:
  - $C = M^e \bmod n = 48^5 \bmod 91 = 5245.803.968 \bmod 91 = 55$
- Se envia el mensaje 55 al receptor
- Para decriptar:
  - $M = C^d \bmod n = 55^{29} \bmod 91 = 48$

Lámina 147 Dr. Roberto Gómez C.

Observaciones del ejemplo

- Número pequeños para entender funcionalidad
- Aunque:
  - 55^{29} ya es "*número grande*"
  - 55^{29} es un número con 51 dígitos...
  - 55^{29} = 295473131755644748809642476009391248226165771484375
  - ¿Cómo podemos acelerar esta operación?

1ª opción: usar reducibilidad  2ª opción: algoritmo exp. rápida 

Opción óptima: usar el Teorema del Resto Chino 

Lámina 148 Dr. Roberto Gómez C.

¿Solo se encriptan números?

- Mensaje M se transforma en números y éstos se dividen en bloques de de g-1 dígitos, siendo g el número de dígitos del módulo de trabajo: el valor n para RSA.
- Si el mensaje M fuese mayor que el módulo de trabajo (n = pq para RSA)
  - habrá que romper el mensaje original en grupos
- En la práctica la longitud es mucho mayor dado que n es un número con mucho más dígitos (el cuerpo de encripción es como mínimo de 512 bits) y el "mensaje" a encriptar tendrá sólo una centena de bits

Lámina 149 Dr. Roberto Gómez C.

Como pasar de un mensaje a un número

- Primera opción
  - representar el mensaje en su valor ANSI decimal
- Segunda opción
  - codificar las letras del alfabeto en base 26
- En los dos casos hay que cuidar que el número resultante no sea mayor que el módulo de trabajo
  - n = pq para RSA y
  - p para ElGamal

Lámina 150 Dr. Roberto Gómez C.

Ejemplo representación ANSI decimal

Se representará el mensaje en su valor ANSI decimal.

$n = p*q = 89*127 = 11303 \Rightarrow$ bloques de <u>cuatro</u> dígitos

$\phi(n) = 11088;\ e = 25;\ d = \text{inv}(25, 11088) = 10201$

M = Olé = 079 108 233 $\Rightarrow$ M = 0791 0823 3

Se recupera el mensaje agrupando en bloques de 4 dígitos excepto el último

ENCRIPCION

$C_1 = 791^{25} \bmod 11303 = 7853$

$C_2 = 823^{25} \bmod 11303 = 2460$

$C_3 = 3^{25} \bmod 11303 = 6970$

DECRIPCION

$M_1 = 7853^{10201} \bmod 11303 = 0791$

$M_2 = 2460^{10201} \bmod 11303 = 0823$

$M_3 = 6970^{10201} \bmod 11303 = 3$

Lámina 151 Dr. Roberto Gómez C.

Ejemplo segunda opción

Se representará el mensaje con letras del alfabeto en base 26

$n = p*q = 281*167 = 46927 \Rightarrow$ bloques de <u>tres</u> letras

$26^3 = 1756 < n < 456976 = 26^4$

$\phi(n) = 46480;\ e = 39423;\ d = \text{inv}(39423, 46927) = 26767$

M = YES

ENCRIPCION

$YES = Y \cdot 26^2 + E \cdot 26 + S$

$= (24 \cdot 26^2) + (4 \cdot 26) + 18 = 16346$

$\therefore m = 16346$

$C = 16346^{39423} \bmod 46927 = 21166$

DECRIPCION

$M = 21166^{26767} \bmod 46927 = 16346$

$M = 16346$

$= (24 \cdot 26^2) + (4 \cdot 26) + 18$

$= YES$

Lámina 152 Dr. Roberto Gómez C.

El problema de factorización

- En 1977 se lanzó un reto matematico
- Artículo *A New Kind of Cipher that Would Take Millions of Years to break*
- Columna *Mathematical Games* en *Scientific American*
- Criptosistema encriptado con llave pública

  114,381,625,757,888,867,669,235,779,926,146,612,010,218,296,721,
  242,362,562,561,842,935,706,935,245,733,897,830,597,123,563,958,
  705,058,989,075,147,599,290,026,879,543,541

- Se estima que la factorización tomo aproximadamente 4000 a 6000 MIPS años de computo sobre un periodo de seis a ocho meses.

Lámina 153 Dr. Roberto Gómez C.

La solución

- El 26 de abril de 1994, un equipo de 600 voluntarios anunciaron los factores de N
- El factor q

  3,490,529,510,847,650,949,147,849,619,903,898,133,417,764,638,
  493,387,843,990,820,577
- El factor p

  32,769,132,993,266,709,549,961,988,190,834,461,413,177,642,967,
  992,942,539,798,288,533
- El mensaje era:

  200805001301070903002315180419000118050019172105011309190800
  151919090618010705

  "THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE"

Lámina 154 Dr. Roberto Gómez C.

Tiempos factorizacion

Numero Digitos decimales	Número de bits (aprox)	Fecha del logro	MIPS-año	Algoritmo
100	332	abril 1991	7	Quadratic sieve
110	365	abril 1992	75	Quadratic sieve
120	398	junio 1993	830	Quadratic sieve
129	428	abril 1994	5000	Quadratic sieve
130	431	abril 1996	500	Generalizado

MIPS-año: procesador de un millón de instrucciones por segundo corriendo un año, lo cual equivale a $2x10^{13}$ instrucciones ejecutadas. Un Pentium 200 MHz equivale aprox. a una máquina de 50 MIPS

Lámina 155 Dr. Roberto Gómez C.

¿Y hoy en día?

Lámina 156 Gómez C.

Ejemplo de una llave pública

Lámina 157
Dr. Roberto Gómez C.

Otros algoritmos de llave pública

- El Gammal
- Pohling Hellman
- Rabin
- McEliece
- Criptosistemas de llave pública de automatas finitos.

Lámina 158
Dr. Roberto Gómez C.

Algoritmos de intercambio de llaves

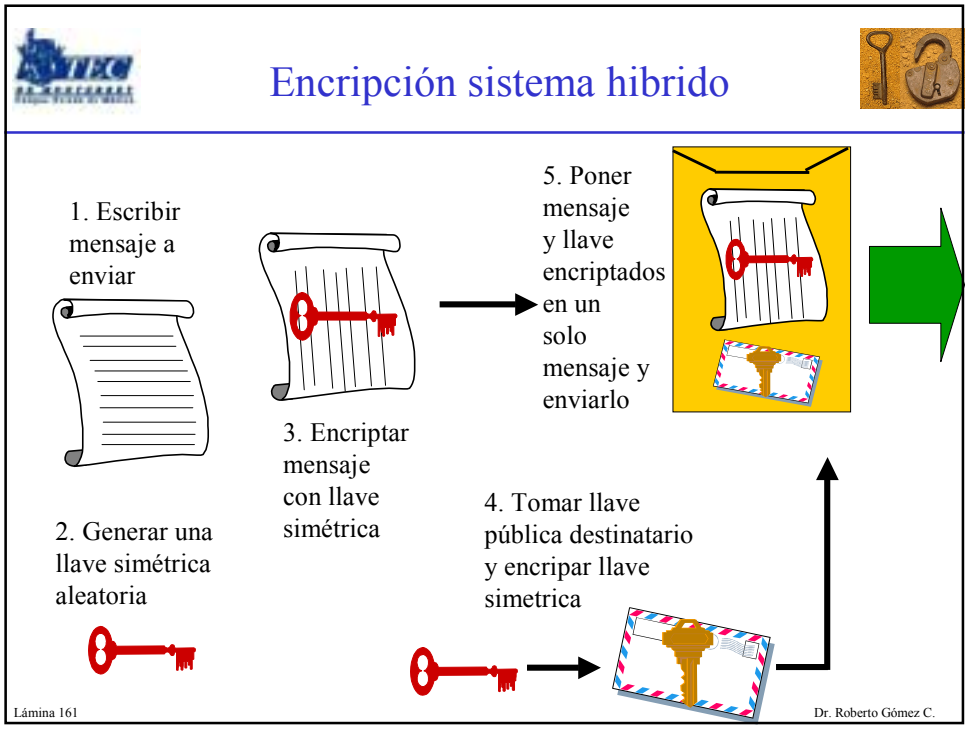
- Protocolo de estación-estación
- Protocolo de tres pasos de Shamir
- COMSET
- Encrypted Key Exchange
- Fortified Key Negotiation
- Conference Key Distribution and Secret Broadcasting

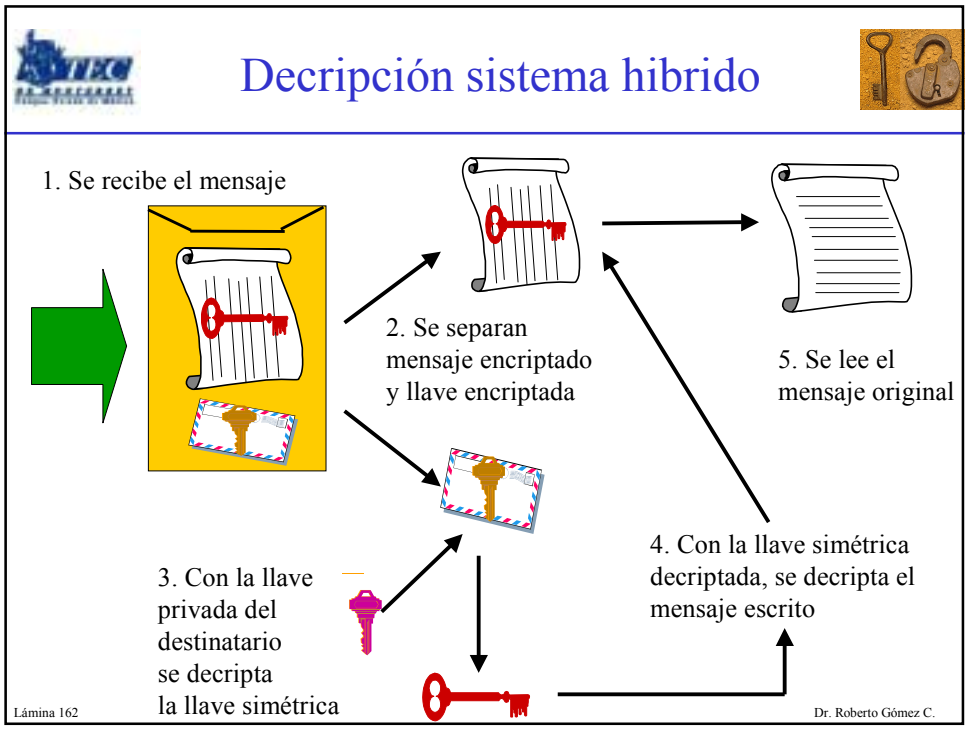
Lámina 159 Dr. Roberto Gómez C.

Sistemas Hibridos

- Un algoritmo simétrico con una llave de sesión aleatoria es usada para encriptar un mensaje.
- Un algoritmo de llave pública es usado para encriptar la llave de sesión aleatoria.

Lámina 160 Dr. Roberto Gómez C.


Encripción sistema hibrido
1. Escribir mensaje a enviar
2. Generar una llave simétrica aleatoria
3. Encriptar mensaje con llave simétrica
4. Tomar llave pública destinatario y encripar llave simetrica
5. Poner mensaje y llave encriptados en un solo mensaje y enviarlo
Lámina 161
Dr. Roberto Gómez C.


Decripción sistema hibrido
1. Se recibe el mensaje
2. Se separan mensaje encriptado y llave encriptada
3. Con la llave privada del destinatario se decripta la llave simétrica
4. Con la llave simétrica decriptada, se decripta el mensaje escrito
5. Se lee el mensaje original
Lámina 162
Dr. Roberto Gómez C.

Funciones de autenticación

- Encripción de mensajes
  - el criptograma del mensaje entero sirve como su autenticador.
- Funciones hash
  - una función pública que mapea el mensaje de cualquier tamaño en un valor hash de tamaño fijo, el cual sirve de autenticador.
- Códigos de autenticación de mensajes
  - una función pública del mensjae y una llave secreta que produce un valor de longitud variable que sirve de autenticador

Lámina 163 Dr. Roberto Gómez C.

Un esquema de autenticación

Lámina 164 Dr. Roberto Gómez C.

Las funciones hash

- Sistema anterior es lento y produce gran cantidad de información
- Mejoramiento: añadir una one-way hash function
  - función toma una variable de tamaño variable (cientos o miles de bits) y una salida de tamaño fijo (p.e. 160 bits)
- Función asegura que, si la información es cambiada (aún en sólo un bit) un valor completamente diferente es producido

Lámina 165 Dr. Roberto Gómez C.

Características hash

- Libre de colisión:
  - difícil de generar dos entradas que generen la misma salida
- La salida es única
  - asegura que, si la información es cambiada (aún en sólo un bit) un valor completamente diferente es producido
- Es pública
  - no hay secretos en el proceso, la seguridad radica en su único sentido y en el hecho de que la salida no depende de la entrada

Lámina 166 Dr. Roberto Gómez C.

La función hash MD5

- ***MD5*** toma como entrada un mensaje de longitud arbitraria y regresa como salida una "*huella digital*" de 128 bits del mensaje (llamado message-digest o compendio del mensaje).
- Se estima que es imposible obtener dos mensajes que produzcan la misma huella digital.
- También es imposible producir un mensaje que arroje una huella predefinida

Lámina 167 Dr. Roberto Gómez C.

Descripción del algoritmo

- El mensaje de entrada puede tener cualquier longitud, no necesariamente debe ser múltiplo de 8.
- Los pasos que sigue el algoritmo son:
  - **Paso 1.** Agregado de bits de relleno (*Padding*).
  - **Paso 2.** Agregado de la longitud.
  - **Paso 3.** Inicialización del buffer del MD
  - **Paso 4.** Procesamiento del mensaje en bloques de 16 palabras.
  - **Paso 5.** Compendio del mensaje.

Lámina 168 Dr. Roberto Gómez C.

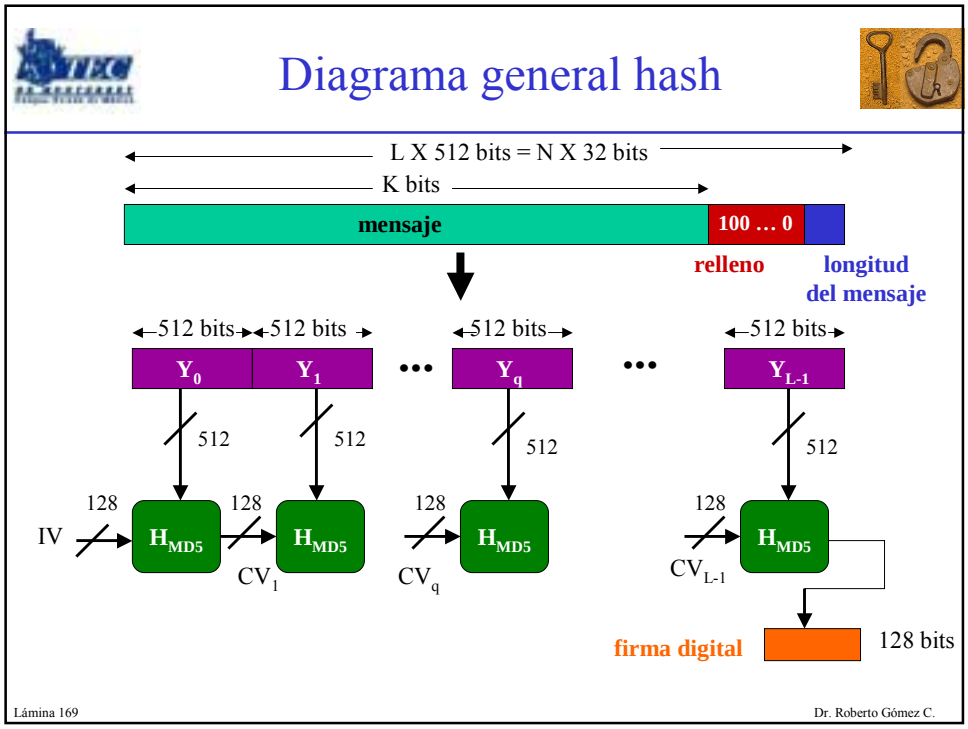


Diagrama general hash
L X 512 bits = N X 32 bits
K bits
mensaje
100 … 0
relleno
longitud del mensaje
512 bits
512 bits
512 bits
512 bits
Y0
Y1
Yq
YL-1
512
512
512
512
128
128
128
128
IV
HMD5
HMD5
HMD5
HMD5
CV1
CVq
CVL-1
firma digital
128 bits
Lámina 169
Dr. Roberto Gómez C.

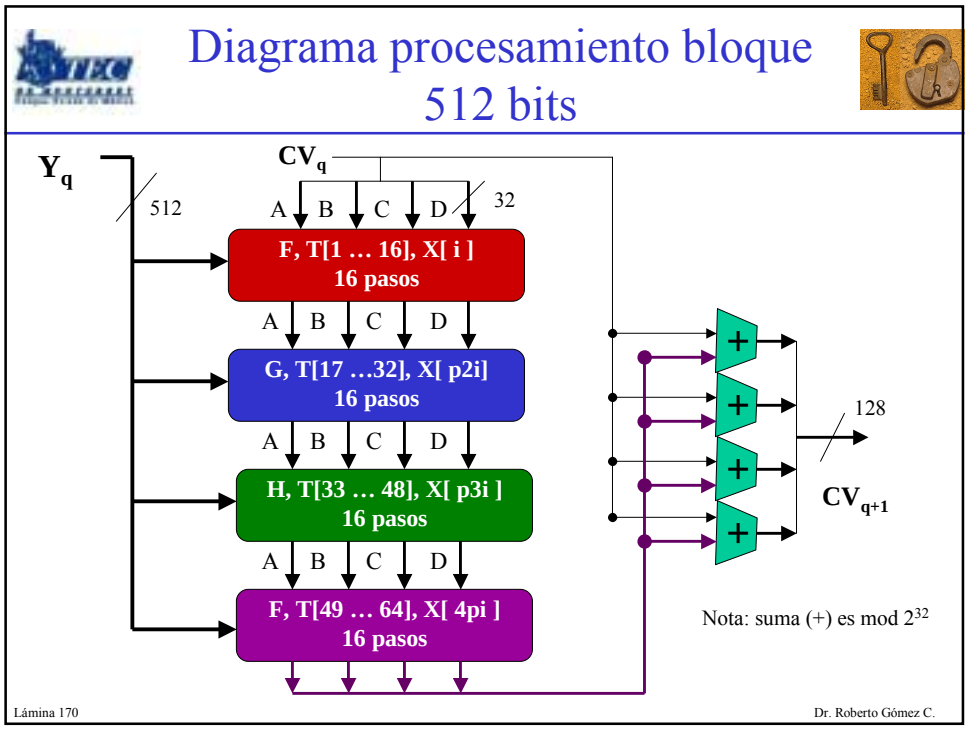


Diagrama procesamiento bloque 512 bits
Yq
512
CVq
A B C D
32
F, T[1 … 16], X[i]
16 pasos
G, T[17 …32], X[p2i]
16 pasos
H, T[33 … 48], X[p3i]
16 pasos
F, T[49 … 64], X[4pi]
16 pasos
128
CVq+1
Nota: suma (+) es mod 2^32
Lámina 170
Dr. Roberto Gómez C.

Salida de MD5

rogomez@armagnac:464>more toto
ULTRA SECRETO

Siendo las 19:49 hrs del dia 19 de noviembre de 1999
pretendo anunciar que se termino el presente texto
para pruebas de programas hash.

Atte;

RGC
rogomez@armagnac:465>md5 toto
MD5 (toto) = 0c60ce6e67d01607e8232bec1336cbf3
rogomez@armagnac:466>

Lámina 171 Dr. Roberto Gómez C.

rogomez@armagnac:467>more toto
ULTRA SECRETO

Siendo las 19:49 hrs del dia 19 de noviembre de 1999
pretendo anunciar que se termino el presente texto
para pruebas de programas hash.

Atte

RGC
rogomez@armagnac:468>hash1 toto
MD5 (toto) = 30a6851f7b8088f45814b9e5b47774da
rogomez@armagnac:469>

Lámina 172 Dr. Roberto Gómez C.

Otra función hash SHA-1

- Desarrollado por el National Institute of Standards and Technology (NIST) y publicado como una FIPS.
- Toma un mensaje de entrada con una longitud máxima de 264 bits y produce una salida de 160 bits.
- Entrada es procesada en bloques de 512 bits.
- Pasos que sigue:
  - Añadir bits de relleno (padding bits).
  - Añadir la longitud.
  - Inicializar el buffer de 160 bits MD
  - Procesar el mensaje en bloques de 512 palabras
  - Imprimir la salida

Lámina 173 Dr. Roberto Gómez C.

Otras funciones hash de un solo sentido

- Algoritmo MD2
- Algoritmo MD4
- RIPE MD-160
- HMAC
- N-Hash
- Havalk

Lámina 174 Dr. Roberto Gómez C.

La huella digital

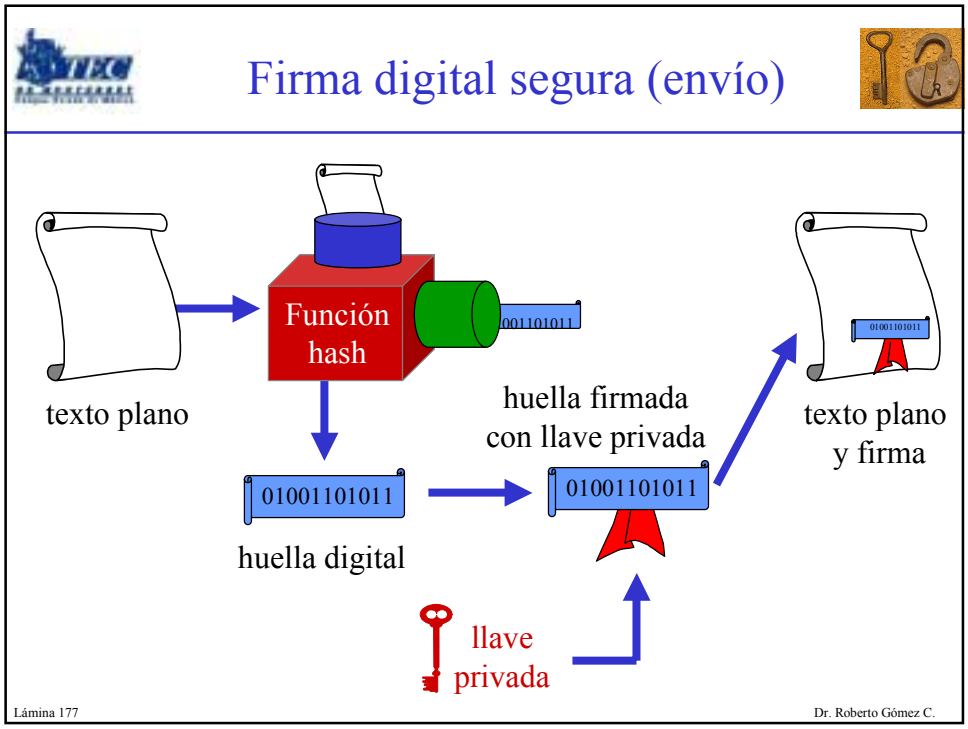
- La salida producida por una función hash aplicada a un documento, es conocida con el nombre de huella digital de dicho documento
- Cualquier cambio en el documento produce una huella diferente
- Huella digital también es conocida como compendio de mensaje (cuando el documento es un mensaje)

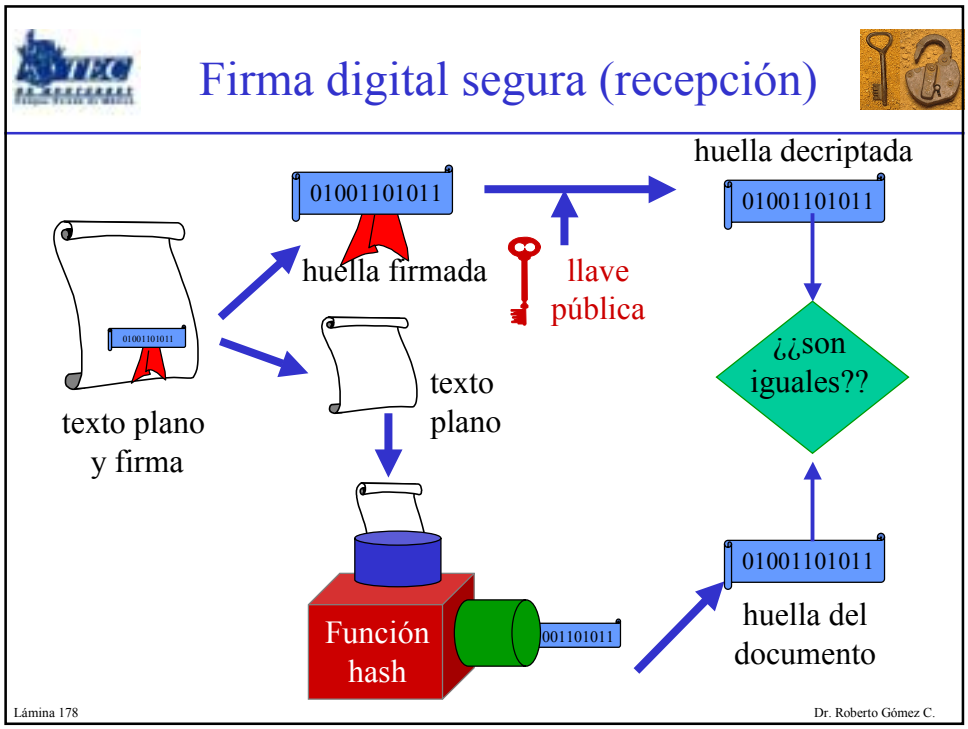
Lámina 175 Dr. Roberto Gómez C.

Firmas digitales y huellas digitales

- Es posible usar la huella y la llave privada para producir una firma
- Se transmite el documento y la firma juntos
- Cuando el mensaje es recibido, el receptor utiliza la función hash para recalcular la huella y verificar la firma
- Es posible encriptar el documento si así se desea

Lámina 176 Dr. Roberto Gómez C.


Firma digital segura (envío)
Función hash
texto plano
huella digital
huella firmada con llave privada
texto plano y firma
llave privada
Lámina 177
Dr. Roberto Gómez C.


Firma digital segura (recepción)
huella decriptada
huella firmada
llave pública
texto plano y firma
texto plano
¿¿son iguales??
Función hash
huella del documento
Lámina 178
Dr. Roberto Gómez C.

Seguridad de la firma

- Seguridad depende de lo seguro de la función hash
- No existe ninguna forma de tomar la firma de alguien de un documento y ponerla en otro
- No es posible alterar un mensaje firmado
- El más simple cambio en el documento firmado se verá en la verificación

Lámina 179 Dr. Roberto Gómez C.

Códigos Autenticación Mensaje

- MAC por sus siglas en inglés
- También conocido bajo el nombre de DAC (Data Authentication Code)
- Función de un solo sentido junto con una llave secreta:

$$MAC = C_K(M)$$

- M es el mensaje, K es una lleve que conoce tanto el emisor como el receptor, y C_K es una función hash basada en K.

Lámina 180 Dr. Roberto Gómez C.

Códigos Autenticación Mensaje

- El principio es el mismo, pero si alguien conoce la llave puede verificar el valor hash.
- El sitio emisor pega el MAC al mensaje cuando se decide que el mensaje es correcto.
- El receptor auténtica re-calculando el MAC
- Ejemplo MAC
  - Data Authentification Algorithm.

Lámina 181 Dr. Roberto Gómez C.

Firma digital en base a MAC (emisión)

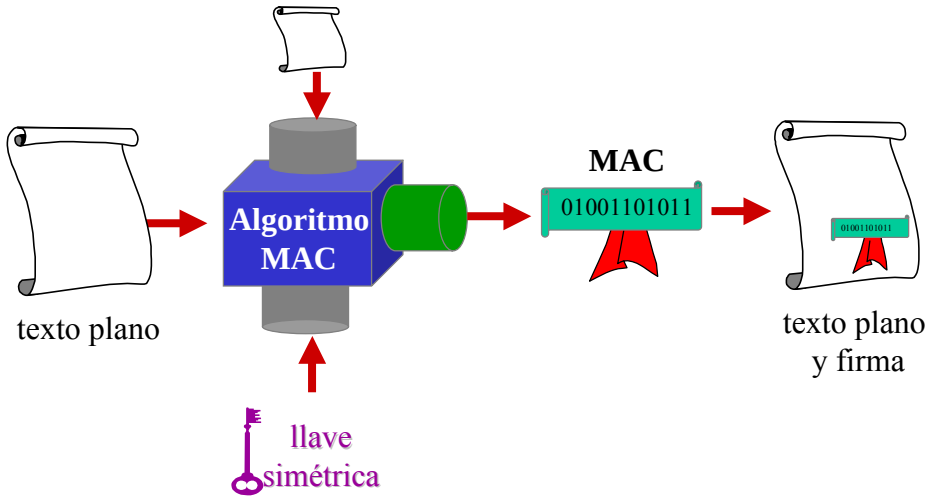


Lámina 182 Dr. Roberto Gómez C.

Firma digital en base a MAC (recepción)

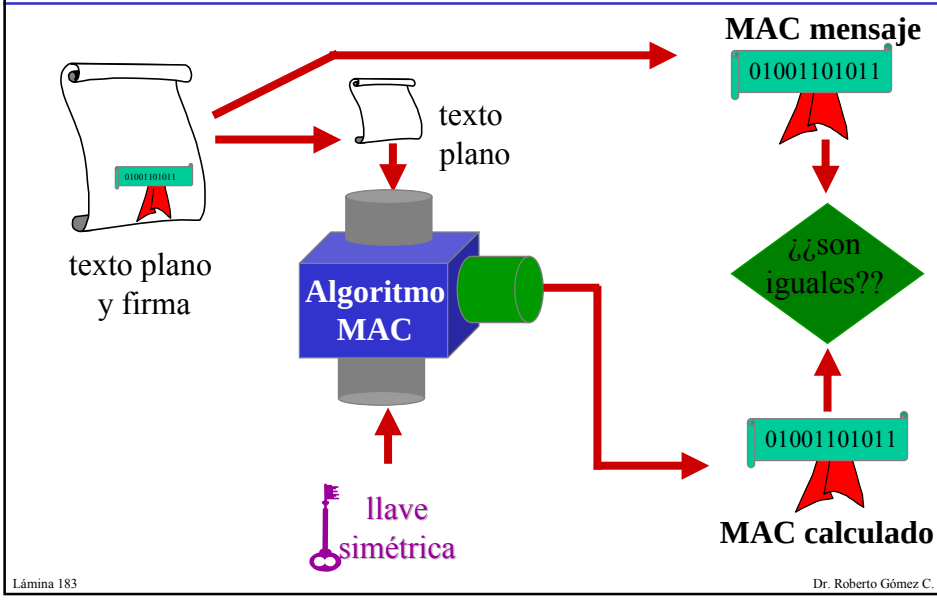


Lámina 183
Dr. Roberto Gómez C.

Otros algoritmos de firma digital de llave pública

- Digital Signature Algorithm (DSA)
- Variantes DSA
- Gost Digital Signature Algorithm
- Discrete Logarithm Signature Schemes
- Ong-Schorr-Shamir
- ESIGN
- Automatas celulares

Lámina 184
Dr. Roberto Gómez C.

Problemas de la criptografía de llave pública

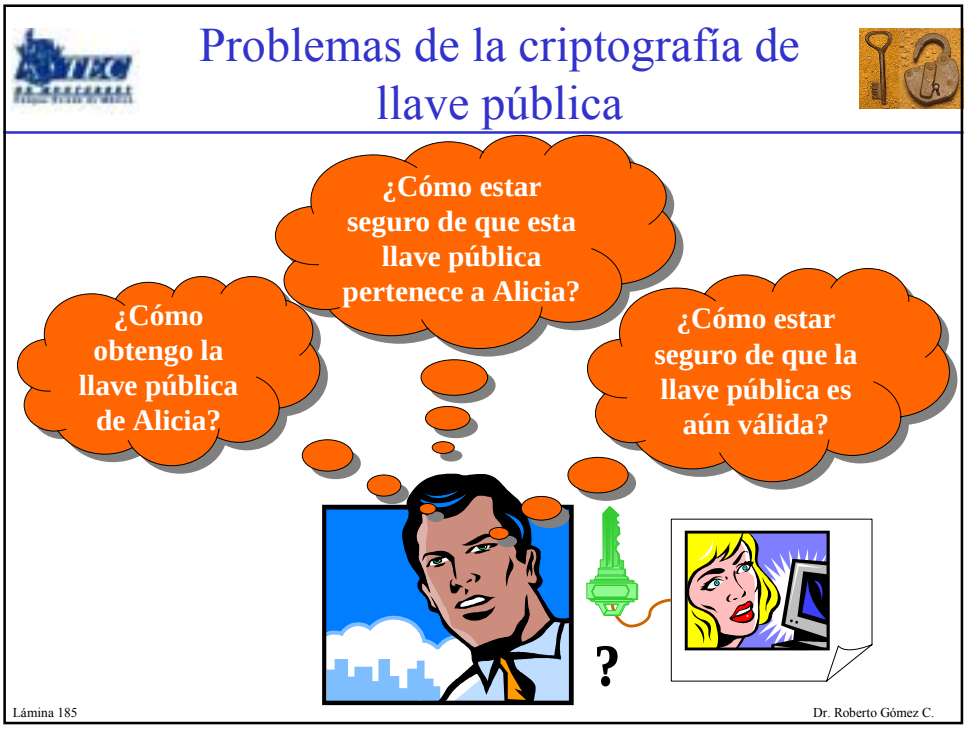


Lámina 185
Dr. Roberto Gómez C.

Solicitando una llave pública

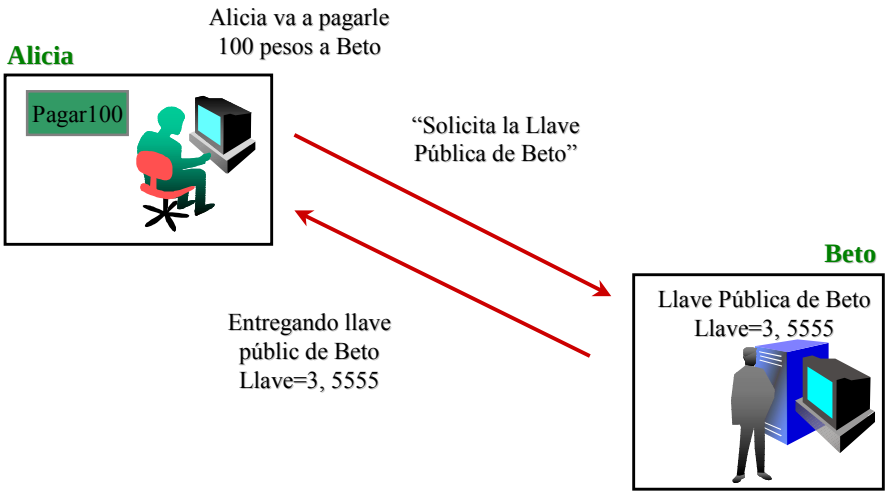


Lámina 186
Dr. Roberto Gómez C.

El ataque "Man in the Middle" (MIM)

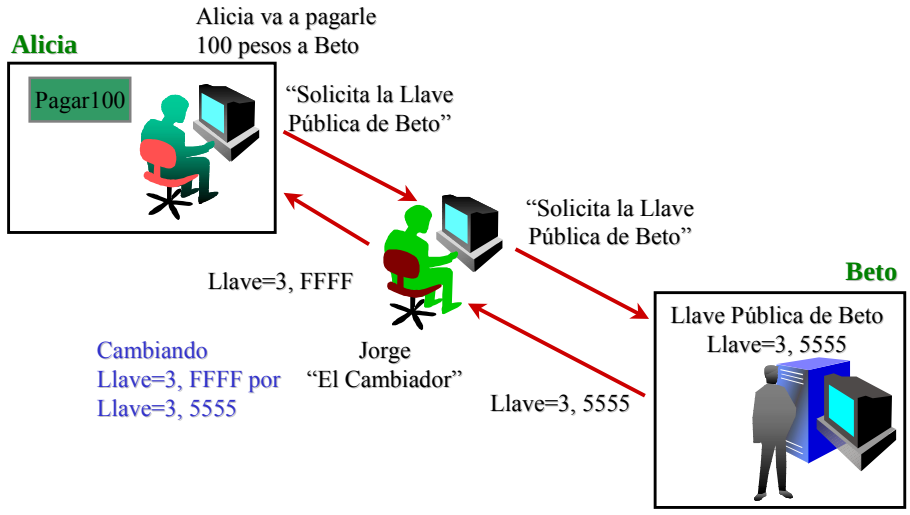


Lámina 187 Dr. Roberto Gómez C.

Solución al MIM

- Solución:
  - Intercambio de llaves públicas firmadas digitalmente con la llave privada de una 3a persona.
  - 3a. persona de confianza que de a conocer su llave pública.
- Uso de un certificado digital que certifique que la llave pertenece en realidad a la persona.

Lámina 188 Dr. Roberto Gómez C.

Ese momento desafortunado cuando 2 cybernautas se encuentran cara a cara

Lámina 189 Dr. Roberto Gómez C.

Los Certificados Digitales

- Es un documento que asienta que una llave pública y su correspondiente llave privada pertenecen a un individuo en particular, certificando de esta manera la identidad de dicho individuo.
- Tiene el propósito de hacer disponible a otras personas una llave pública personal.

Lámina 190 Dr. Roberto Gómez C.

Autoridades Certificadoras (CAs)

- Los certificados son expedidos por autoridades confiables conocidas como *Autoridades Certificadoras*, (CA por sus siglas en inglés).
- Estas entidades son responsables de certificar la identidad de un individuo y su posesión de una llave pública.
- Generan y administran certificados y los publican en repositorios.

Lámina 191 Dr. Roberto Gómez C.

Elementos Certificados Digitales

- Partes importantes:
  - Nombre del usuario y otra información adicional, tal como su e-mail.
  - Llave pública del usuario.
  - Nombre del emisor (CA).
  - Número serial.
  - Periodo de validez.
  - Firma que enlaza todas las partes del certificado.
- No contiene información que deba ser segura.

Lámina 192 Dr. Roberto Gómez C.

Estandares Certificados Digitales

- La interoperabilidad entre sistemas de distintos fabricantes se logra a través del estándar público X.509, que gobierna el formato y el contenido de los certificados digitales.
- Algunas implementaciones del formato son:
  - SSL (cliente o servidor)
  - SET
  - S/MIME

Lámina 193 Dr. Roberto Gómez C.

El formato X.509

- Definido por la ISO.
- Debe contener información tanto de la entidad que lo solicitó como de la Autoridad Certificadora que lo expidió.
- Consta de dos partes:
  - la información del certificado
  - la firma de la Autoridad Certificadora

Lámina 194 Dr. Roberto Gómez C.

Elementos estándar X.509

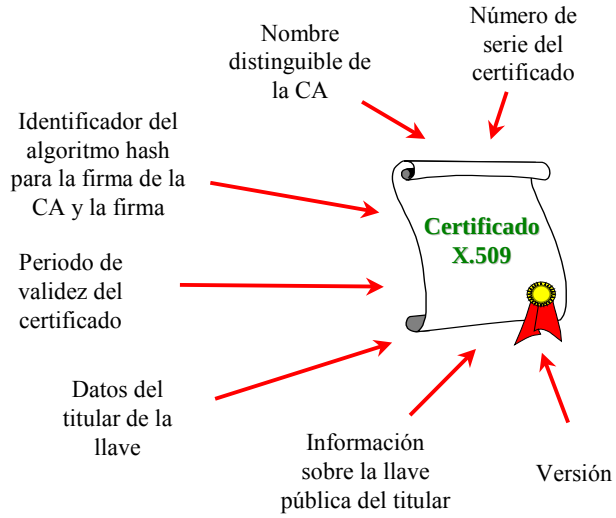


Lámina 195
Dr. Roberto Gómez C.

Ejemplo Certificado Digital

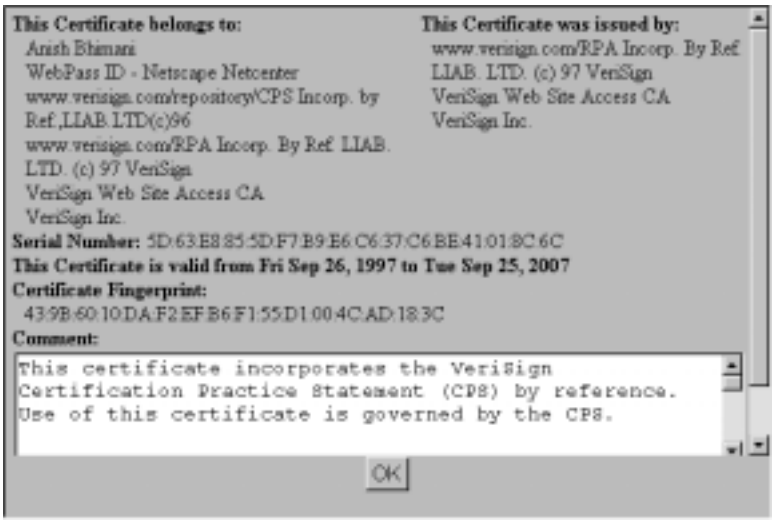
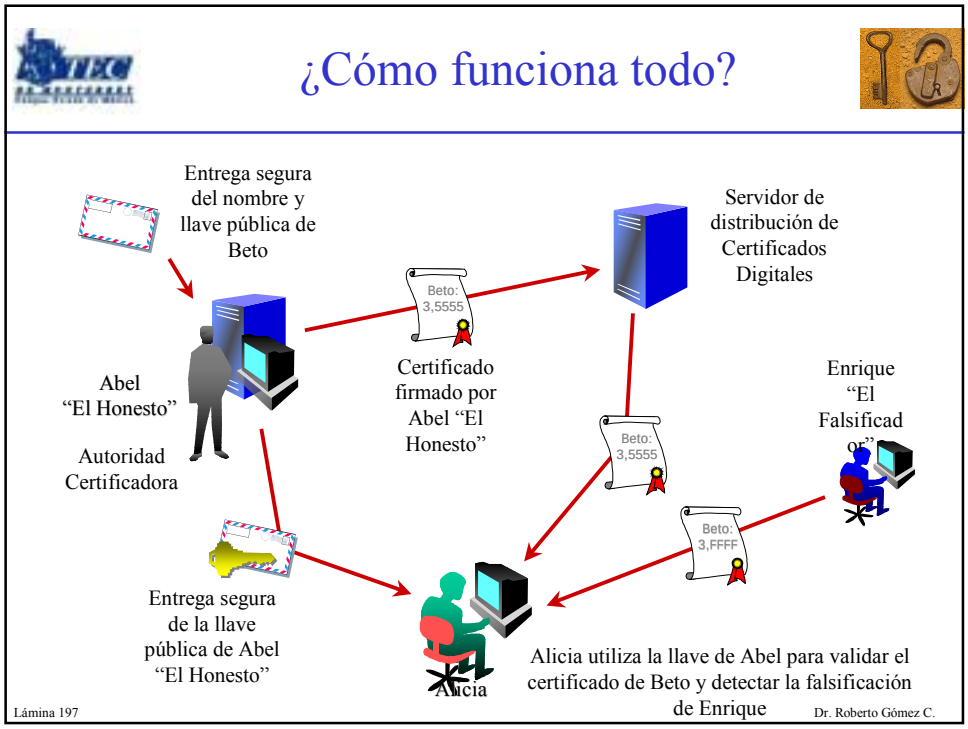
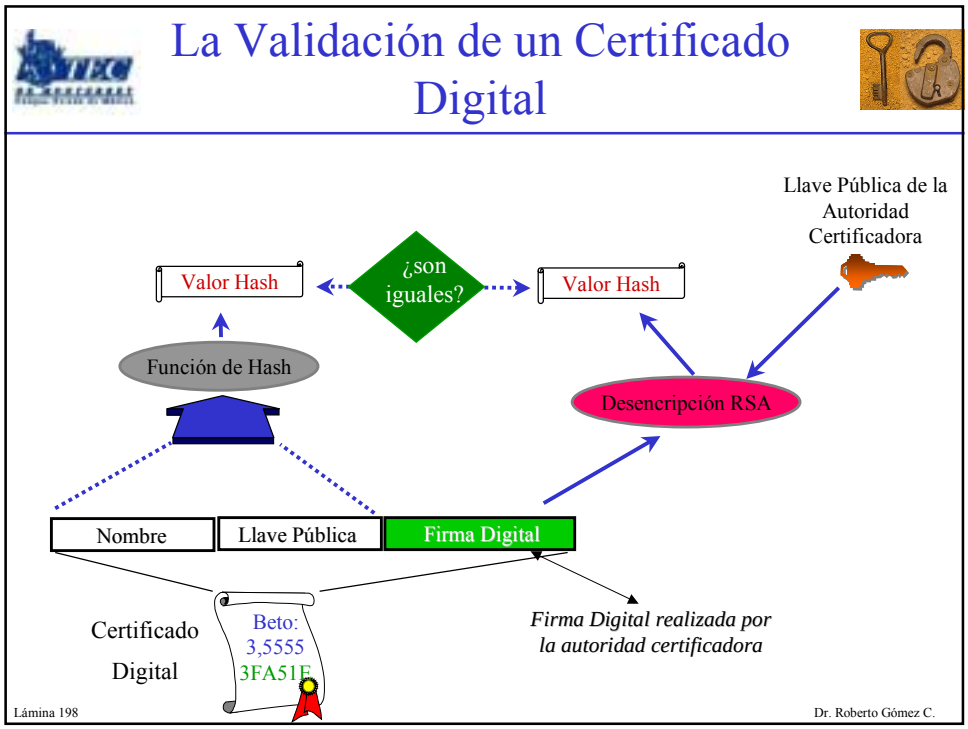


Lámina 196
Dr. Roberto Gómez C.


¿Cómo funciona todo?
Entrega segura del nombre y llave pública de Beto
Servidor de distribución de Certificados Digitales
Beto: 3,5555
Certificado firmado por Abel "El Honesto"
Abel "El Honesto"
Autoridad Certificadora
Enrique "El Falsificador"
Beto: 3,5555
Beto: 3,FFFF
Entrega segura de la llave pública de Abel "El Honesto"
Alicia
Alicia utiliza la llave de Abel para validar el certificado de Beto y detectar la falsificación de Enrique
Lámina 197
Dr. Roberto Gómez C.


La Validación de un Certificado Digital
Llave Pública de la Autoridad Certificadora
Valor Hash
¿son iguales?
Valor Hash
Función de Hash
Desencripción RSA
Nombre
Llave Pública
Firma Digital
Certificado Digital
Beto: 3,5555 3FA51E
Firma Digital realizada por la autoridad certificadora
Lámina 198
Dr. Roberto Gómez C.

Verificando una firma

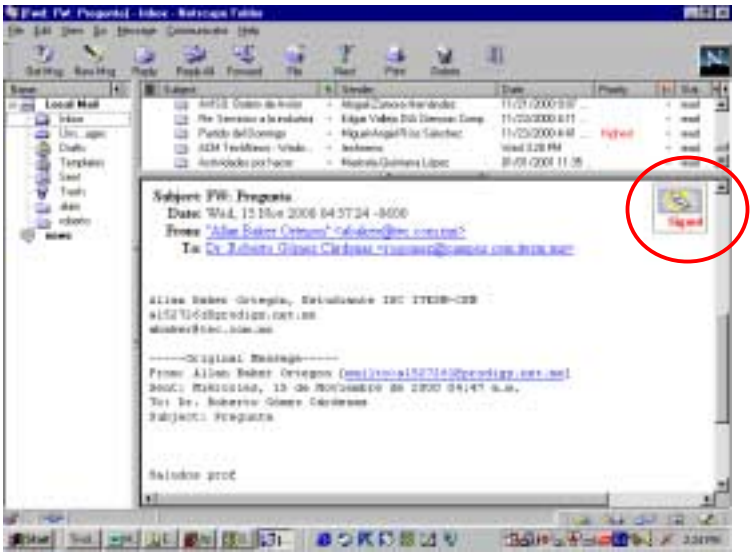


Lámina 199
Dr. Roberto Gómez C.

Verificando una firma

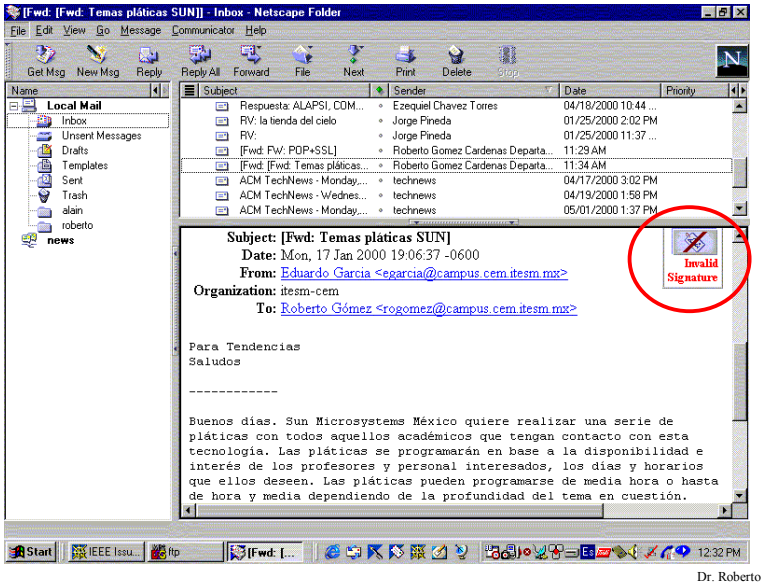


Lámina 200
Dr. Roberto Gómez C.

La Generación de un Certificado Digital

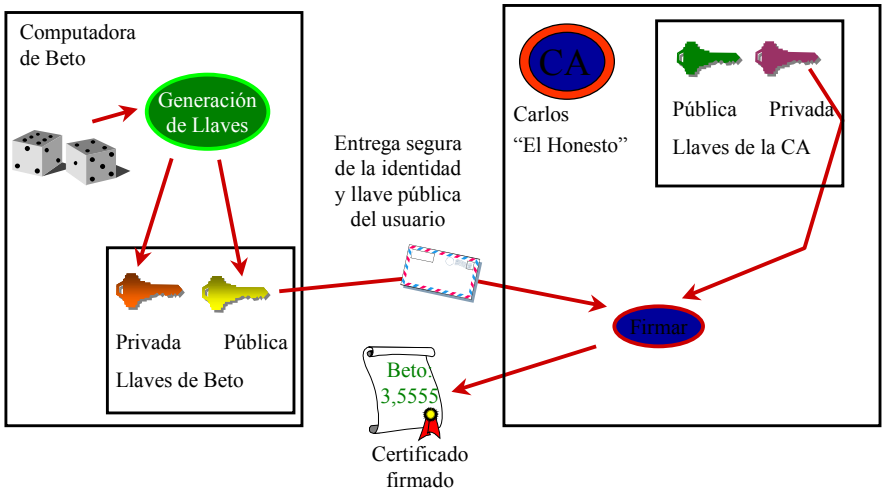


Lámina 201 Dr. Roberto Gómez C.

Revocación

- Las CAs necesitan alguna forma de revocar los certificados
- Propuesta: listas de revocación de certificados CRL (Certificate Revocation List)
- Idealmente una CA emite una CRL a intervalos regulares.
- Además de listar los certificados revocados, la CRL especifica durante cuanto tiempo es válida esta lista y cuando obtener la siguiente.

Lámina 202 Dr. Roberto Gómez C.

Causas revocación

- Baja solicitada por el usuario.
- Baja por exposición de llaves.
- Baja por finalización del periodo de vida del certificado.
- Baja por abandono de la organización.
- Baja por orden superior (mal uso del Certificado).

Lámina 203
Dr. Roberto Gómez C.

Infraestructura de llave pública (PKI)

Una infraestructura de llave pública (PKI) es la arquitectura, organización, tecnología, prácticas, políticas y procedimientos que en conjunto soportan la implantación y operación de un sistema criptográfico de llave pública basado en certificados.

PKI´s son 80% políticas y 20% tecnología

Lámina 204
Dr. Roberto Gómez C.

Componentes de una PKI

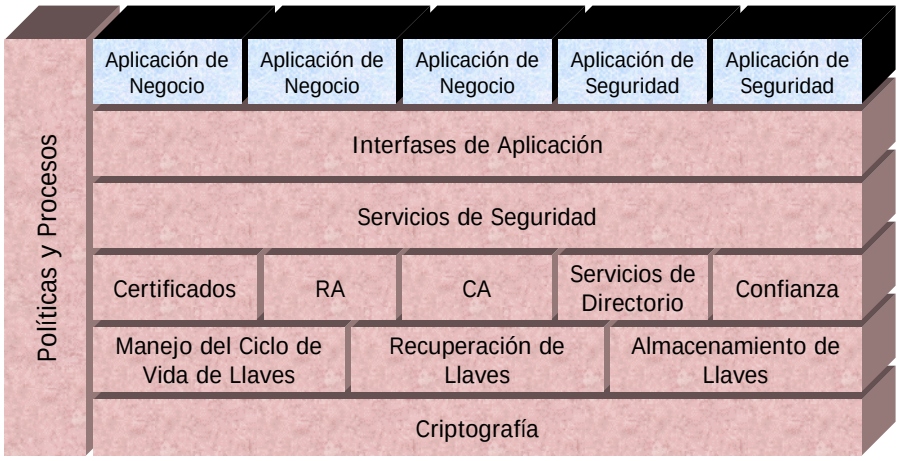


Lámina 205 Dr. Roberto Gómez C.

Criptologia y transmisión datos

Protocolos de transmisión de datos seguros en Internet

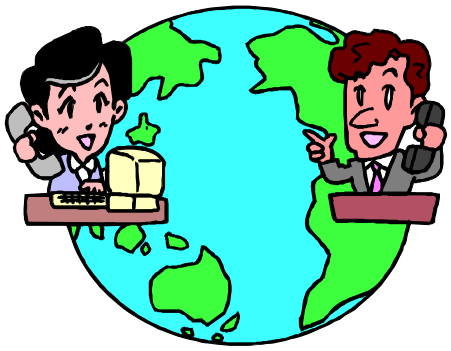


Lámina 206 Dr. Roberto Gómez C.

Protocolos existentes

- SSL
- PCT
- TLS
- S-HHTP
- Ipsec e IPv6
- SSH
- PGP
- S/MIME
- iKP
- SET
- CyberCash/CyberCoin
- DNSEC
- Kerberos
- S/Key

Lámina 207 Dr. Roberto Gómez C.

SSL, PCT y TCL

- Protocolos criptográfico de propósito general para asegurar canales de comunicación bidireccionales
- Se utilizan comúnmente junto con el protocolo TCP/IP
- Sistema encripción usado por navegadores Netscape e Internet Explorer

Lámina 208 Dr. Roberto Gómez C.

SSL, PCT y TLS

- 1994: SSL V 2.0 (Netscape)
  microsoft descubre un problema en SSL
- 1995: PCT V 1.0
- 1996: SSL V 3.0
- 1997: PCT V 4.0
  se decide terminar con la pelea: Microsoft y Netscape deciden sacar un protocolo en común
- 1999: TLS V 1.0

Lámina 209 Dr. Roberto Gómez C.

¿Cómo funciona?

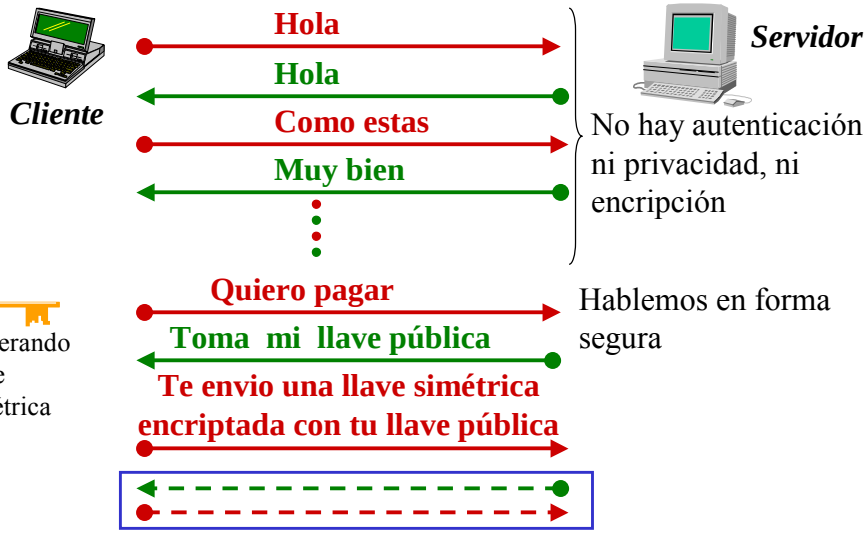


Lámina 210 Dr. Roberto Gómez C.

Otro posible escenario

Hablemos de forma segura, aquí están los protocolos y criptosistemas que manejo

Escogo este protocolo y criptosistema. Aquí esta mi llave pública, un certificado digital y un número random

Usando tu llave pública encripte una llave simétrica aleatoria

Comunicación encriptada con la llave enviada por el cliente y un hash para autenticación de mensajes

Lámina 211 Dr. Roberto Gómez C.

Ejemplo protocolo seguro (1er. paso)

Lámina 212 Dr. Roberto Gómez C.

Ejemplo protocolo seguro (2do.paso)

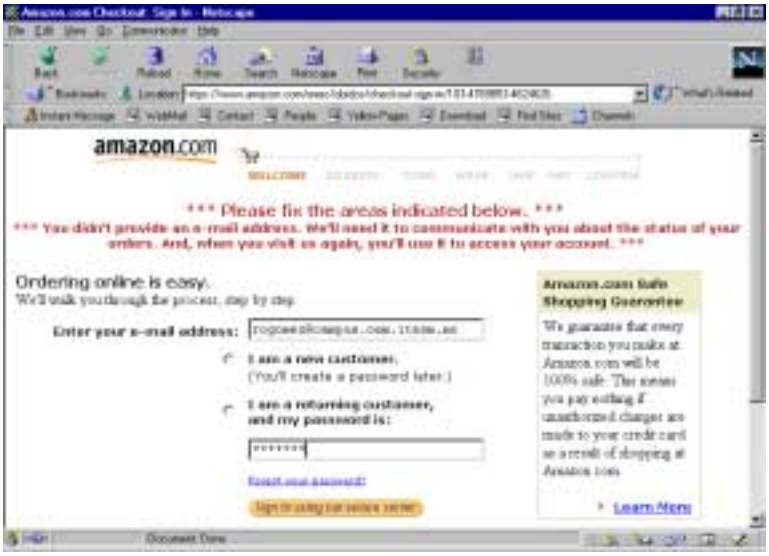


Lámina 213
Dr. Roberto Gómez C.

Tipos ataques criptográficos

Clasificación de acuerdo a los datos que se requieren para el ataque.

- Ciphertext only attack
- Kown-Plaintext attack
- Chosen text attack
  - Chosen plaintext Attack
  - Chosen ciphertext Attack
  - Adaptive Chosen Plaintext Attack
  - Adaptive Chosen Ciphertext Attack

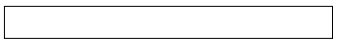
Lámina 214
Dr. Roberto Gómez C.

Ciphertext only attack

Dado:

criptograma 

Se busca por

texto claro
o llave 

Ejemplo

Análisis de frecuencia en el criptograma

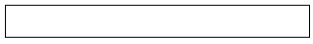
Lámina 215 Dr. Roberto Gómez C.

Ciphertext only attack

Dado:

criptograma 
un fragmento del texto claro 

Se busca por

resto texto claro
o llave 

Ejemplo

Búsqueda exhaustiva de llave
(ataque de fuerza bruta)

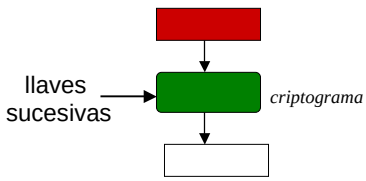


Lámina 216 Dr. Roberto Gómez C.

Chosen plaintext attack

Dado:

Capacidad de encriptar un fragmento arbitrario, elegido, del texto en claro

Se busca por

llave

Ejemplo

Criptoanálisis diferencial

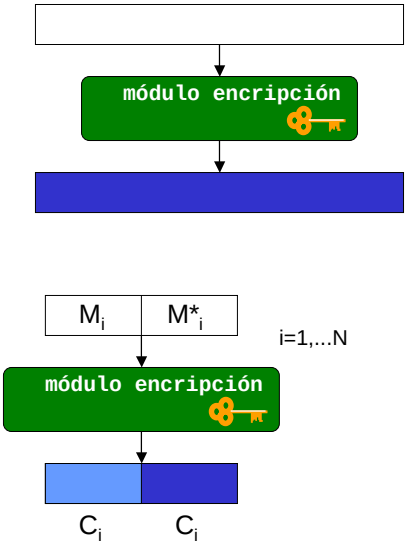


Lámina 217
Dr. Roberto Gómez C.

Resumiendo ...

Alicia : $C \leftarrow encripta(M, K)$

Alicia : envia C a Beto

Beto : $N \leftarrow decripta(C, K)$

1. Ciphertext-only attack
   Eva conoce: $C_1, C_2, \ldots C_n$

2. Known-plaintext attack
   Eva conoce: $\{M_1, C_1\}, \ldots \{M_n, C_n\}$

3. Chosen-plaintext attack
   Lucifer elige $M_1, \ldots M_n$
   Lucifer conoce $\{M_1, C_1\}, \ldots \{M_n, C_n\}$

4. Adaptive chosen-plaintext attack
   Lucifer elige M_1
   Lucifer conoce $\{M_1, C_1\}$
   .....
   Lucifer elige M_n
   Lucifer conoce $\{M_n, C_n\}$

5. Chosen-ciphertext attack
   Lucifer elige $C_1, \ldots C_n$
   Lucifer conoce $\{M_1, C_1\}, \ldots \{M_n, C_n\}$

6. Adaptive chosen-ciphertext attack
   Lucifer elige C_1
   Lucifer conoce $\{M_1, C_1\}$
   .....
   Lucifer elige C_n
   Lucifer conoce $\{M_n, C_n\}, \{M_n, C_n\}$

Lámina 218
Dr. Roberto Gómez C.

Ataque Fuerza Bruta

- También llamado Exhaustive Attack.
- Consiste en probar todas las posibles combinaciones de la llave que pueden llevarme a decriptar el mensaje.
- Consiste en descubrir datos secretos al tratar todas las posibilidades y checar para corregir
- Por ejemplo: para una contraseña de cuatro dígitos
  - uno puede iniciar con 0000 y moverse al 0001, 0002 hasta 9999.
- Requiere de grandes recursos para llevarse a cabo.
- Solo en ciertos criptosistemas es posible realizarlo a mano

Lámina 219 Dr. Roberto Gómez C.

Tiempo requerido para busqueda de llaves

Tamaño llave	Número de llaves posibles	Tiempo requido con 1 encrip/us	Tiempo requido con 10^6 encrip/us
32	$2^{32}= 4.3 \times 10^9$	2^{32} us=35.8 minutos	2.15 milisegundos
56	$2^{56}= 7.2 \times 10^{16}$	2^{56}us=1,142 años	10.01 horas
128	$2^{128}= 3.4 \times 10^{38}$	2^{127}us=3.4×10^{24} años	5.4×10^{18} años

Lámina 220 Dr. Roberto Gómez C.

Algunas técnicas ataque fuerza bruta para llaves simétricas

- Hardware crackers
- Software crackers
- Virus
- La lotería china
- Biotecnología
- DNA Computing
- Quantum Computing

Lámina 221 Dr. Roberto Gómez C.

¿Qué tan grande debe ser la llave?

- La respuesta no es simple.
- Depende de la situación.
  - ¿qué tanto vale la información?
  - ¿cuánto tiempo necesita estar segura?
  - ¿cuáles son los recursos de los posibles adversarios?

Lámina 222 Dr. Roberto Gómez C.

Longitudes llaves simétricas y asimétricas con similar resistencia

Longitud de llave simétrica	Longitud de llave pública
56 bits	384 bits
64 bits	512 bits
80 bits	768 bits
112 bits	1792 bits
128 bits	2304 bits

Lámina 223 Dr. Roberto Gómez C.

Requerimientos para diferente información

Tipo de tráfico	Tiempo de vida	Longitud mínima de la llave
Información militar táctica	minutos/horas	56-64 bits
Anuncios productos, rangos interes	dias/semanas	64 bits
Planes de negocios a largo termino	años	64 bits
Tratos/convenios secretos	decadas	112 bits
Secretos de H-bomb	>40 años	128 bits
Identidades de espias	>50 años	128 bits
Asuntos personales	>50 años	128 bits
Asuntos diplomáticos	>65 años	al menos 128 bits
Datos de censo de USA	100 años	al menos 128 bits

Lámina 224 Dr. Roberto Gómez C.

Una nota sobre longitud de llave

This entire chapter (chapter 7: Key Length) is a whole of nonsense. The very notion of predicting computing power 10 years in the future, let alone 50 years is absolutely ridiculous. These calculations are meant to be a guide, nothing more. If the past is any guide, the future will be vastly different form anything we can predict.

Be conservative. If your keys are longer than you imagine necessary, then fewer technological surprises can harm you.

Bruce Schneider
Sección 7.6 (Cave Emptor)
Applied Cryptography
2da. edición, 1996

Lámina 225 Dr. Roberto Gómez C.

Ataque por diccionario

- Consiste en probar todas las opciones contenidas en un diccionario
- Diccionario = lista de palabras.
- Muy usado en contra de archivos de passwords

Lámina 226 Dr. Roberto Gómez C.

Ataques sobre funciones de un solo sentido

- Existen dos ataques de fuerza bruta sobre una función de solo un sentido:
  - dado el hash de un mensaje, H(M), el adversario quiere ser capaz de crear otro documento M' tal que H(M) = H(M´).
  - el adversario quisiera encontrar dos mensajes al azar, M y M' tal que H(M) = H(M'), a esto se le conoce como colisión.

Lámina 227 Dr. Roberto Gómez C.

Birthday attack

- Es un problema de tipo estadístico.
- ¿Cuál es el valor mínimo de k, para que la probabilidad de que al menos una persona, en un grupo de k gentes, cumpla años el mismo día que usted, sea mayor a 0.5?
  - Respuesta: 253
- ¿Cuál es el valor mínimo de k, para que la probabilidad de que al menos dos personas, en un grupo de k gentes, cumplan años el mismo día, sea mayor a 0.5?
  - Respuesta: 23

Lámina 228 Dr. Roberto Gómez C.

Analogía con funciones un solo sentido

- Encontrar a alguien con un dia de nacimiento es analogo a encontrar un mensaje que coincida con un valor de hash conocido.
- Encontrar a dos gentes con el mismo dia de cumpleaños al azar es analogo a encontrar una colisión de mensajes. Este es conocido como el *birthday attack*.

Lámina 229 Dr. Roberto Gómez C.

¿Es complejo el ataque?

- Asumir función hash produce una salida de m bits y se almacena en x.
- Encontrar un mensaje cuyo valor hash sea igual a x, requiere aplicar la función a 2^m mensajes.
- Encontrar dos mensajes cuyo valor hash sea igual a x, requiere aplicar la función a $2^{m/2}$ mensajes.
- Una máquina que procese un millón de mensajes por segundo tomaría 600,000 años para encontrar un mensaje que colisione con un valor hash de 64 bits.

Lámina 230 Dr. Roberto Gómez C.

Implementando lo anterior

- Programar las rutinas de encripción/decripción uno mismo
- Usar librerías/bibliotecas con rutinas de encripción decripción
- Utilizar estándares aplicaciones disponibles en internet.

Lámina 231 Dr. Roberto Gómez C.

Liberías/rutinas criptográficas

- Crypto++
- Cryptix
- Cryptlib Encryption Toolkit
- OpenSSL
- JCSI - Java Crypto and Security Implementation
- JGSS
- The Delphi Cryptography Page
- Encrypt-COM
- API Java Card
- PowerCrypt
- Elliptic

Lámina 232 Dr. Roberto Gómez C.

Crypto C++

- Página
  - http://www.eskimo.com/~weidai/cryptlib.html
- Aspectos importantes
  - librería gratuita de clases C++.
  - Compilable sin cambios en Visual C++ 6.0 SP3 y gcc (y con reservas en otros compiladores Windows, UNIX y Mac).
  - Permite implementar la mayoría de algoritmos criptográficos, incluidos los cinco candidatos AES.

Lámina 233 Dr. Roberto Gómez C.

Cryptix

- Página
  - http://www.cryptix.org/
- Aspectos importantes:
  - Proyecto internacional de voluntarios destinado a proporcionar librerías gratuitas en Java que permitan implementar los principales algoritmos criptográficos.

Lámina 234 Dr. Roberto Gómez C.

Cryptlib Encryption Toolkit

- Página
  - http://www.cs.auckland.ac.nz/~pgut001/cryptlib/
- Aspectos importantes:
  - Conjunto de herramientas dirigidas a proporcionar seguridad criptográfica a usuarios poco experimentados "en tan sólo media hora".
  - Gratuito para usos no comerciales, existen ciertos terminos para su uso comercial

Lámina 235 Dr. Roberto Gómez C.

Implementación funciones criptologicas

- S/MIME
- PEM
- PGP

Lámina 236 Dr. Roberto Gómez C.

S/MIME

- MIME: Multipurpose Internet Mail Extensions
  - estándar para enviar mensajes con archivos binarios anexos (attach) a través de Internet
- S/MIME extiende el estándar MIME para proporcionar correo electrónico firmado
- Proviene de RSA Data Security (1996)

Lámina 237 Dr. Roberto Gómez C.

S/MIME (cont)

- No fue implementado como un programa sencillo, sino como una biblioteca diseñada para agregarse a los paquetes de correo
- Ofrece:
  - confidencialidad (usuario elige algo encripción)
  - integridad a través de una función hash
  - autenticación con certificados
  - no repudiación con mensajes firmados

Lámina 238 Dr. Roberto Gómez C.

Algoritmos criptograficos usados por S/MIME

- Utiliza un enfoque híbrido para proveer seguridad, conocido como sobre digital.
- La encripción del mensaje es realizada con un algoritmo simétrico y un algoritmo público es usado para el intercambio de llaves.
- S/MIME recomienda usar los algoritmos simétricos: DES, Triple-DES y RC2
- Usa certificados con formato X.509
- S/MIME está disponible en Netscape y Microsoft Outlook Explorer.

Lámina 239 Dr. Roberto Gómez C.

PEM: Privacy-Enhanced Mail

- Estándar de Internet que proporciona intercambio seguro de correo electrónico (RFC 1421).
- Emplea una serie de técnicas criptográficas que proporcionan confidencialidad, autenticación del emisor e integridad del mensaje.
- Autenticación emisor permite a un usuario verificar que el mensaje que recibió es verdaderamente de la persona que dice que lo envió.
- Integridad permite asegurarse que el mensaje no fue modificado durante su transporte.

Lámina 240 Dr. Roberto Gómez C.

¿Dónde se puede obtener PEM?

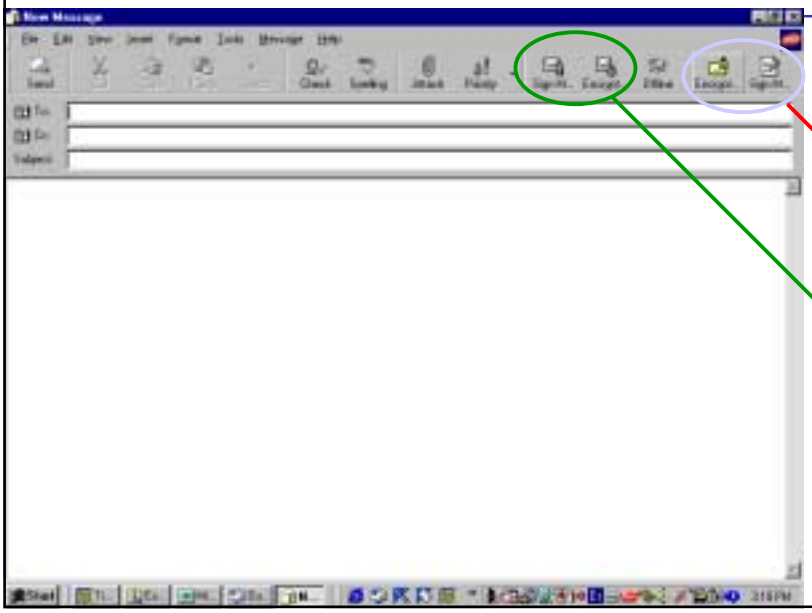
- Existen dos implementaciones de PEM.

1
- Riordan's Internet Privacy Enhanced Mail (RIPEM)
- escrito por Mark Riordan
- disponible de ripem.msu.edu, directorio /pub/crypt y leer el archivo GETTING ACCESS

2
- Originalmente llamada TIS/PEM escrita por Trusted Information Systems
- substituida por TIS/MOSS (versión 7.1)
- un programa que implementa PEM dentro de MIME
- disponible es ftp.tis.com en directorio /pub/MOSS, leer el archivo README

Lámina 241 Dr. Roberto Gómez C.

Integración con Outlook



Dr. Roberto Gómez C.

Notas

- Verificar las leyes locales de los países donde se van a utilizar/programar las funciones criptográficas.
- Verfiricar los permisos y las licencias
- Algunos sistemas ya están preconfigurados de acuerdo al país donde se instalen (ejemplo Netscape)

Lámina 243 Dr. Roberto Gómez C.

Pretty Good Privacy

Lámina 244 Dr. Roberto Gómez C.

¿Qué es PGP?

- Encripción de archivos
- Encripción de correo electrónico
- Manejo de llaves
- Borrado seguro (secure wipe)
- No es
  - esteganografía

Lámina 245 Dr. Roberto Gómez C.

Características de PGP

- Software acceso libre (http://www.pgpi.org).
- Desarrollado por Phil Zimmermann en 1994.
- Protección de e-mail y de archivos de datos.
- Comunicación segura a través de canales inseguros.
- Administración de llaves.
- Firmas digitales.
- Compresión de datos.

Lámina 246 Dr. Roberto Gómez C.

Versiones de PGP

- PGP Freeware v6.5.8 está disponible para Windows 95/98/NT/2000! y el Macintosh.
- PGP Freeware v6.5.8 está disponible para MacOS 7.6.1+
- PGP Command Line Freeware v6.5.8 está disponible para AIX/HP UX/Linux/Solaris!
- PGP Certificate Server Freeware v2.5.8 está disponible para Windows NT/2000 y Solaris

Lámina 247 Dr. Roberto Gómez C.

Servicios de Seguridad con PGP

- Privacidad.
  - *Sólo aquellos que deben recibir un mensaje pueden leerlo.*
- Autenticación.
  - *El origen de un mensaje es comprobable.*
- Borrado seguro
  - *Un archivo es borrado escribiendo n veces sobre el sector*

Lámina 248 Dr. Roberto Gómez C.

Funciones de PGP

- Criptosistemas
  - 1) Convencional (Llave secreta)
  - 2) Llave Pública
- Firmas Digitales
- Compendios de Mensajes (huellas digitales)
- Administración de llaves
- VPN: Virtual Private Networks

Lámina 249 Dr. Roberto Gómez C.

Algoritmos usados por PGP

- Especificados en RFC 2440.
- En orden de preferencia son:
  - ElGamal y RSA para intercambio de llaves
  - triple DES, IDEA y CAST5 para encripción completa de mensajes.
  - DSA y RSA son usados para firmas digitales
  - SHA-1 y MD5 son usados para obtener huellas digitales
  - El programa shareware ZIP es usado para comprimir mensajes para su transmisión y almacenamiento.
- Compatibilidad de correo es lograda con el uso de conversión Radix-64.

Lámina 250 Dr. Roberto Gómez C.

Instalando PGP (MS Outlook)

- Extraer archivo ZIP
- Cerrar programas
- Ejecutar Setup.exe

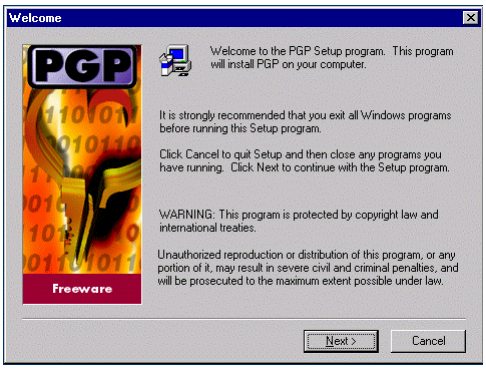


Lámina 251
Dr. Roberto Gómez C.

Manejo de llaves

- Generar llaves
- Importar llaves
- Exportar llaves
- Firmar una llave
- Ajustando el nivel de seguridad
- Revocando llaves
- Particionando llaves

Lámina 252
Dr. Roberto Gómez C.

Generando llaves

- Introducir nombre y correo
- Seleccionar tipo DH o RSA
- Seleccionar tamaño llave
  - más grande es mejor
  - más grande es más lento
- Seleccionar opción de expiración
  - un periodo determinado
  - indeterminado

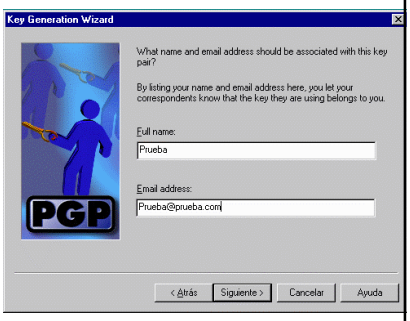


Lámina 253
Dr. Roberto Gómez C.

Generando llaves ...

- Dar una frase
  - escoger una buena frase
  - confirmar frase
- Enviar la llave al servidor (opcional)

En unix:

toto@kiko:1>**pgp -kg**

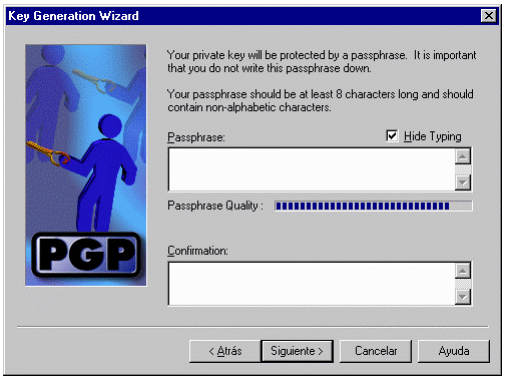


Lámina 254
Dr. Roberto Gómez C.

Importando llaveros existentes

- Cuando se pregunte el uso de llaves existentes responder [yes]
- Seleccionar los archivos .pkr y .skr a importar
- Después de la instalación:
  - menu Options de Edit de PGPKeys
  - asignar la llave secreta al archivo .skr
  - asignar la llave publica al archivo .pkr

Lámina 255 Dr. Roberto Gómez C.

Definiendo lugar llaves

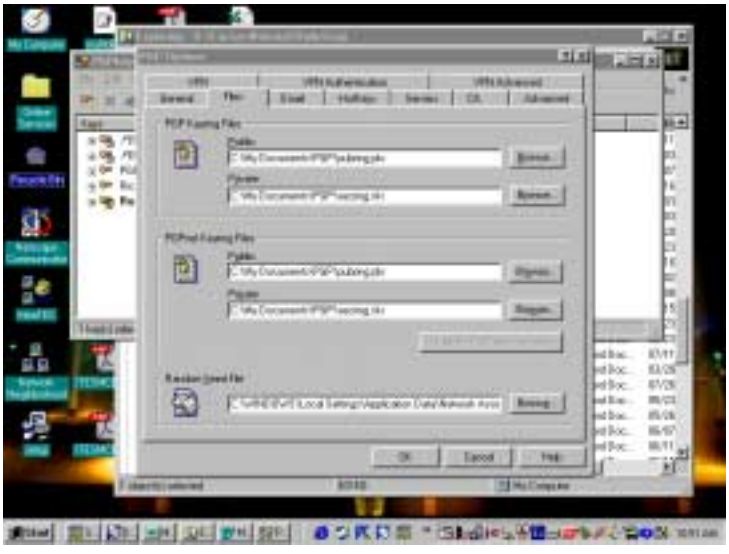


Lámina 256 Dr. Roberto Gómez C.

Exportando llaves públicas a servidores llaves

- Abrir PGPkeys.
- Seleccionar la llave a enviar y presionar botón derecho.
- Seleccionar enviar.
- Seleccionar servidor.

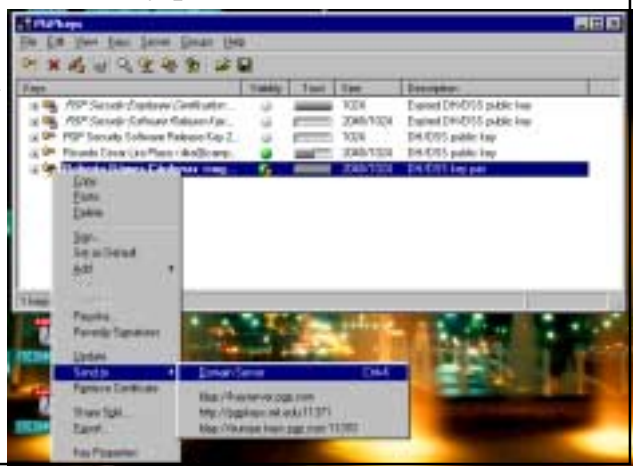


Lámina 257

Exportar llaves públicas a archivos o correo

- Abrir PGPkeys
- Seleccionar la llave
- Del menú de Edit seleccionar Copy (o dar ctrl-c)
- Abrir el archivo o el correo
- Seleccionar Paste
- El bloque de texto que representa la llave es pegada al objetivo
- Otra opción es seleccionar opcion Export de Keys de PGPkeys

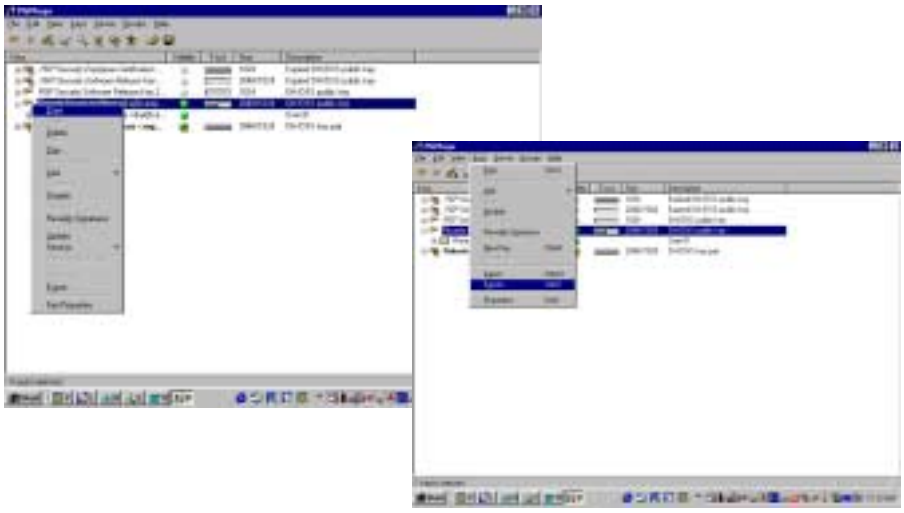
Lámina 258
Dr. Roberto Gómez C.

Ejemplo llave

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 7.0.3 for non-commercial use <http://www.pgp.com>

mQGiBDsSvdARBADaMEJC5APkTg7N8mSL1uBvwugX3qMEw12dPsUfAAbayhK9obV9
rapBewT+8d3Z6Pkace4zeoaHMidaVwjkkaHH9EQ4mHrzVaj2JS3bQu4YIDWfGB7f
ycKGpotoMIwhgVWrqtQbM5y6v/CZpowZ/LDgldeaACYwDvdzdE2dOVjRmwCg/8oY
2ShKzhwrwNeaGzvHWjMPqGsEAMmTPqPmG2+ZWojI4NywP0yfUodrilJNzkou8Lg0
TxkWz4B24km2q+JCxDC22Za6/7FI6FjdKFxsvQCOH3h2H9KrohyG8UOIea/xiFeO
GKQOZgJpQkpS6z74JDOuBzUVhf8W0BzVFOfygJEWCnBJBwwUm+PQD6nWss1g22uE
Wkg+BACLIOgIgMQHEyVbS7nQtUK+2++kkuafMIHkhD1ir66qT4Z2YFmx8dYwHhuH
5WW7Q6XlZ4fYZwNxWGyF5HOnKP1mWg7OKSBTjWqnooimGI+6o+nivPdncZP0eS6U
aTv38iH3omjVuH7q4xU021d10axmqpKYP0kwT1NoCwJXcrOeW7Q0Um9iZXJ0byBH
821leiBD4XJkZW5hcyA8cm9nb21lekBjYW1wdXMuY2VtLml0ZXNtLm14PokAWAQQ
EQIAGAUCOxK90AgLAwkIBwIBCgIZAQUbAwAAAAAKCRBXbZv9lLLoJd+LAJ0Tr2vl
4fhZ5uC9iFwOQfSONq8IwwCdHNFcmkRCfyT73uRbAj6RPj1GvEW5Ag0EOxK90BAI
APZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU6Y9AVfPQB8bLQ6mU
rfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXklnN/biudE/F/Ha8g8VH
MGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAWCvl9Ij9WE5J280gtJ3kkQc2
azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0/XwXV0OjHRhs3jMh
LLUq/zzhsSlAGBGNflSnCnLWhsQDGcgHKXrKlQzZlp+r0ApQmwJG0wg9ZqRdQZ+c
fL2JSyIZJrqrol7DVekyCzsAAgIIAKci2FNty+7XFOoaMJ7CNYS556Kx0nHflYWP
b+qw46TXBTtNnDJ0RiT/G2vePo3nL6FgaHQ/SJsKoFZvbpSeM1hTgAR97VE5y0j6
iJC1u9tM9B48ccAHlihpQLiyv49TAxk/Tp8buWjornM5+FH5J6ZCb5mikVRdtdQ8
iWQPjAuWTxnHUNEGwYah1GJK6C+yZZT90EDprvb8MqYkkBfgiI5Fd2Lmh6Nsppqz
bXAJw8u36HUJkdCZ6IKWUy4EMPo9X1TNFBHYd3IcE+34F1kKVtbz1syoSqyxYSf4
5x3H6uMZmDbRYKSc+rYwerAhVu4fkAXIwGisUewS/ZsvTaSPLpGJAEwEGBECAAwF
AjsSvdAFGwwAAAAACgkQV22b/ZSy6CWUCACgxIbD3+x/vMCNxPXBLwp/4XvKvWgA
oJxAsML1N7AgOkFBTZk5IXiUN65t
=VYg2
-----END PGP PUBLIC KEY BLOCK-----

Opciones para exportar llaves públicas



Importando llaves públicas de servidores

- Abrir PGPkeys
- Del menú de Server seleccionar Search
- Seleccionar el servidor
- Introducir opciones búsqueda
- Dar click a Search
- Con el botón derecho seleccionar la llave adecuada y selecionar importar al llavero local

Lámina 261
Dr. Roberto Gómez C.

Ejemplo importación

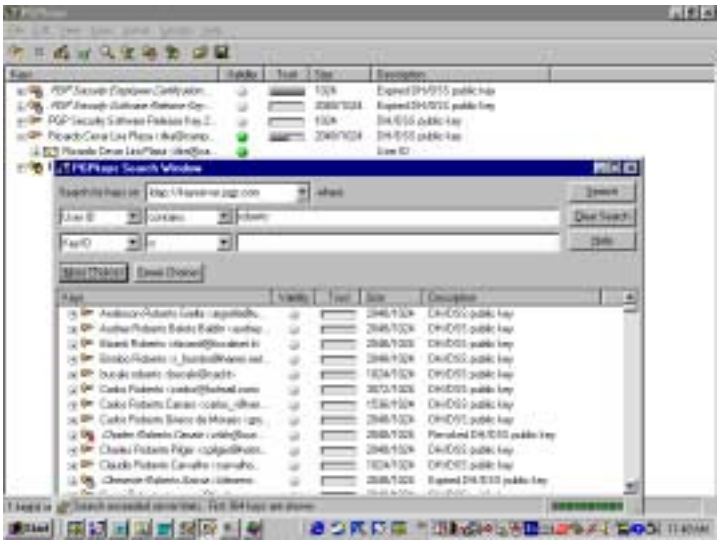


Lámina 262
Dr. Roberto Gómez C.

Respaldando llaves

- Exportar llave a un archivo o a una ubicación segura (CD, diskette, zip, etc.)
- O
  - respaldar archivos del llavero
  - copiar pubring.pkr
  - copiar secring.pkr
- Tener cuidado en la selección de la ubicación.
- No hay backdoor en PGP, si se pierden las llaves NO se puede recuperar la información encriptada.

Lámina 263 Dr. Roberto Gómez C.

¿¿Y en Unix???

- Agregar una llave al llavero
  ```
  pgp -ka archivo_llave [llavero]
  ```
- Suprimir una llave del llavero
  ```
  pgp -kr usuario_id [llavero]
  ```
- Copiar una llave del llavero
  ```
  pgp -kx usuario_id archivo_llave
            [llavero]
  pgp -kax usuario_id archivo_llave
                [llavero]
  ```

Lámina 264 Dr. Roberto Gómez C.

¿¿Y en Unix…???

- Ver el contenido del llavero

```
pgp -kv[v] [usuario_id] [llavero]
pgp keyfile
```

Lámina 265 Dr. Roberto Gómez C.

Validando llaves

- Abrir PGPkeys
- Seleccionar la llave a verificar
- Presionar botón derecho
- Seleccionar Key Properties
- Contactar al dueño de la llave
  - asegurarse de verificar su identidad
- Verificar la huella (fingerprint)
  - a través de las palabras
  - a través del número hexadecimal

Lámina 266 Dr. Roberto Gómez C.

Validando llaves con palabras

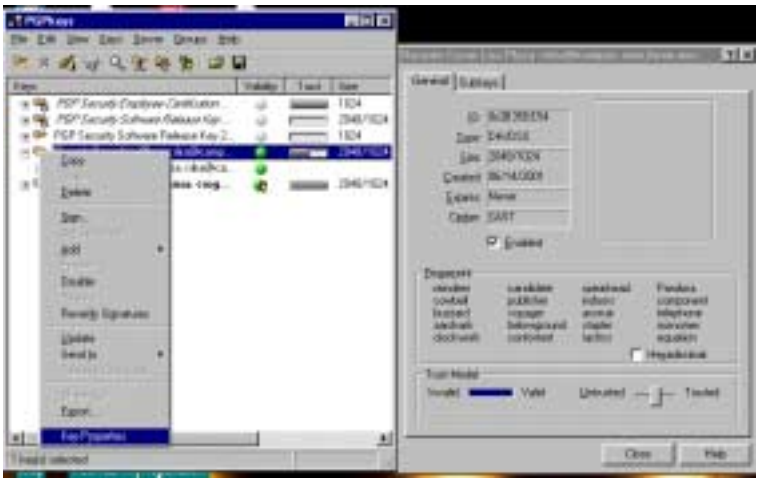


Lámina 267
Dr. Roberto Gómez C.

Firmando llaves

- Primero hay que verificar la llave
- Abrir PGPkeys
- Boton derecho de la llave seleccionada
- Seleccionar Sign
- Introducir la frase secreta
- Seleccionar ok

Lámina 268
Dr. Roberto Gómez C.

Ajustando el nivel de confianza

- Primero hay que verificar y firmar la llave.
- Decidir el nivel de confianza
  - cómo se adquirio y se verifico la llave
- Botón derecho en la llave y seleccionar la opción Key Propierties
- Ajustar el indicador al nivel de confianza deseado.

Lámina 269 Dr. Roberto Gómez C.

Revocando llaves

- Abrir PGPkeys
- Seleccionar la llave a revocar
- Estar seguros de que se desea revocar dicha llave!!!
- Botón derecho en esa llave y seleccionar la opción Revoke
- Introducir la frase secreta de la llave
- Confirmar la acción
  - aparecerá una X en el icono de la llave
  - al descripción mostrará revocado

Lámina 270 Dr. Roberto Gómez C.

Particionando llaves

- Aplicando el concepto de secretos compartidos.
- Botón derecho de la llave que se desea particionar
- Selecciona Split
- En la caja de diálogo de split introducir los nombres de las personas que van a compartir las llaves y sus frases secretas
- Seleccionar el número requerido para reconstruir la llave
- Seleccionar la ubicación de las partes de la llave
- Distribuir las partes a sus propietarios

Lámina 271 Dr. Roberto Gómez C.

Encripción/Decripción

- Encripción
- Decripción
- Firmas
- Verificación de firmas
- Combinaciones

Lámina 272 Dr. Roberto Gómez C.

Encriptando y firmando correos (consejos generales)

- Asegurarse de que se tiene la llave del destinatario
- Realizar operaciones de validación y firma
- Si se firma, asegurarse de que el destinatario cuenta con una copia de su llave de firma
  - ellos deben realizar verificación y firma
- Seleccionar entre enviar via Attachment o de forma automática vía Outlook

Lámina 273 Dr. Roberto Gómez C.

Encriptando y firmando correos (usando MS Outlook)

- Crear un nuevo mensaje
- Seleccionar opciones Sign y Verify del menú de PGP
  - usar el botón de la barra
- Introducir el mensaje (y añadir attachments)
- Introducir dirección del destinatario y enviar
- Seleccionar las llaves a usar para encriptar
  - las que pertenecen al recipiente
  - PGPkeys seleccionara la llave apropiada si puede
- Si se firma el archivo
  - seleccionar la llave para firmar e introducir la frase

Lámina 274 Dr. Roberto Gómez C.

Encriptando y formando correos (usando attach)

- Escribir mensaje en un archivo
  - asegurarse que el destinatario pueda leer dicho archivo (i.e. cuente con el programa)
- Del botón derecho del archivo seleccionar encrypt o encrypt and sign
- Seleccionar la(s) llave(s) a encriptar
- Seleccionar la llave de firma
- Introducir la frase de la llave con la que se va a firmar

Lámina 275 Dr. Roberto Gómez C.

Ejemplo encripción/firma

- Attach el mensaje encriptado a su correo electrónico y enviarlo como normalmente se hace
  - sólo el contenido del archivo en attach es seguro

Lámina 276 Dr. Roberto Gómez C.

Decriptando y verificando e-mail

- Determinar el método de envío
  - si el mensaje aparece como un archivo en attach con una extensión .asc
  - utilizar el método de attach del archivo

Lámina 277 Dr. Roberto Gómez C.

Decripción/verificación automática

- Abrir el mensaje en su correo electrónico
- Seleccionar Decrypt Verify del menú PGP
  - usar el button bar
- Introducir la frase secreta de la llave
- El mensaje decriptado debe aparecer en el cuadro de diálogo del correo

Lámina 278 Dr. Roberto Gómez C.

Decripción y verificación en attach

- Abrir el mensaje con su correo
- Copiar el archivo en attach al disco duro
- Botón derecho en el archivo
  - escoger Decrypt verify del menú de PGP
- Seleccionar la ubicación del archivo decriptado.
- Borrar el archivo (wipe) si así se desea

Lámina 279 Dr. Roberto Gómez C.

Ejemplo decripción

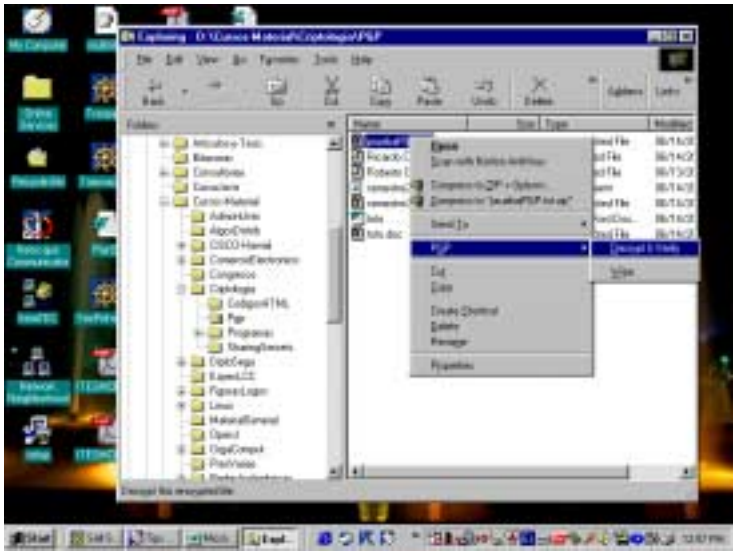


Lámina 280 Dr. Roberto Gómez C.

¿Y en Unix?

- Encriptado (convencional)
  ```
  pgp -c archivo
  ```
- Decriptado (convencional)
  ```
  pgp archivo [-o arch_salida]
  ```
- Encriptado (llave pública)
  ```
  pgp -e archivo receptor_id
  ```
- Decriptado (llave pública)
  ```
  pgp archivo [-o arch_salida]
  ```

Lámina 281 Dr. Roberto Gómez C.

¿Y en Unix...?

- Firma de un documento
  ```
  pgp -s documento [-u tu_id]
  ```
- Comprobación de la firma
  ```
  pgp archivo [-o arch_salida]
  ```
- Firma y encriptado de un documento
  ```
  pgp -se documento receptor_id [-u tu_id]
  ```
- Comprobación de la firma y decriptado
  ```
  pgp archivo [-o arch_salida]
  ```

Lámina 282 Dr. Roberto Gómez C.

Reuniendo llaves

- Decriptar o firmar usando una llave particionada.
- Aparece cuadro diálogo de Key Share Collection
- Click sobre los archivos compartidos
- Seleccionar los archivos .shf a ser usados
- Introducir la frase secreta
- Repetir seleccionando los archivos e introduciendo el resto de las frases.

Lámina 283 Dr. Roberto Gómez C.

Uso de criptologia convencional

- Destinatario no necesita conocer PGP
- Seleccionar archivo a encriptar
- Botón derecho sobre el archivo y seleccionar Encrypt del menú de PGP
- Cuando aparezca la llave seleccionar opciones:
  - Use conventional encryption
  - Self Decrypting Archive
- Introducir la frase secreta usada y encriptar el archivo.
  - necesario que los dos conozcan la frase

Lámina 284 Dr. Roberto Gómez C.

Ejemplo encripción convencional

Lámina 285 Dr. Roberto Gómez C.

Uso de borrado seguro

- Asegurarse de que el archivo no se necesita.
- Botón derecho del archivo a borrar
- Seleccionar Wipe del Menú de PGP
- Click OK
- Es posible ajustar el número de pasadas del General Tab del menú de opciones de la ventana de diálogo.
  - elegir Options del menú Edit de PGPkeys
  - mas es mejor y más lento

Lámina 286 Dr. Roberto Gómez C.

Desventajas PGP

- Fuera de Estados Unidos, debe usarse la versión internacional.

- En Estados Unidos, no puede usarse la versión internacional.

Lámina 287 Dr. Roberto Gómez C.

Integrando PGP al correo electrónico

- PGP proporciona plug-ins para integrar PGP a los programas de correo más comunes:
  - Microsoft Outlook 97/98/2000,
  - Microsoft Outlook Express 4.x/5.x, Qualcomm Eudora 4.x
  - Claris Emailer 2.x.
- Para usuarios de Emacs en sistemas Unix, existe un Mailcrypt disponible en:
  - http://cag-www.lcs.mit.edu/mailcrypt/
- El MIT pone a la disposición de todo el mundo un servidor de llaves públicas PGP.

Lámina 288 Dr. Roberto Gómez C.

Integrando PGP al correo electrónico

- Para usar el correo MH de Unix, exmh es una interfaz de sistema de X Windows para el programa de correo MH que porporciona soporte PGP.
- Offline AutoPGP es un paquete de encripción de correo electrónico para ser usado con PGP y lectores de correo fuera de línea en máquinas DOS.

Lámina 289 Dr. Roberto Gómez C.

Bajo la lupa

- Se usa la llave actual (publica/privada) seleccionada para encriptar el mensaje.
- No realmente:
  - Llave pública es muy lenta para encriptar el mensaje.
  - Las llaves DH o RSA son usadas para "negociar" una llave de sesión.
  - Llaves de sesión son usadas para encriptar el mensaje.

Lámina 290 Dr. Roberto Gómez C.

VPNs y PGP

- VPN:Virtual Private Network
  - es un canal de comunicación seguro definido sobre un medio inseguro de comunicación (generalmete Internet)
- PGPnet
  - posible definir una VPN entre dos organismos
- Posible crear un VPN a nivel
  - host
  - subred
  - gateway
- Posible definir un intercambio de llaves en condiciones seguras.

Lámina 291 Dr. Roberto Gómez C.

VPNs y PGP

- Posibilidad de bloquear comunicaciones, activar bitácoras (logs), basado en el concepto de SA (Security Association)
  - acuerdo que contiene los términos para establecer una comunicación segura entre dos máquinas
  - se crea la primera vez que una máquina se conecta con otra
  - descrine como una máquina que se va a comunicar con otra: tipo de encripción, duración de la asociación y método de autenticación

Lámina 292 Dr. Roberto Gómez C.

Referencias


Applied Cryptography, Protocols, Algorithms and Source Code in C, Bruce Schneier, Ed. John Wiley & Sons, 1996


Handbook of applied Cryptography, A Menezes P van Oorsschot and Vanston, CRC Press, 1996 (http://www.cacr.math.uwaterloo.ca/hac)


Cryptography in C and C++, by Michael Welschenbach, APress, 2001


Cryptography and Network Security, Principles and Practice, William Stallings, Ed. Prentice Hall, 2da. edición, 1999


The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptography by Simon Singh, Anchor edition, 2000

Lámina 293
Dr. Roberto Gómez C.