

Introducción a la criptología

Roberto Gómez Cárdenas

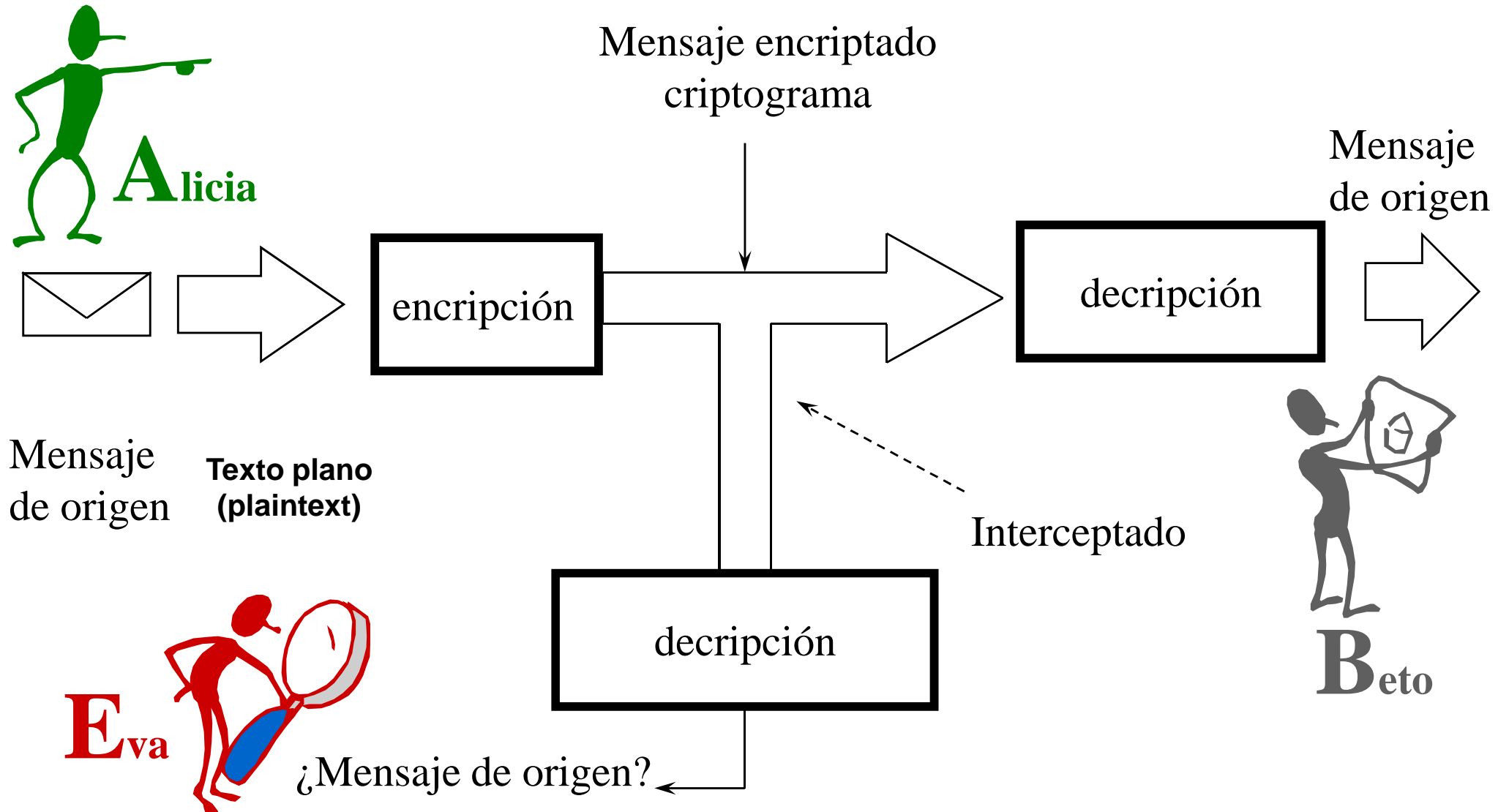
rogomez@itesm.mx

<http://cryptomex.org>

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*.

Proceso encriptación/decriptación



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

- 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.

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

- 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 encriptación pueden ser descifrados en un tiempo NO muy grande.

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 Kerckhoffs

Procedimientos clásicos de encriptación

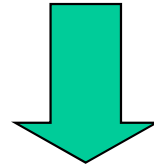
- Primeros metodos criptograficos
 - epoca romana hasta siglo XX
- Basados en dos técnicas
 - transposición
 - substitución

La transposición

- Principio:
 - “barajar” los símbolos del mensaje original colocándolos 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 de transposición

T R A N S P O S I C I O N

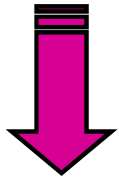


S I N O I O N A C T R P S

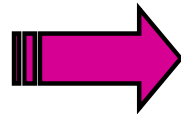
- Principio:
 - “barajar” los símbolos del mensaje original colocándolos en un orden distinto, de manera que el criptograma contenga los mismos elementos del texto claro, pero colocados de tal forma que resulten incomprensibles

Ejemplos transposición

EN UN LUGAR DE LA MANCHA
DE CUYO NOMBRE NO
QUIERO ACORDARME



E	N	U	N	L	U	G
A	R	D	E	L	A	M
A	N	V	C	H	A	C
U	Y	O	N	O	M	B
R	E	N	O	Q	U	I
E	R	O	A	C	O	R
D	A	R	M	E	X	X



E	N	U	N	L	U	G
A	R	D	E	L	A	M
A	N	V	C	H	A	C
U	Y	O	N	O	M	E
R	E	N	O	Q	U	I
E	R	O	A	C	O	R
D	A	R	M	E	X	X

**EAAURED NRNYERA UDVONOR
NECNOAM LLHOCQE UAAMUOX
GMCBIRX**

**GMCBIRX UAAMUOX LLHOCQE
NECNOAM UDVONOR NRNYERA
EAAURED**

E	N	U	N	L	U	G
A	R	D	E	L	A	M
A	N	V	C	H	A	C
U	Y	O	N	O	M	B
R	E	N	O	Q	U	I
E	R	O	A	C	O	R
D	A	R	M	E	X	X

**EANARUU NDNRYVE LEECLU
DRNNHAG AOOAMR AQMCMCU
BEOIXRX**

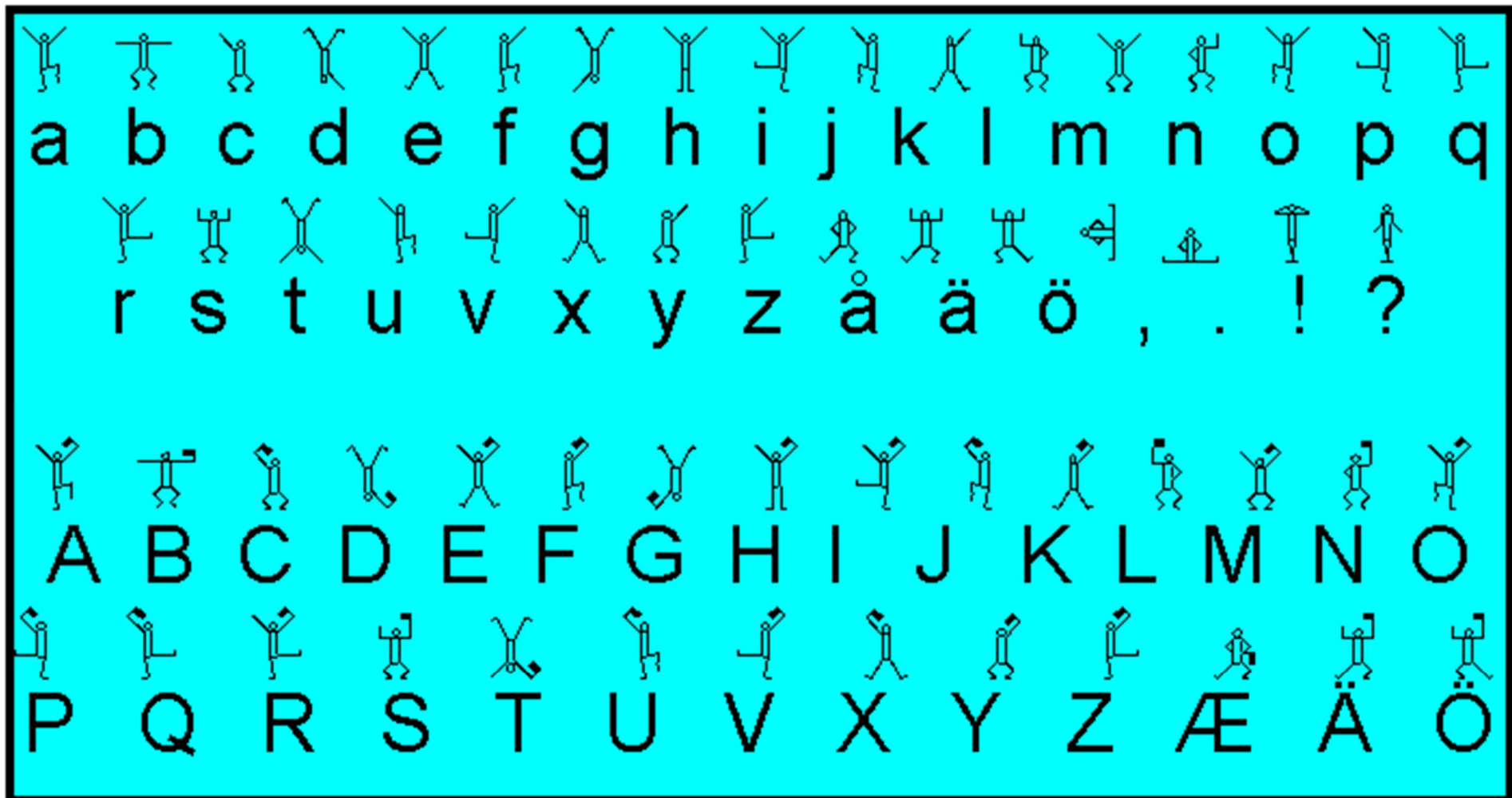
**ENAUAN DNULEVY RULCOEE
GAHNNRD MAOOAC MQARBUCM
IOERXX**

E	N	U	N	L	U	G
A	R	D	E	L	A	M
A	N	V	C	H	A	C
U	Y	O	N	O	M	B
R	E	N	O	Q	U	I
E	R	O	A	C	O	R
D	A	R	M	E	X	X

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).

Criptosistema de Adventures Dancing Men



Cifrado de Cesar

Alfabeto original

correspondencias

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

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

*Alfabeto
desfasado*

Mensaje:

VENI

VIDI

VICI

Llave:

DDDD

DDDD

DDDD

Criptograma:

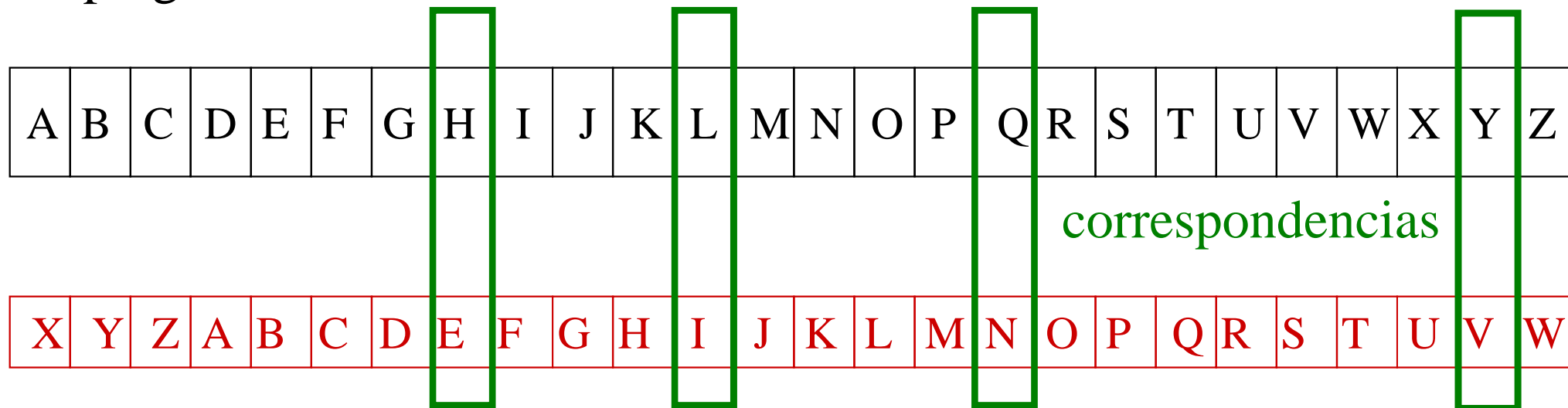
YHQL

YLGL

YLFL

Descifrando en Cesar

criptograma



Criptograma:

YHQL

YLGL

YLFL

Llave:

DDDD

DDDD

DDDD

Mensaje:

VENI

VIDI

VICI

Análisis por frecuencia

Word Frequency Count In Multiple Text & HTML Files ...

File(s)

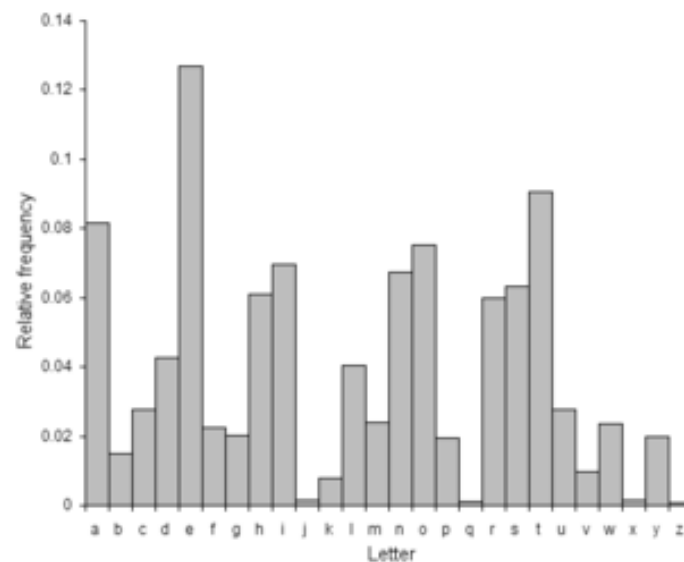
Add File(s) Add All File(s) In Folder

Count Word Frequency in Text File(s) Count Word Frequency in MS Word File(s)

Ignore letter case Sort by frequency

Results

Save Results As List Clear List

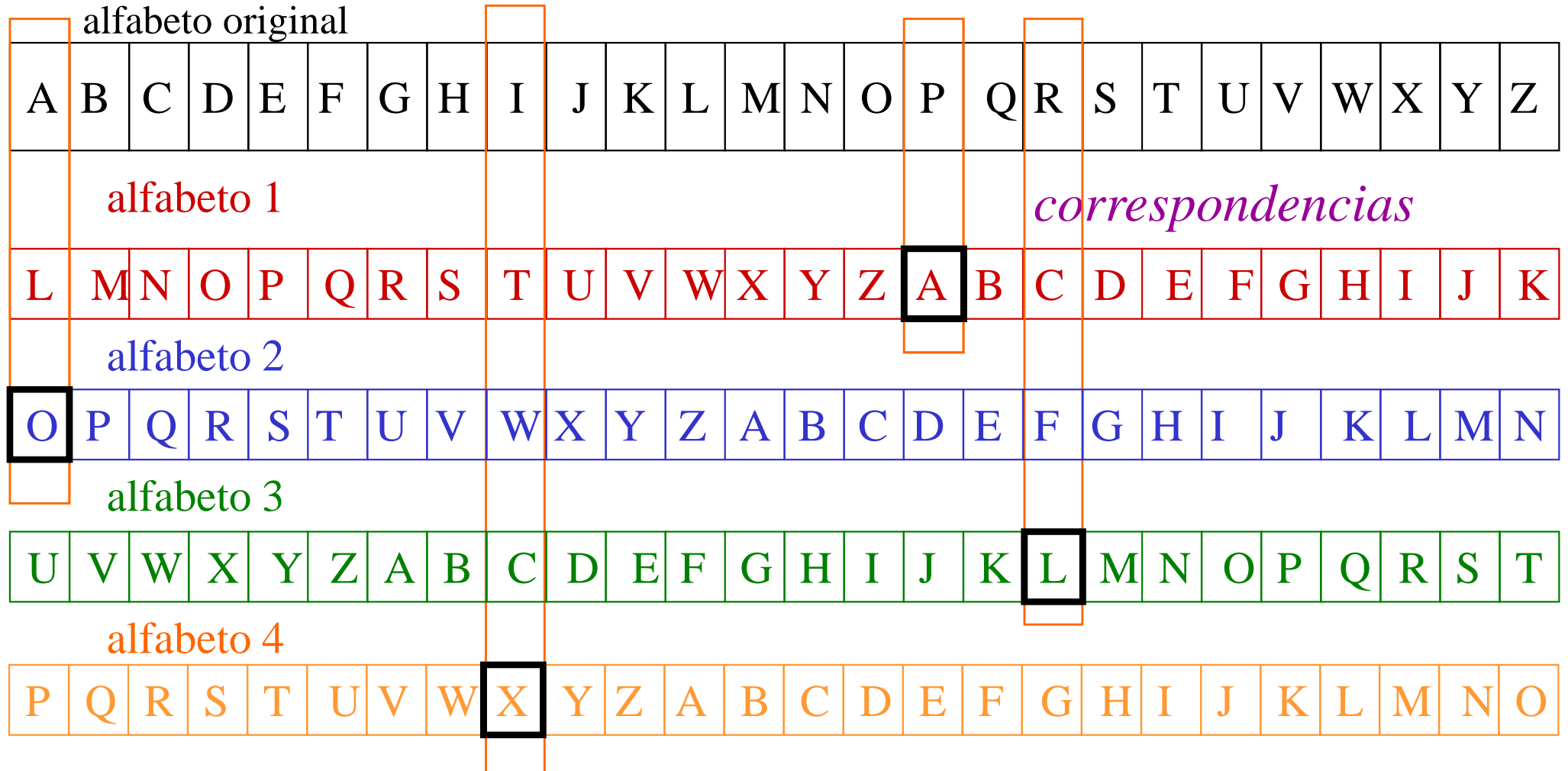


Letter	French	German	Spanish	Portuguese	Esperanto	Italian	Turkish	Swedish	Polish	Toki Pona	Dutch
a	7.636%	6.51%	12.53%	14.63%	12.12%	11.74%	11.68%	9.3%	8.0%	17.2%	7.49%
b	0.901%	1.89%	1.42%	1.04%	0.98%	0.92%	2.95%	1.3%	1.3%	0.0%	1.58%
c	3.260%	3.06%	4.68%	3.88%	0.78%	4.5%	0.97%	1.3%	3.8%	0.0%	1.24%
d	3.669%	5.08%	5.86%	4.99%	3.04%	3.73%	4.87%	4.5%	3.0%	0.0%	5.93%
e	14.715%	17.40%	13.68%	12.57%	8.99%	11.79%	9.01%	9.9%	6.9%	7.4%	18.91%
f	1.066%	1.66%	0.69%	1.02%	1.03%	0.95%	0.44%	2.0%	0.1%	0.0%	0.81%
g	0.866%	3.01%	1.01%	1.30%	1.17%	1.64%	1.34%	3.3%	1.0%	0.0%	3.40%
h	0.737%	4.76%	0.70%	1.28%	0.38%	1.54%	1.14%	2.1%	1.0%	0.0%	2.38%
i	7.529%	7.55%	6.25%	6.18%	10.01%	11.28%	8.27%*	5.1%	7.0%	14.8%	6.50%
j	0.545%	0.27%	0.44%	0.40%	3.50%	0.00%	0.01%	0.7%	1.9%	3.0%	1.46%
k	0.049%	1.21%	0.01%	0.02%	4.16%	0.00%	4.71%	3.2%	2.7%	5.1%	2.25%
l	5.456%	3.44%	4.97%	2.78%	6.14%	6.51%	5.75%	5.2%	3.1%	10.2%	3.57%
m	2.968%	2.53%	3.15%	4.74%	2.99%	2.51%	3.74%	3.5%	2.4%	4.4%	2.21%
n	7.095%	9.78%	6.71%	5.05%	7.96%	6.88%	7.23%	8.8%	4.7%	11.6%	10.03%
o	5.378%	2.51%	8.68%	10.73%	8.78%	9.83%	2.45%	4.1%	7.1%	7.7%	6.06%
p	3.021%	0.79%	2.51%	2.52%	2.74%	3.05%	0.79%	1.7%	2.4%	3.7%	1.57%

La tabla de Viginere

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

Enviando el mensaje



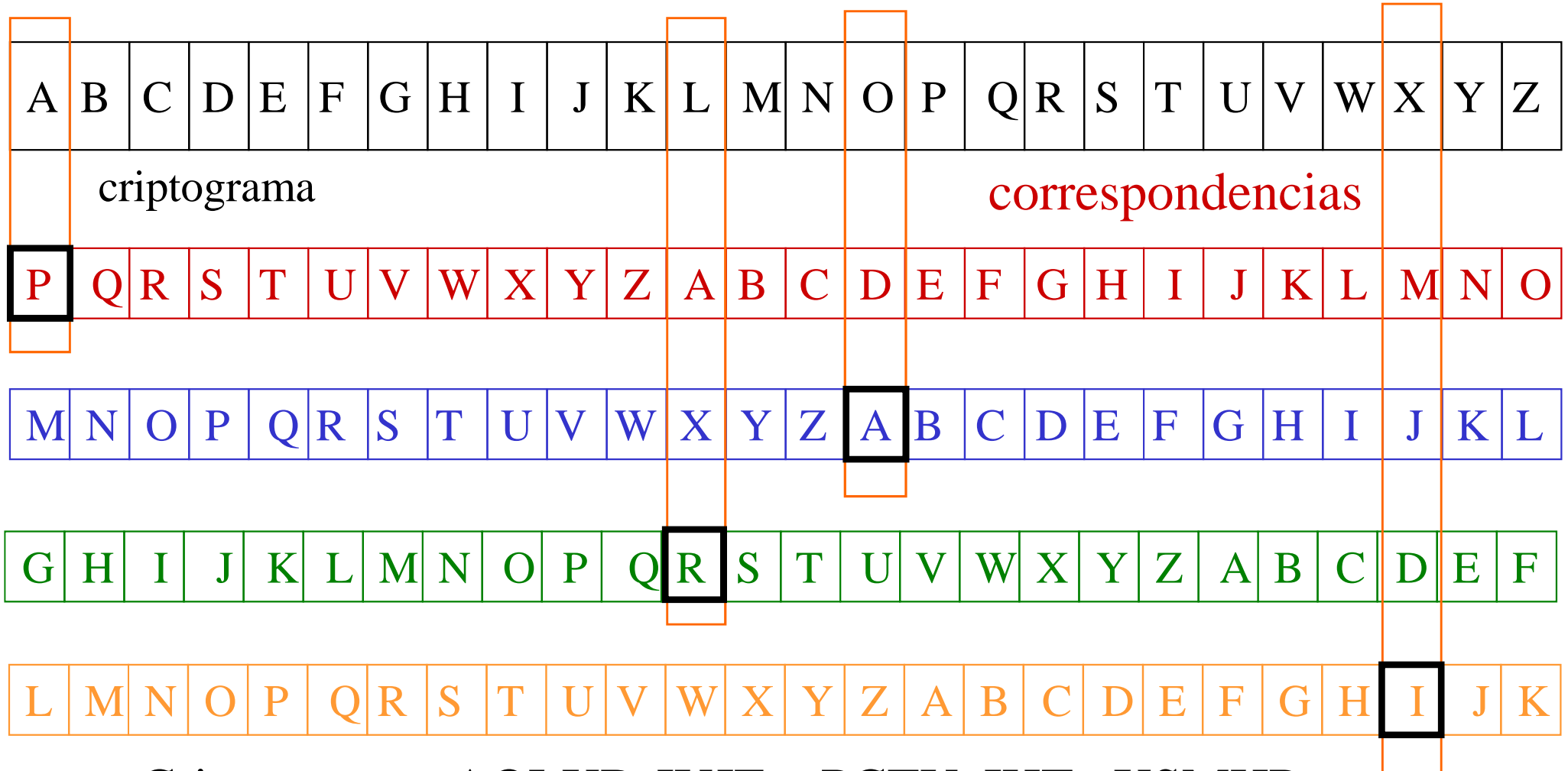
Mensaje: PARIS VAUT BIEN UNE MESSE

Llave: LOUPL OUPL OUPL OUP LOUPL

Criptograma: AOLXD JUJE PCTY IHT XSMHP



Recuperando el mensaje



Criptograma: AOLXD JUJE PCTY IHT XSMHP

Llave: LOUPL OUPL OUPL OUP LOUPL

Mensaje: PARIS VAUT BIEN UNE MESSE

Un criptograma resultado de Vigenere

WUBEF IQL ZURMVOFEHMYMWT
IXCGTMP IFKRZUPMVO IRQMM
WOZMPULMBNYVQQQMVMVJLE
YMHFEFNZ PSDLP PSDL PEVQM
WCXYMDAVQEEFIQCAYTQOWC
XYMWMSEMEFCFWYEYQETRLI
QYCGMTWCWFBSMYFPLRXTQY
EEXMRULUKSGWFPTLRQAERL
UVPMVYQYCXTWFQLMTELSFJ
PQEHMOZCIWCIWFPZSLMAEZ
IQVLQMZVPPXAWCSMZMORVG
VVQSZETRLQZPBJAZVQIYXE
WWOICCGDWHQMMVOWSGNTJP
FPPAYBIYBJUTWRLQKLLMD
PYVACDCFQ NZPIFPPKSDVPT
IDGXMQQVEBMQA LKEZMGCVK
UZK IZBZ LIUAMMVZ

Encontrando patrones

WUB**EFI**QL ZURMV OFEHMYMWT
IXCGTMP IFKRZUPMVO IRQMM
WOZMPULMBNYVQQQMVMVJLE
YMHFEFNZ **PSDLP PSDL**PEVQM
WCXYMDAVQE**EFIQ**CAYTQOWC
XYMWMSEMEFCFWYEQ**ETRLI**
QYCGMTWCWFBSMYFPLRXTQY
EEXMRULUKSGWFPTLRQAERL
UVPMVYQYCXTWFQLMTELSFJ
PQEHMOZCIWCIWFPZSLMAEZ
IQVLQMZVPPXAWCSMZMORVG
VVQSZ**ETRL**QZPBJAZVQIYXE
WWOICCGDWHQMMVOWSGNTJP
FPPAYBIYBJUTWRLQKLLMD
PYVACDCFQ NZPIFPPKSDVPT
IDGXMQQVEBMQA LKEZMGCVK
UZKIZBZLIUAMMVZ

Aplicando análisis por frecuencia a las “primeras letras”

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

Aplicando análisis por frecuencia a las “segundas letras”

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

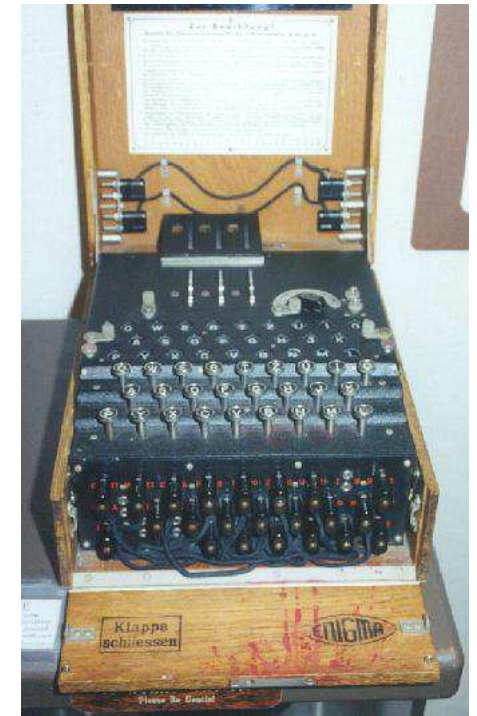
Otros criptosistemas clásicos

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



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



Confusión vs difusión

- La principal amenaza criptoanalítica proviene de la alta redundancia de la fuente.
- Según Shannon, la criptografía se debe basar en dos principios, confusión y difusión que, trabajando en conjunto, puedan proveer de la seguridad deseada
- Difusión
 - procura ocultar las estadísticas que puedan aparecer en un mensaje
- Confusión
 - se fundamenta en la modificación de los símbolos del mensaje original

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 sustitución y transposición
 - elementos del mensaje son substituidos por otros elementos, o sus posiciones son intercambiadas o ambas

Transposición en la computadora

- Convertir mensaje a ASCII

Texto claro:

HELLO = 1001000 1000101 1001100 1001100 1001111

- Transposición: intercambiar las letras en un orden predeterminado

Texto claro:

HELLO = 10010001000101100110010011001001111

Criptograma:

LHOEL = 10011001001000100111110001011001100

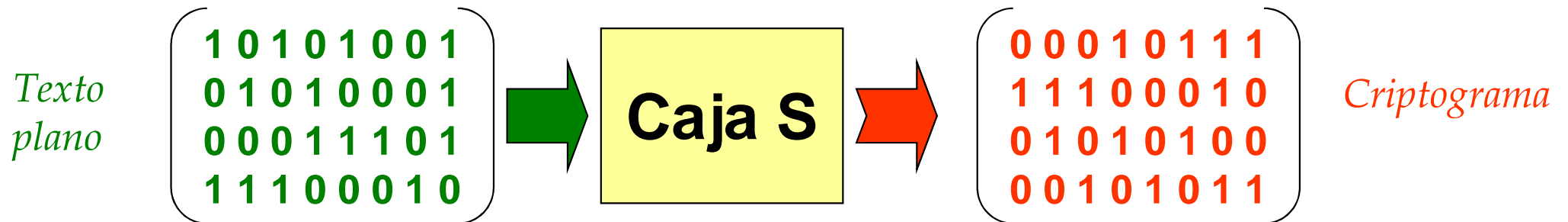
- La transposición puede darse a nivel de bits

Letra original: 1001000

Letra encriptada: 0010010

Substitución en la computadora

- Conjunto de bits es sustituido por otro conjunto de bits.
- El mapeo se efectúa a través de una tabla (p.e. caja S) o una operación matemática (que cuenta con una inversa) sobre el conjunto original de bits (p.e. pseudo transformada de Hadamard)



Utilizando una llave: la función xor

- 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

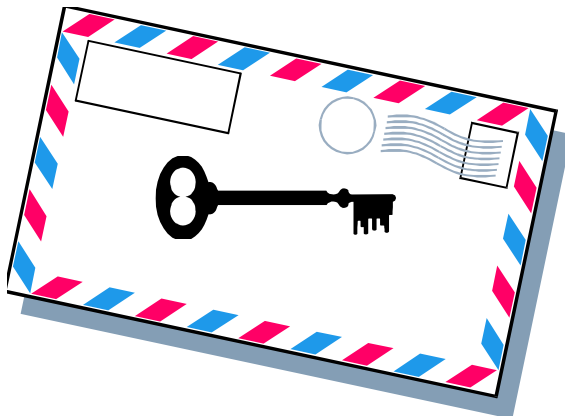
Texto ASCII: 10010001000101100110010011001001111

Llave: 10001001000001101011010010011000100

Criptograma: 00011000000100001101000001010001011

- 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
 - son propios de la criptografía clásica o criptografía de llave secreta
- Métodos asimétrico
 - llave encriptado es diferente a la de decriptado
 - corresponden a la criptografía de la llave pública, introducida por Diffie y Hellman en 1976

Algoritmos encriptación simétricos

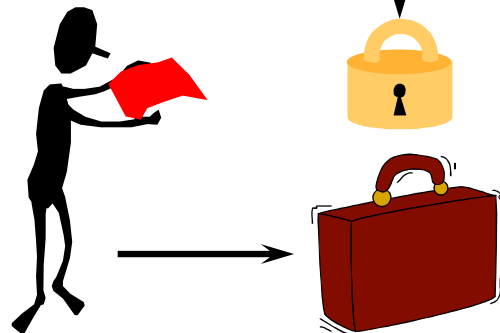


Encriptación llave secreta

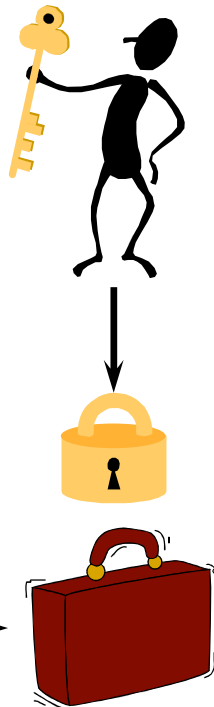
3. Beto asegura la caja con la llave de la caja fuerte.

5. Alicia desasegura la caja con un duplicado de la llave de la caja fuerte.

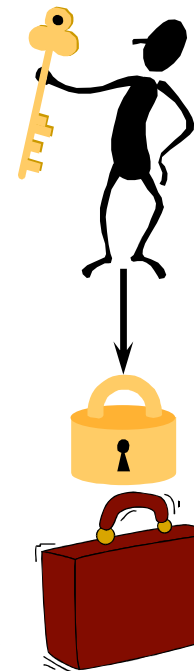
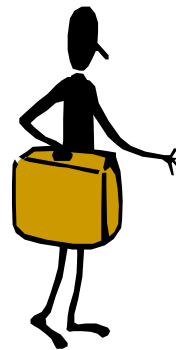
1. Beto escribe documento



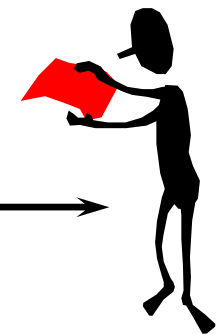
2. Beto coloca el documento en la caja fuerte



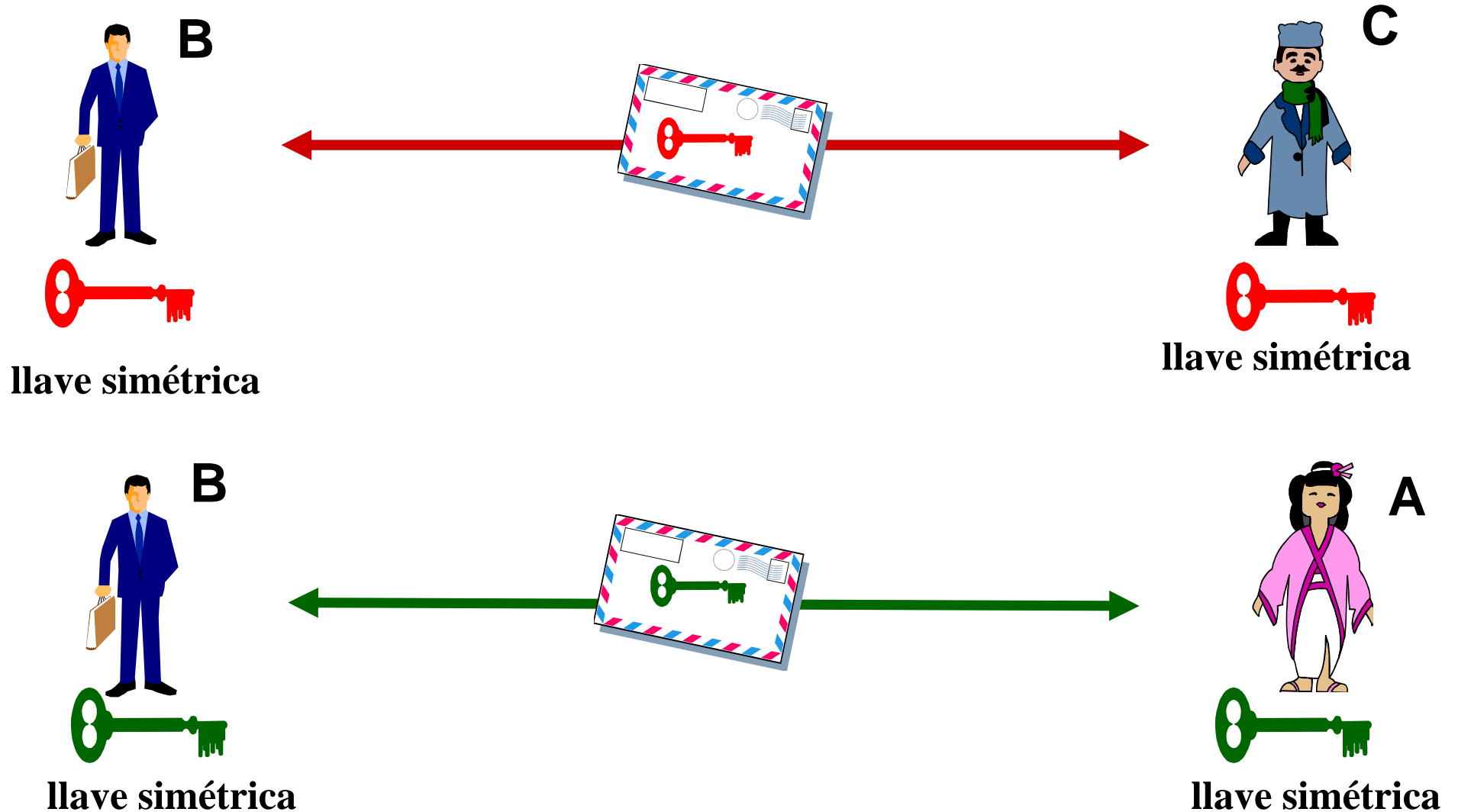
4. La caja se transporta hacia Alicia



6. Alicia obtiene el documento.



Esquema general encriptación llave secreta

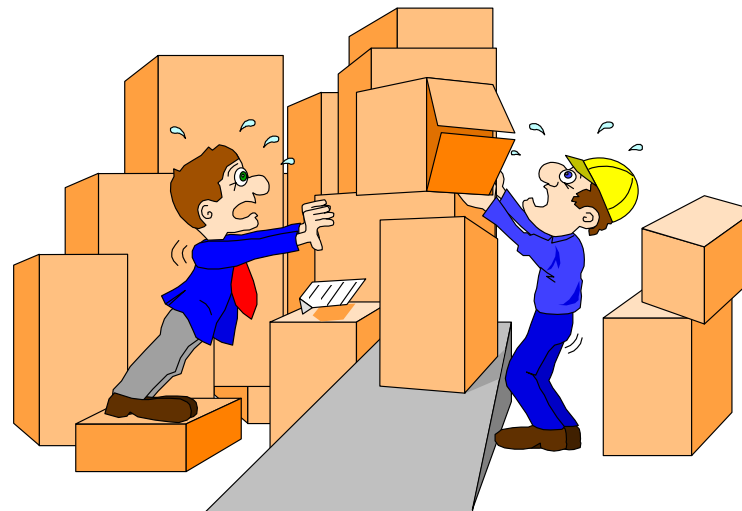


Clasificación métodos encriptación simetricos

- Encriptación en flujo



- Encriptación en bloques



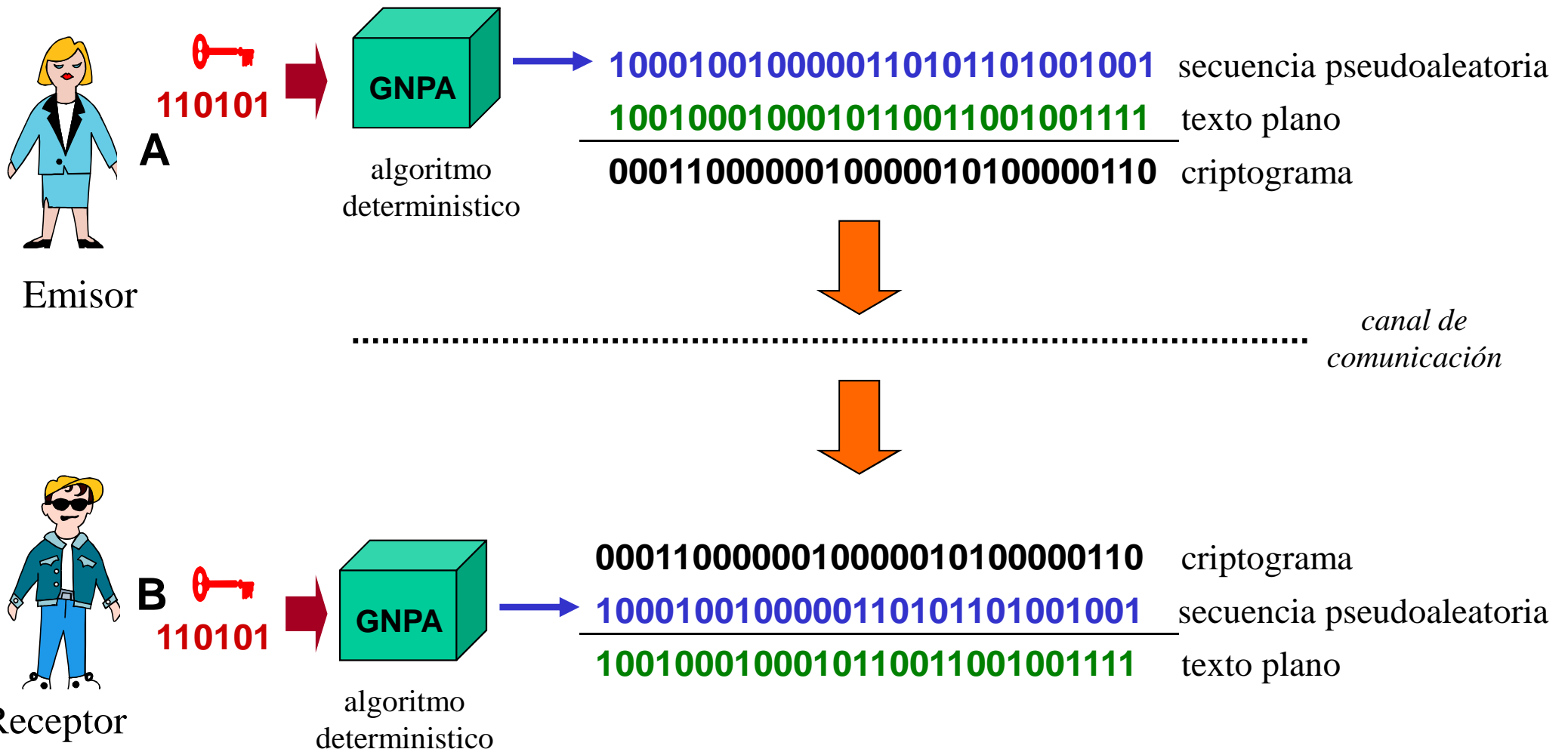
Encriptado en flujo

- En inglés: stream ciphers.
- Se genera una secuencia larga e imprevisible de dígitos binarios a partir de una llave corta
 - la llave debe ser la misma para emisor y receptor
 - criptosistema simétrico
- La secuencia se suma módulo 2 con el texto claro (emisión) o con el criptograma (recepción)
- Es rápido y simple

Ejemplo envío/recepción

Mensaje a enviar: HOLA

HOLA = 1001000100010110011001001111

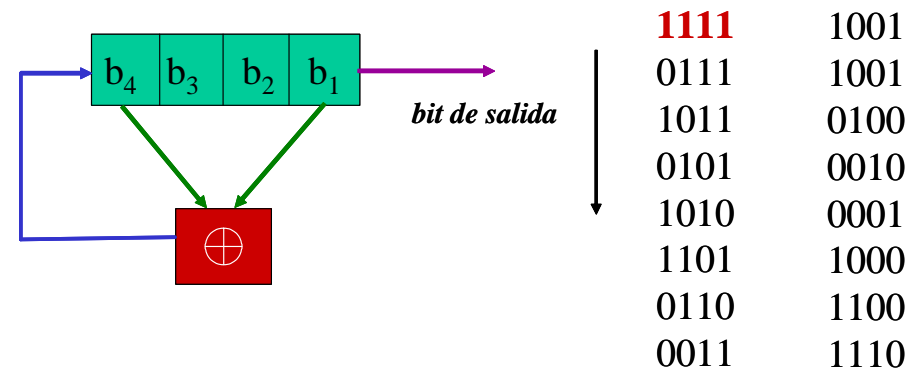


Implementación



- A nivel hardware
 - Feedback Shift Registers

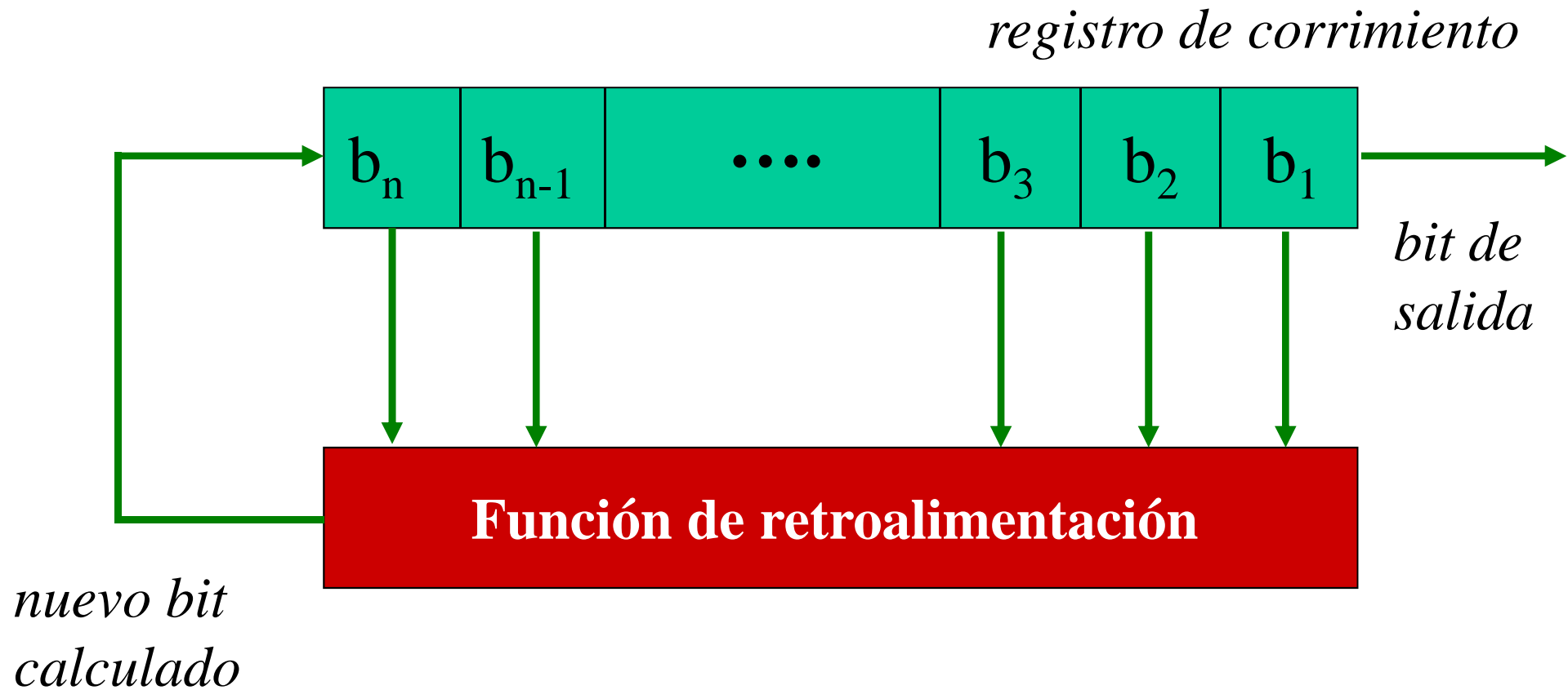
- A nivel software
 - RC4



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.

Esquema general Feedback Shift Registers

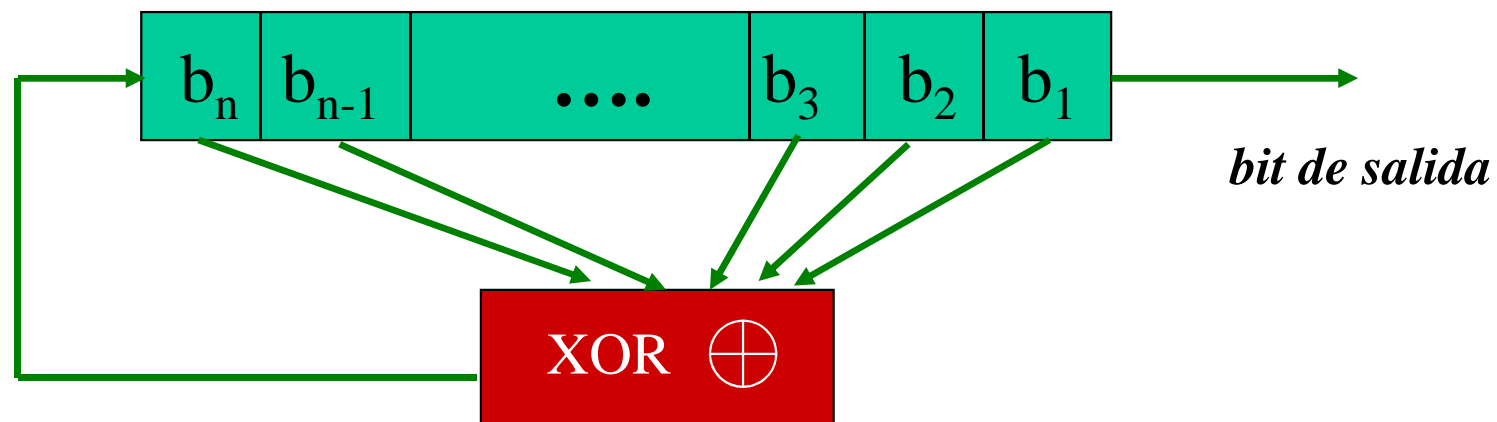


La función de retroalimentación

- De acuerdo a la función de retroalimentación podemos encontrar:
 - Registros de desplazamientos realimentados linealmente (LFSR)
 - Registros de desplazamiento realimentados no linealmente (NLFSR)
 - Registros de desplazamiento realimentados con carries (FCSR)
 - Combinaciones de los anteriores

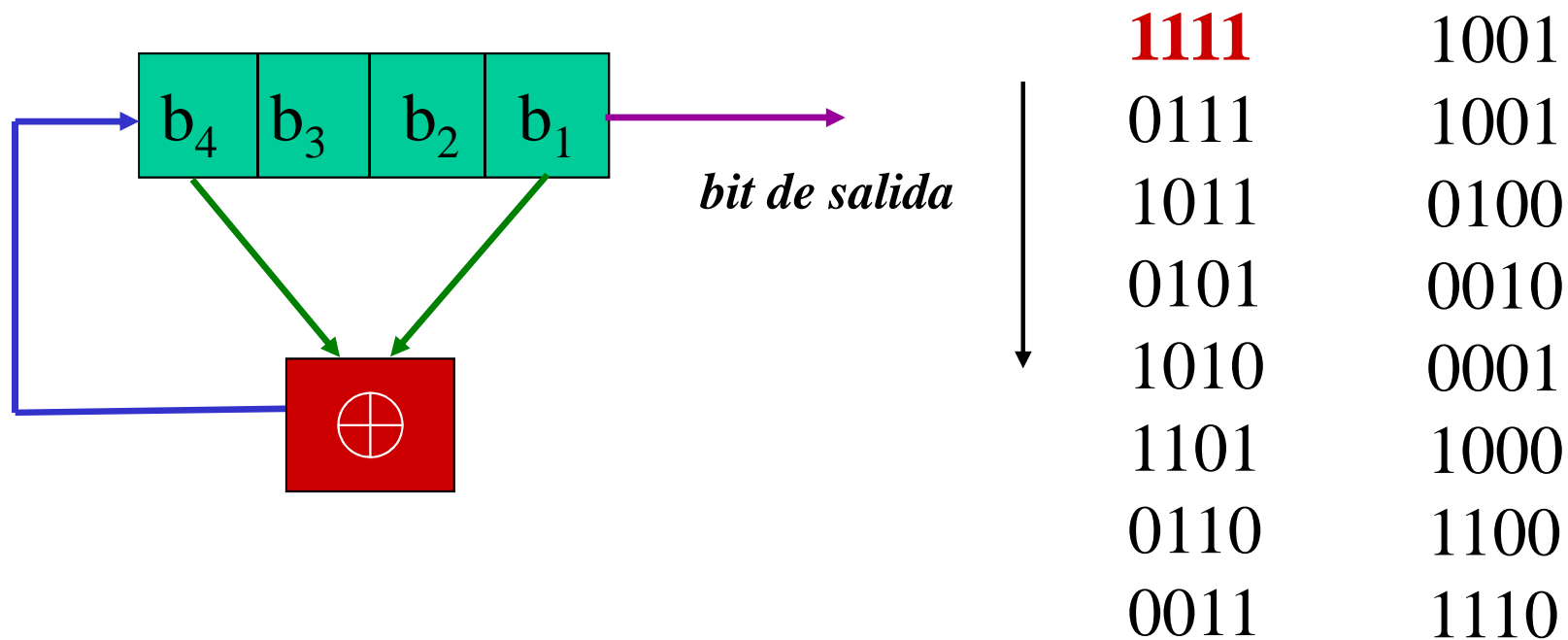
Registros de desplazamientos realimentados linealmente

- 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 denomina tap register (secuencia de entrada)



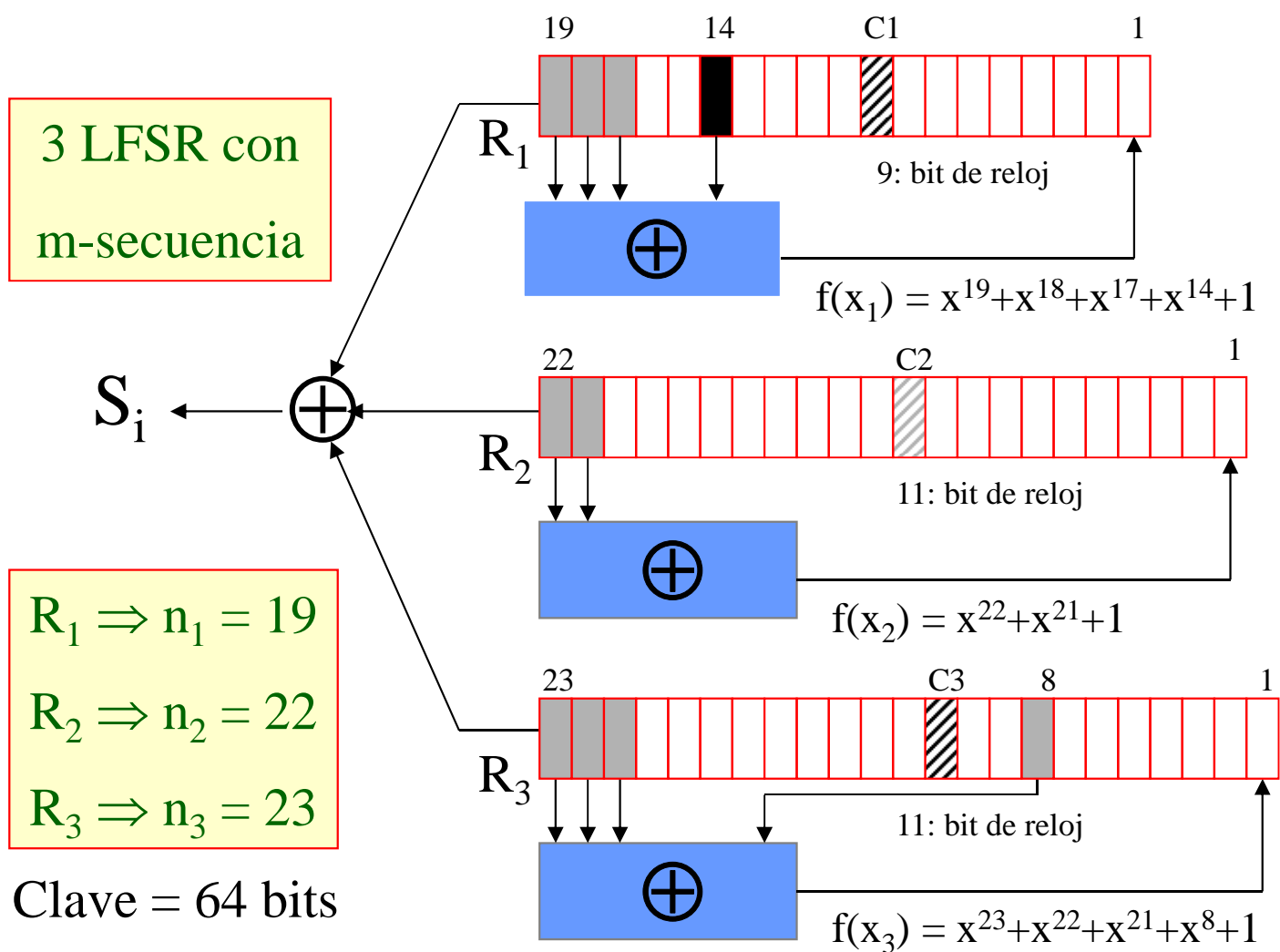
Ejemplo LFSR

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



- La secuencia de salida es: **111101011001000...**

Ejemplo encriptación flujo: A5/1



Una función mayoría entre C_1 , C_2 y C_3 hace que sólo los registros en los que coincide el bit con ese valor produzcan desplazamiento. En cada paso habrá dos o tres registros en movimiento.

El generador RC4

- RC4 es un criptosistema 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.

El mensaje

Newsgroups: sci.crypt,alt.security,comp.security.misc,alt.privacy
From: sterndark@netcom.com (David Sterndark)
Subject: RC4 Algorithm revealed.
Message-ID: <sternCvKL4B.Hyy@netcom.com>
Sender: sterndark@netcom.com
Organization: NETCOM On-line Communication Services (408 261-4700 guest)
Date: Wed, 14 Sep 1994 06:35:31 GMT

I am shocked, shocked, I tell you, shocked, to discover that the cypherpunks have illegally and criminally revealed a crucial RSA trade secret and harmed the security of America by reverse engineering the RC4 algorithm and publishing it to the world.

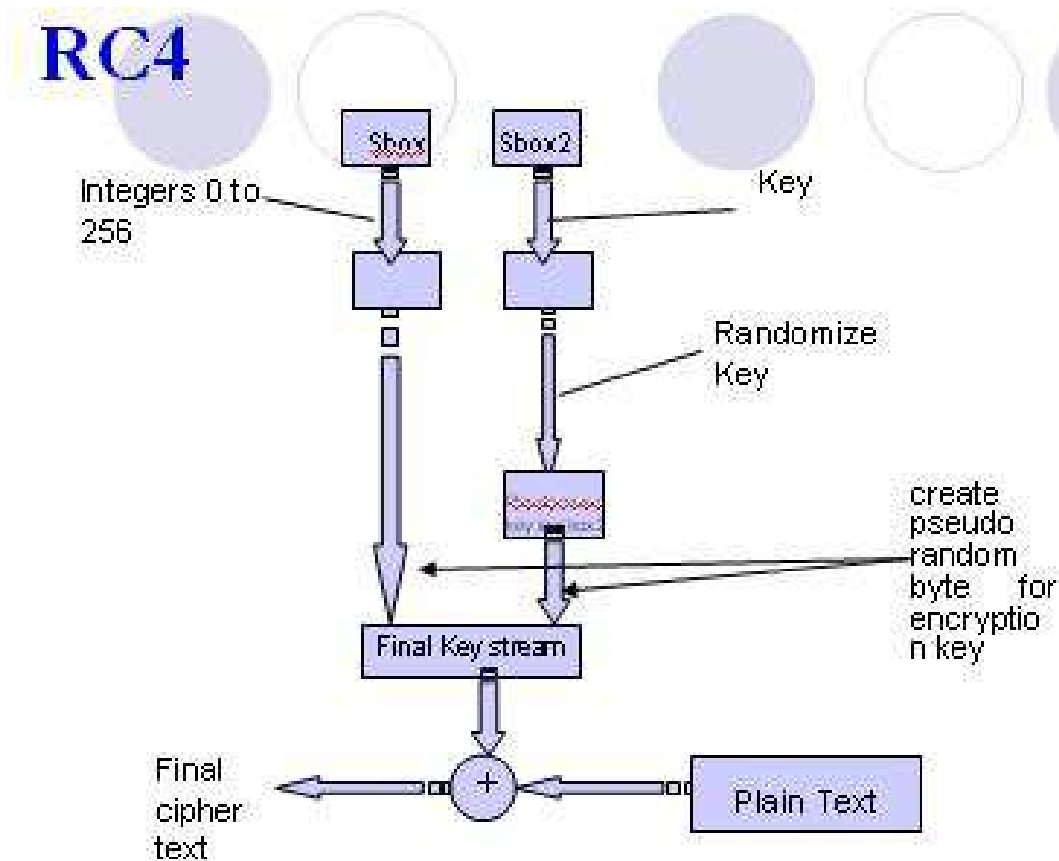
On Saturday morning an anonymous cypherpunk wrote:

SUBJECT: RC4 Source Code

I've tested this. It is compatible with the RC4 object module that comes in the various RSA toolkits.

```
/* rc4.h */  
typedef struct rc4_key  
{  
    unsigned char state[256];  
    unsigned char x;  
    unsigned char y;  
} rc4_key; :
```

Funcionamiento RC4



Inicialización

$S[0..255] = 0, 1, \dots, 255$

$K[0..255] = \text{Key}, \text{Key}, \text{Key}, \dots$

for $i = 0$ to 255

$j = (j + S[i] + K[i]) \bmod 256$

swap $S[i]$ and $S[j]$

Iteración (produciendo un byte al azar)

$i = (i + 1) \bmod 256$

$j = (j + S[i]) \bmod 256$

swap $S[i]$ and $S[j]$

$t = (S[i] + S[j]) \bmod 256$

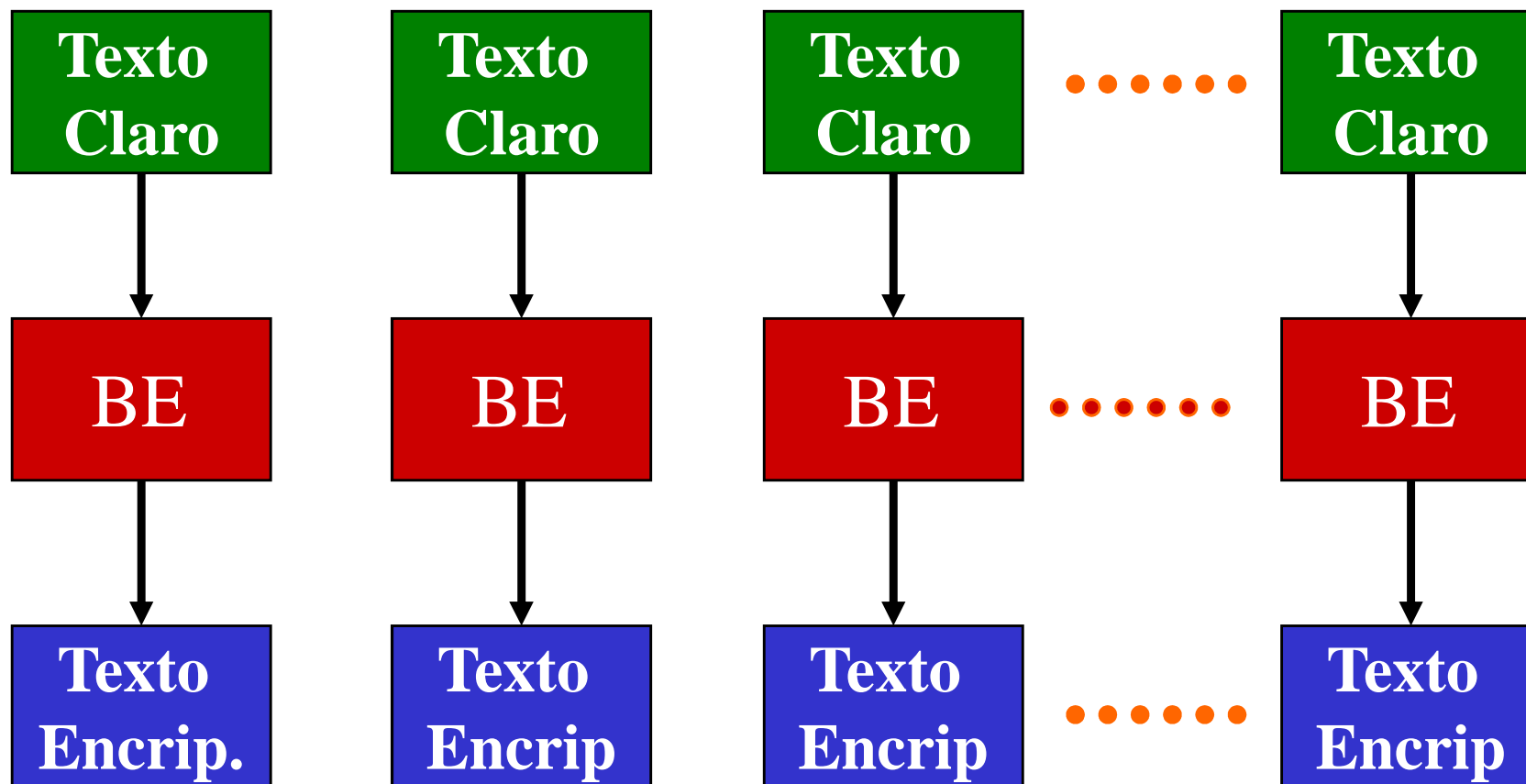
Output $S[t]$

Algoritmos de Encriptación Simétrica en Bloque

Métodos de encriptación en bloque

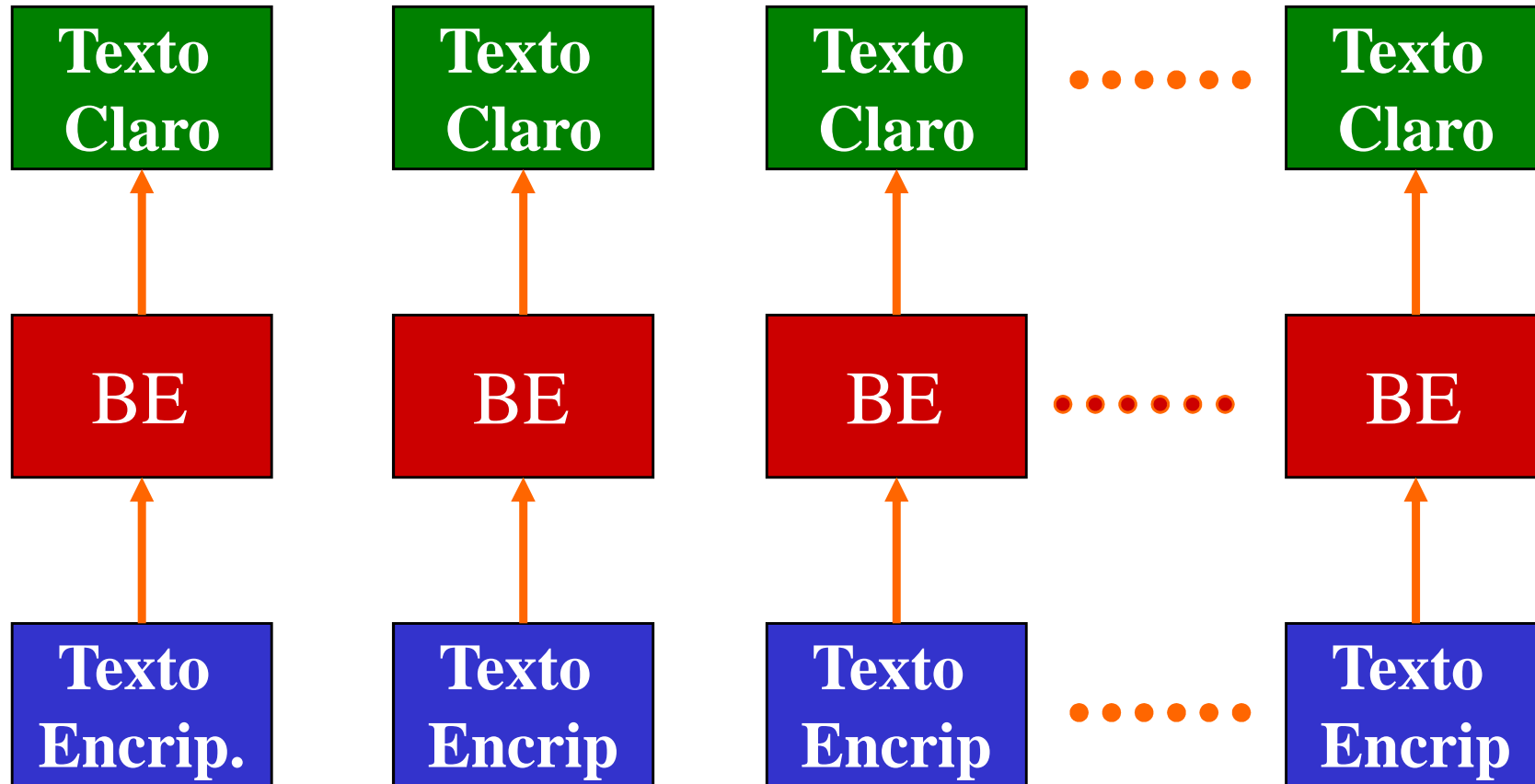
- Se encripta el mensaje original agrupando los símbolos en grupos (bloques) de dos o más elementos
- Modos operación de encriptación en bloque:
 - ECB: Electronic Code Book
 - CBC: Cipher Block Chaining

Esquema ECB de encriptación en bloque



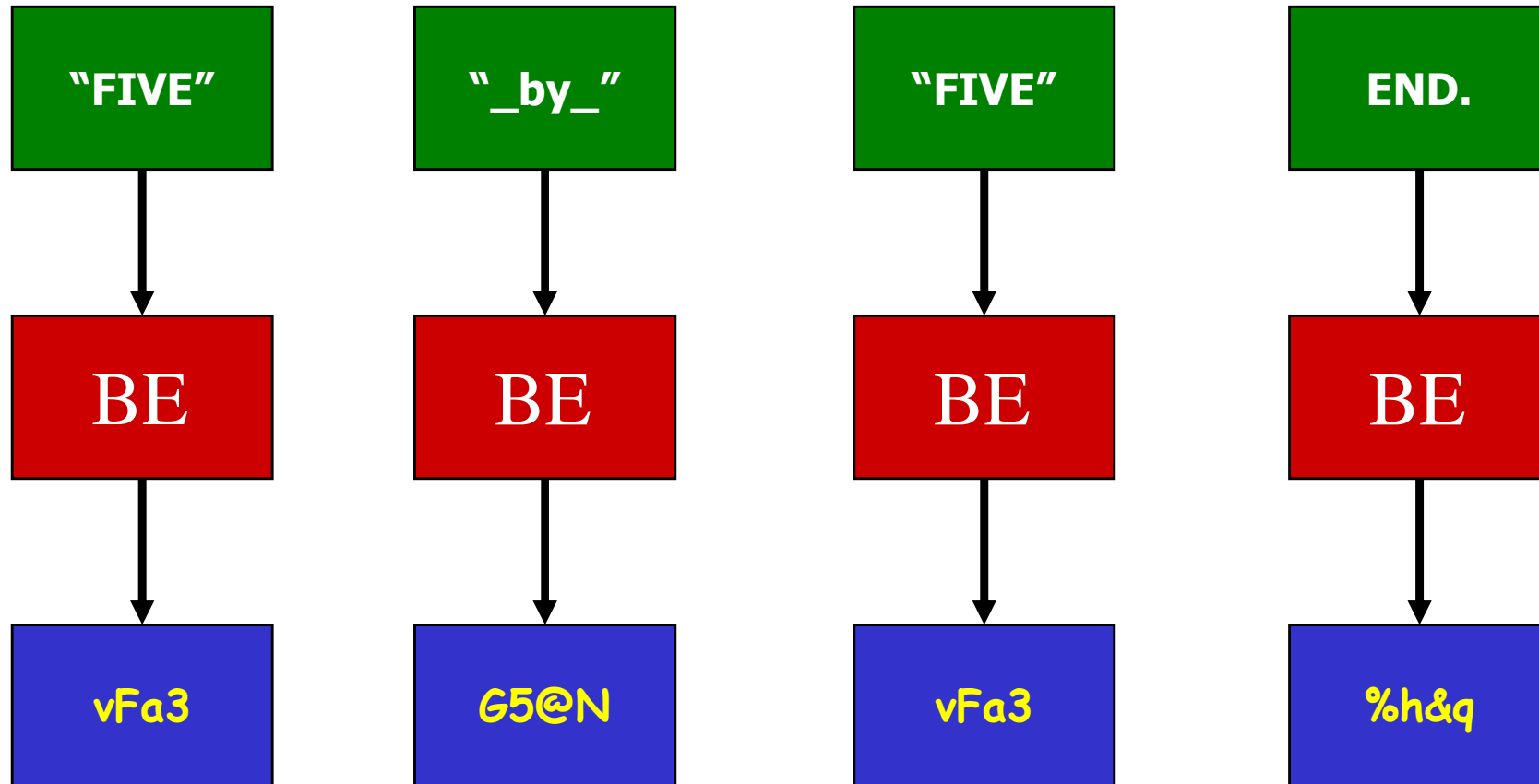
ECB: Electronic Code Book

Esquema ECB decripción en bloque

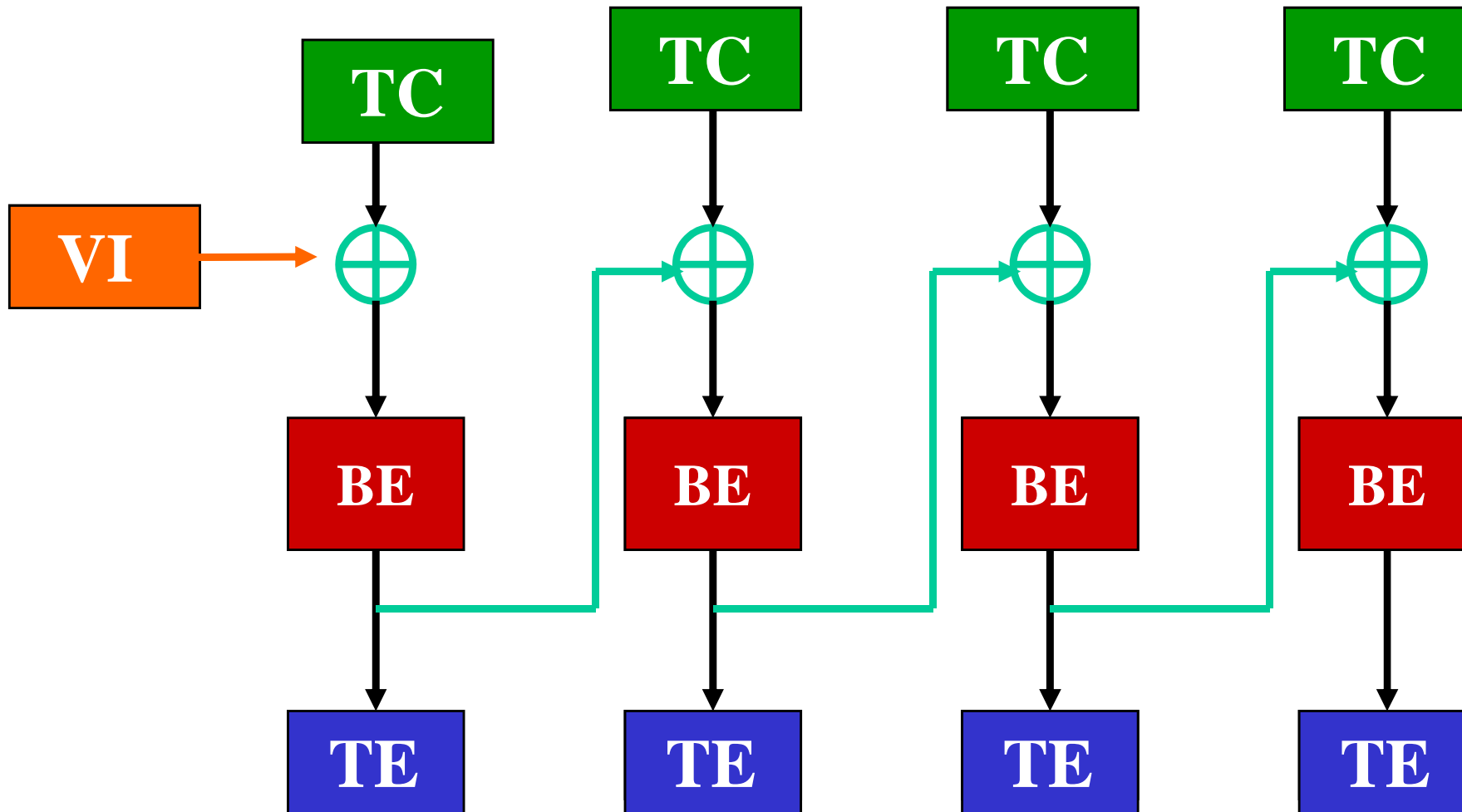


ECB: Electronic Code Book

Ejemplo problema esquema ECB



Cipher Block Chaining (CBC) Encripción

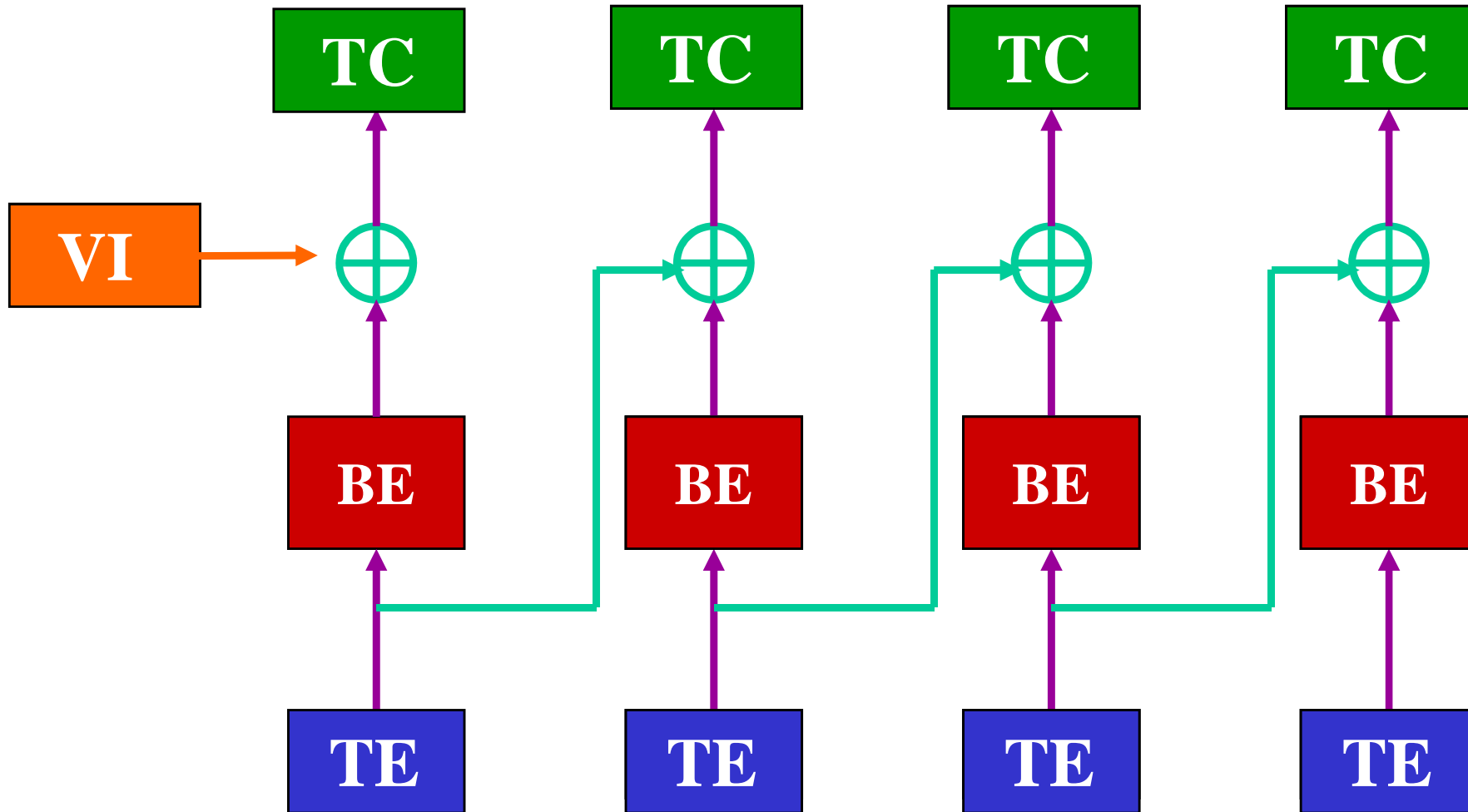


VI: Vector Inicialización
aleatorio

TC: Texto Claro

TE: Texto Encriptado

Cipher Block Chaining (CBC) Encripción

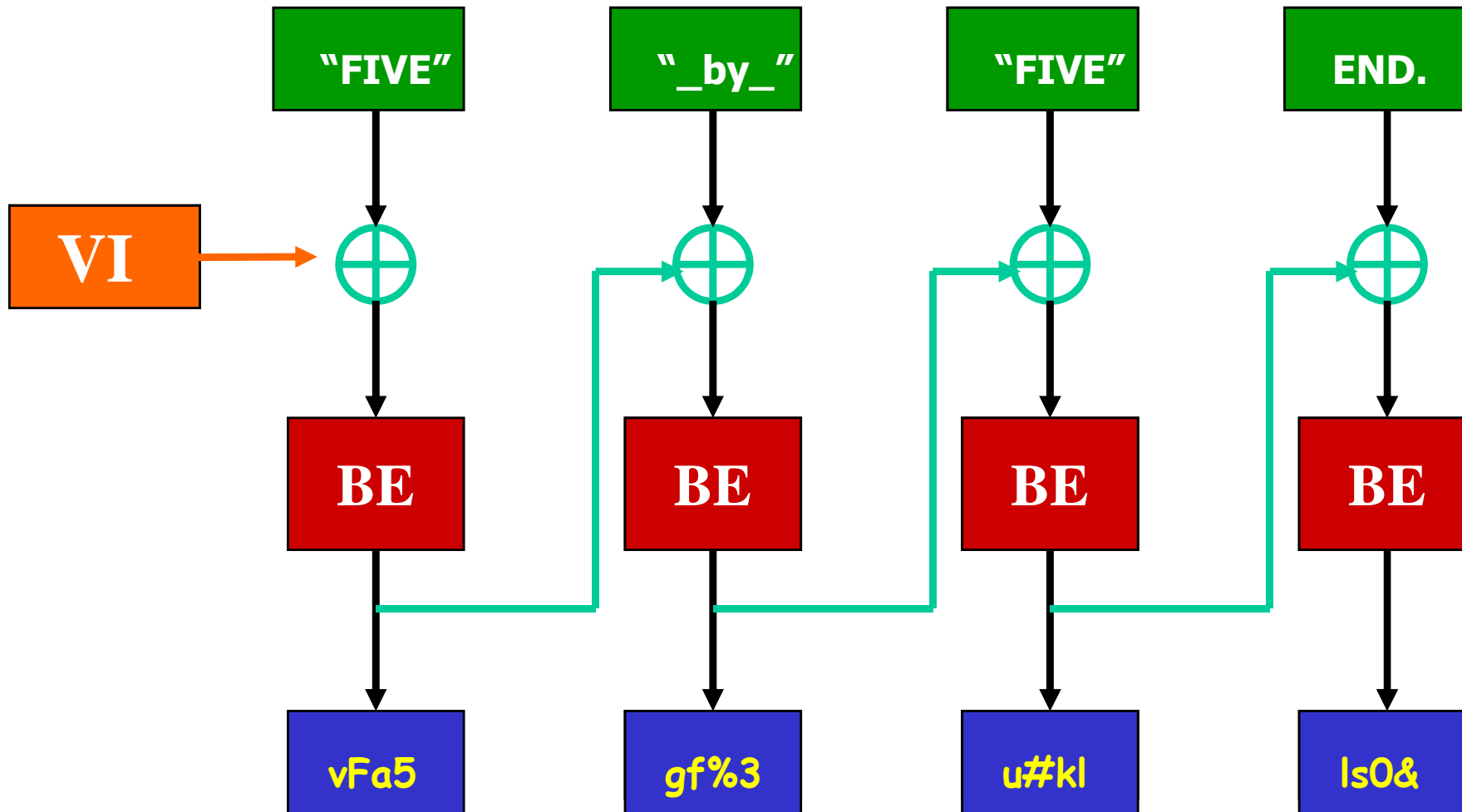


VI: Vector Inicialización
aleatorio

TC: Texto Claro

TE: Texto Encrypted

Cipher Block Chaining (CBC) Decripción



VI: Vector Inicialización
aleatorio

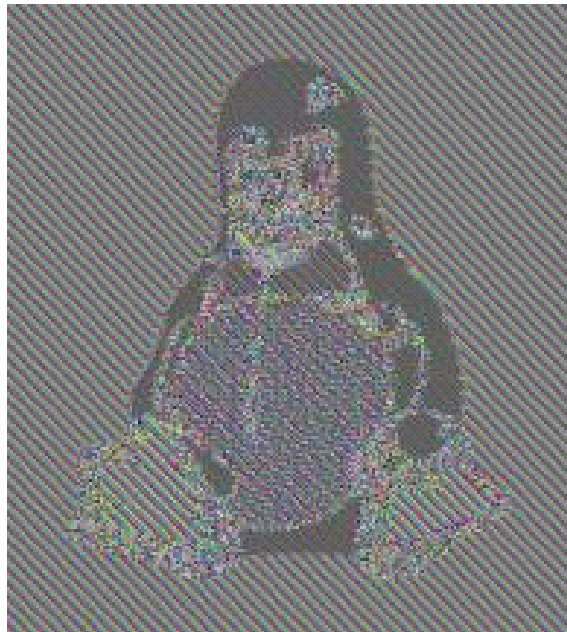
TC: Texto Claro

TE: Texto Encriptado

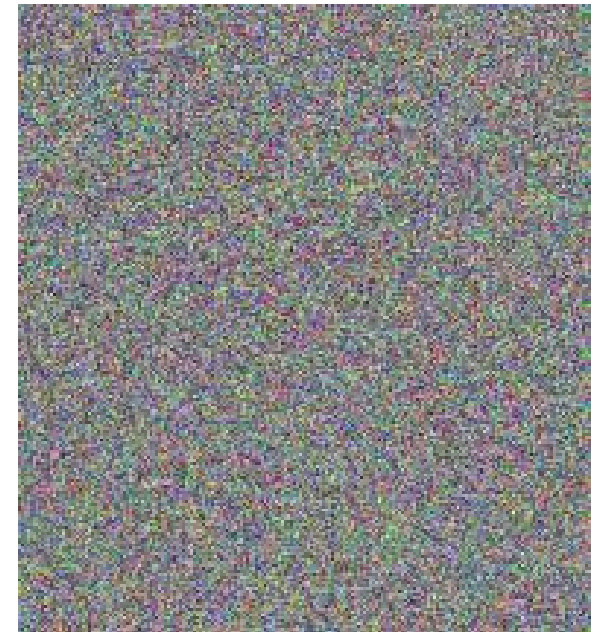
Comparando modos operación



Información original

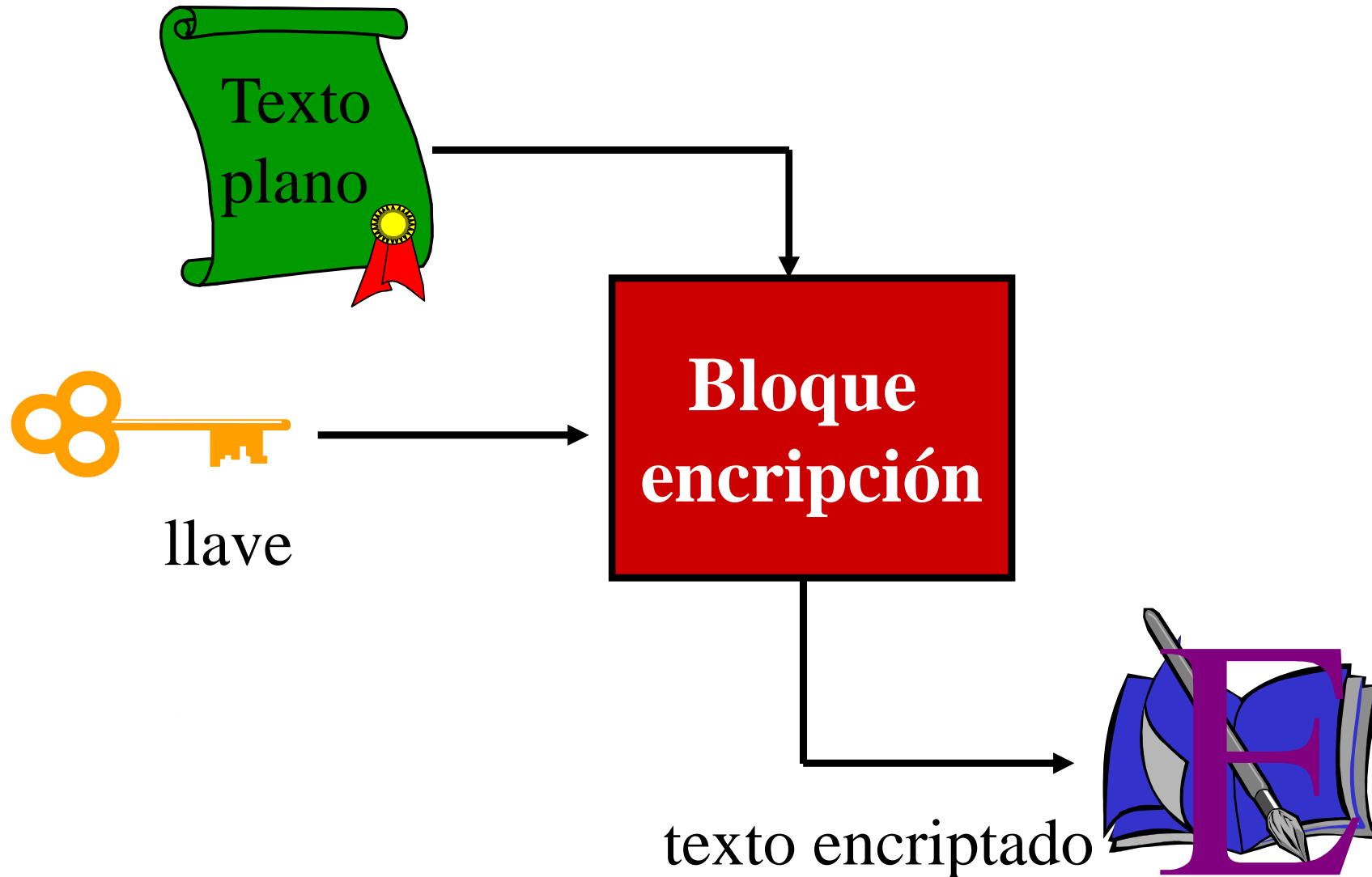


Información encriptada
en modo ECB



Información encriptada
en modo CBC

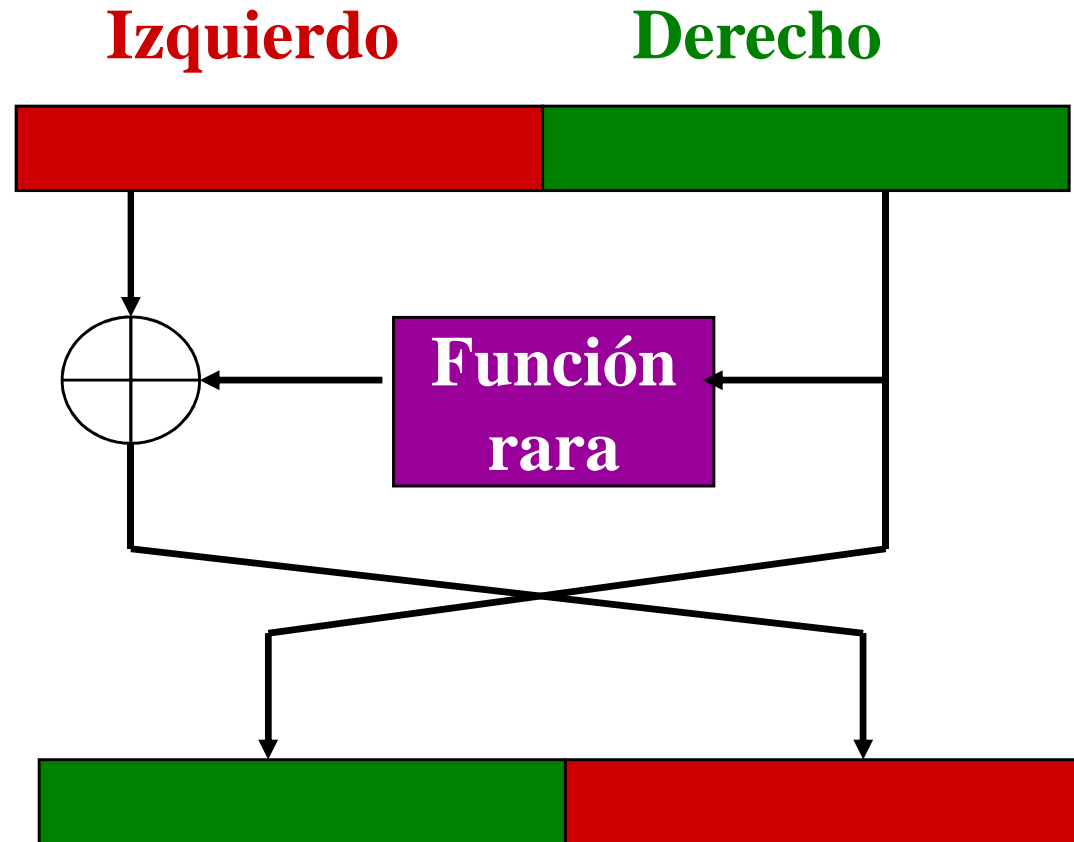
¿Cómo construir un block cipher?



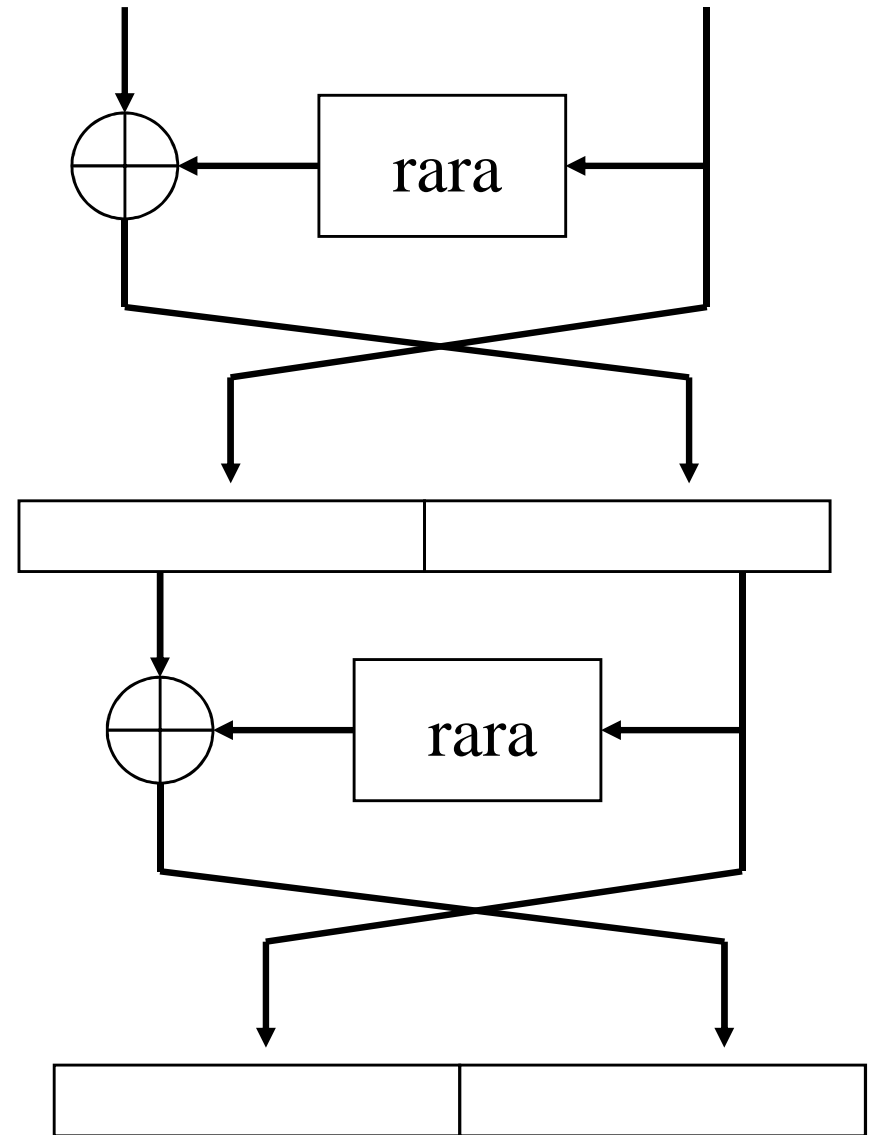
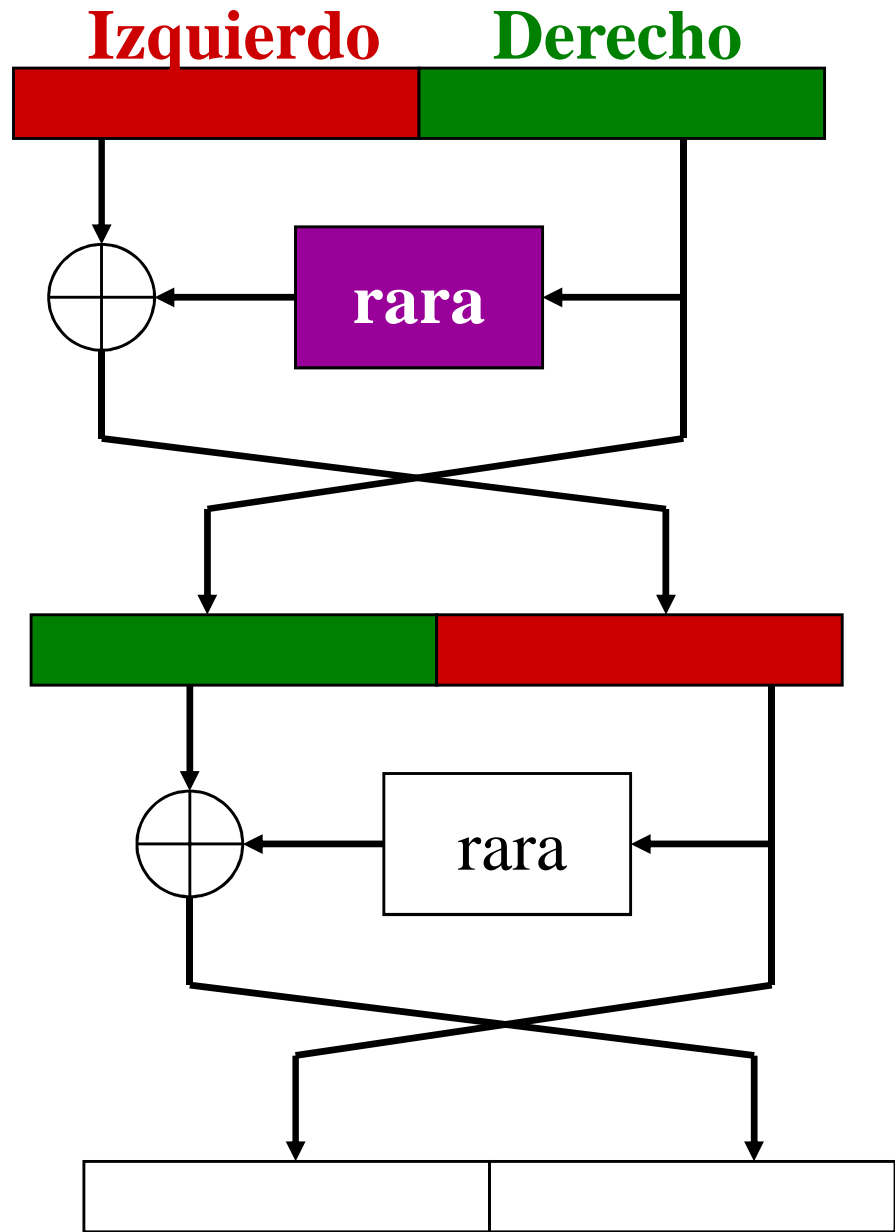
Los criptosistemas de Feistel

- 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

Barajeando los datos de entrada



Repitiendo



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

DES: ejemplo de encriptación 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

Características de DES

- Algoritmo cifrado en bloque y simétrico
- Longitud bloque: 64 bits
- Longitud llave: 56 bits, por lo que existen $2^{56} = 7.2 \times 10^{16}$ 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

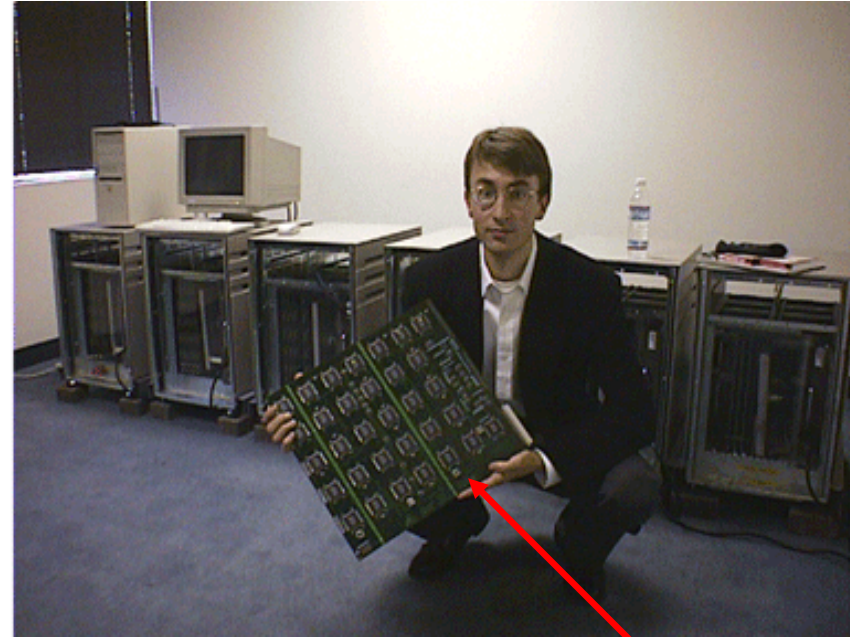
Críticas a DES

- La llave de 56 bits es considerada muy pequeña para soportar ataques de fuerza bruta.
- La estructura interna de DES, las cajas S, son *clasificadas*.
- A excepción de áreas de extrema sensibilidad, el uso de DES debe de ser satisfactorio para la mayoría de las aplicaciones comerciales (William Stallings).
 - es razonable entonces confiar en DES para aplicaciones personales y comerciales

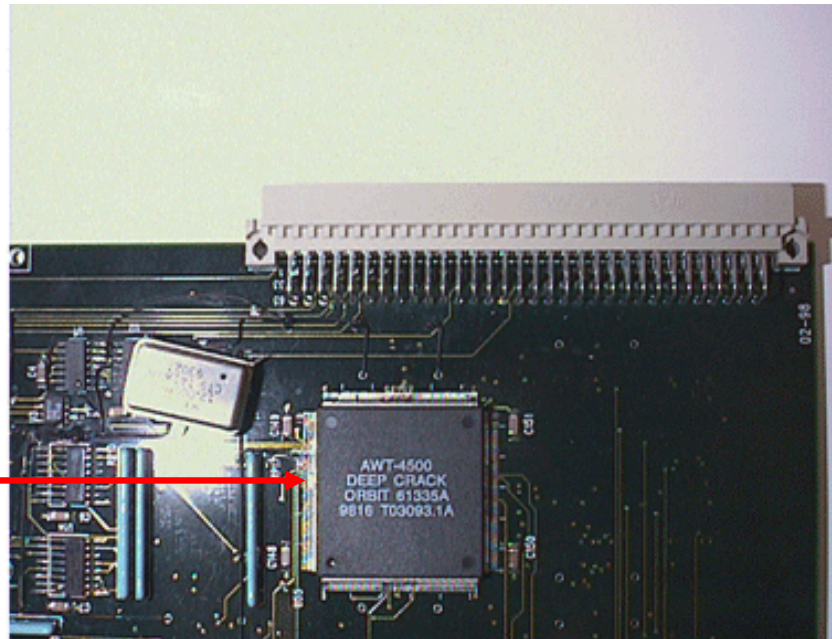
DES Challenges

- 29 enero 1997: DES Challenge I.
 - se rompe la llave en 96 días con 80.000 de computadoras en Internet, se evalúan 7.000 millones de llaves por segundo.
- 13 enero 1998: DES Challenge II-1.
 - se rompe en 39 días: ataque distribuido por distributed.net que llega a evaluar 34.000 millones de llaves por segundo
- 13 julio de 1998: DES Challenge II-2.
 - Electronic Frontier Foundation EFF crea el DES Cracker con una inversión de US \$ 200.000 y en 56 horas (2½ días)
- 18 enero 1999: DES Challenge III.
 - se unen la máquina DES Cracker y distributed.net con 100.000 computadoras para romper la llave en 22 horas
 - se trata del último desafío propuesto por RSA

Imágenes de la máquina



**1800 chips con 24
unidades de búsqueda**



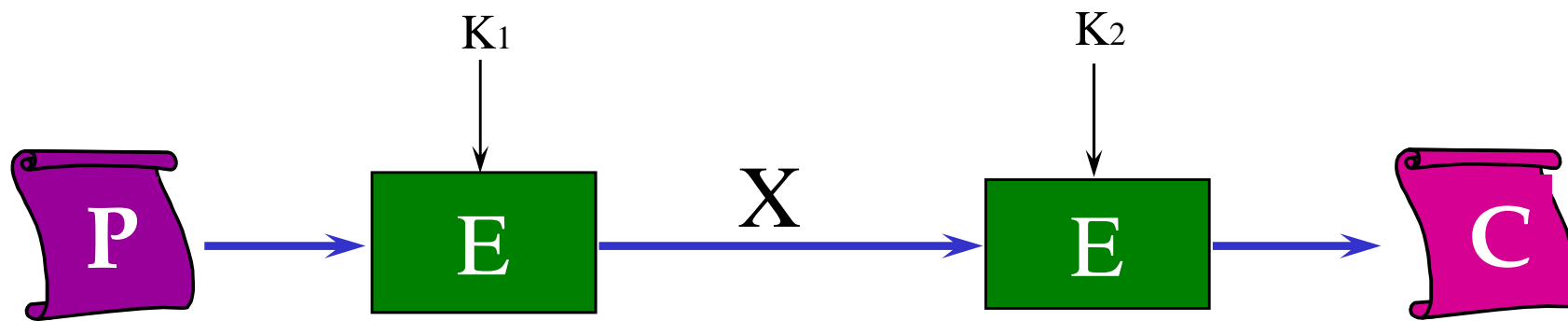
27 tarjetas

Mejoras a DES

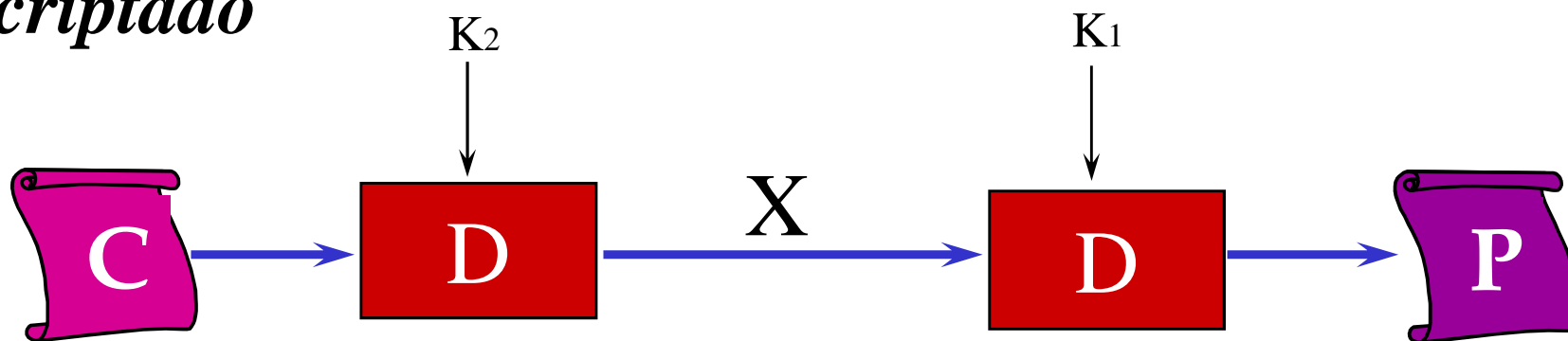
- Debido a las vulnerabilidades que presenta DES contra ataques de fuerza bruta, se han buscado alternativas.
- Una de estas es realizar un múltiple encriptado con DES usando más de una llave.

Doble DES

Encriptado



Decriptado



¿Es suficiente?

- Meet-in-the-middle attack
- Doble DES:

$$C = E(k_2, E(k_1, P))$$

$$P = D(k_1, D(k_2, C))$$

- Si se conoce P y C es posible un ataque de fuerza bruta con todos los pares de llaves k_1 y k_2
 - cada llave es de 56 bits, entonces se tiene que intentar 2^{112} pares de llaves, lo cual hace el ataque muy ineficiente

Atacando doble DES

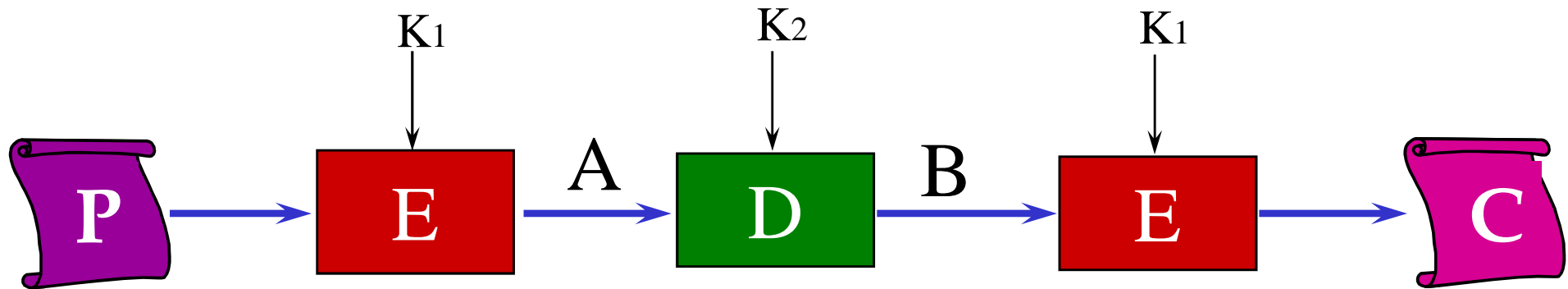
- Re-escribiendo la ecuación

$$\begin{array}{l} C = E(k_2, E(k_1, P)) \\ P = D(k_1, D(k_2, C)) \end{array} \quad \rightarrow \quad \begin{array}{l} M = E(k_1, P) \\ M = D(k_2, C) \end{array}$$

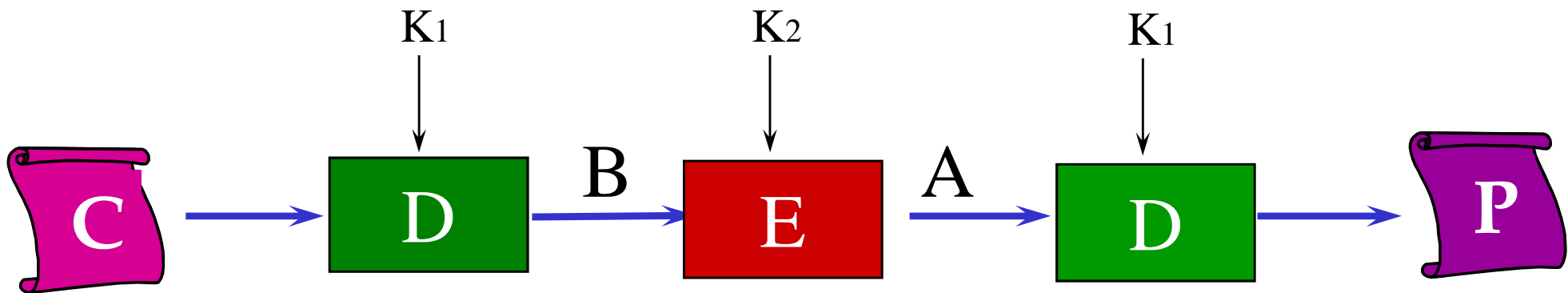
- Se intenta un número grande de decripciones con varios valores de k_2 y se almacenan los resultados en una tabla
- Después se empieza con $E(k_1, P)$ encriptaciones, checando cada resultado con lo almacenado en la tabla.
- Con suficiente espacio: rompe DES con trabajo de 2^{57}
- Requerimientos memoria prohibitivos
 - trabajo investigación para disminuir estos requerimientos

Triple DES

Encriptado



Decriptado



Hacia un nuevo estándar: AES

- En 1997 la NIST anuncia el sustituto 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)

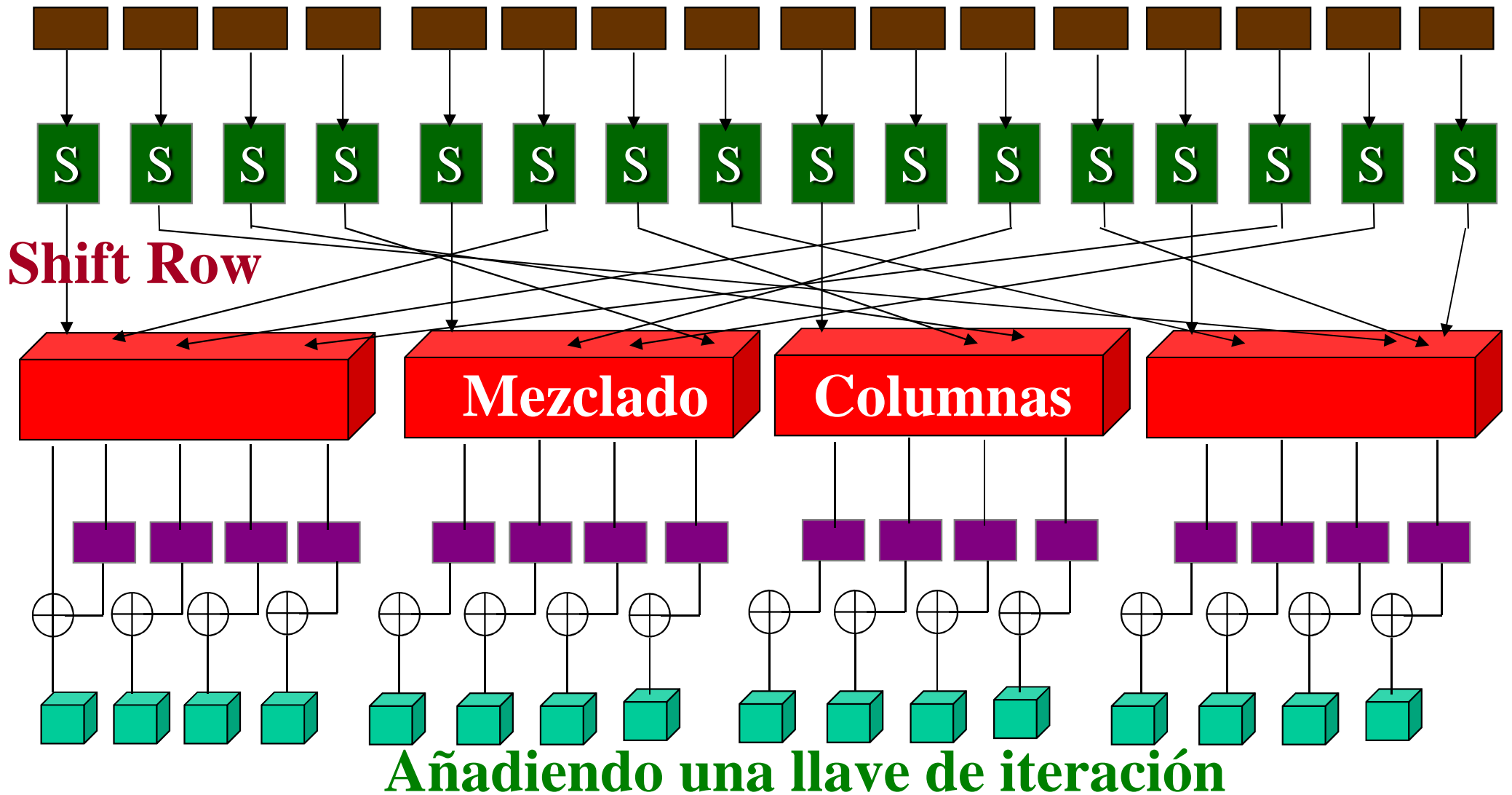


Características

- 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.
- Tamaño de bloque: puede ser de 128 y 256 bits
 - bloque 128 bits no es considerado suficientemente fuerte.
- No usa otros componentes criptográficos.
- No tiene partes obscuras y cosas difíciles de entender entre operaciones aritméticas.
- No deja espacio suficiente para esconder un trapdoor.
- Modo encriptación en bloque ECB.

Funcionamiento Rijndael

Substitución en base caja S



Algunos algoritmos llave simétrica

- DES
- IDEA
- AES
- Twofish
- Blowfish
- IDEA
- RC2, RC4 y RC5
- NewDES
- Feal
- SKIPJACK
- MMB



- CAST
- SAFER
- 3-WAY
- FEAL
- REDOC
- LOKI
- MADRYGA
- Lucifer
- Khufu and Khafre
- CA-1.1
- GOST
- CRAB 342

Características algoritmos encriptación simétrica

Algoritmo	Bloques (bits)	Llave (bits)	Iteraciones
Lucifer	128	128	16
DES	64	56	16
Loki	64	64	16
RC2	64	variable	-----
CAST	64	64	8
Blowfish	64	variable	16
IDEA	64	128	8
Skipjack	64	80	32
Rijndel	128	128 o más	variable
Twofish	128	variable	variable
Khufu	64	512	16,24,32

Características algoritmos encriptación simétrica

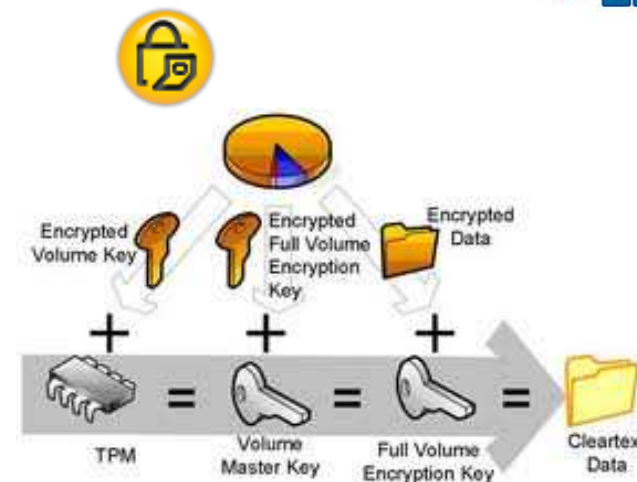
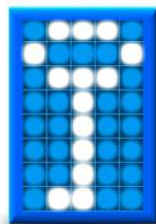
Algoritmo	Bloques (bits)	Llave (bits)	Iteraciones
Khufu	64	512	16,24,32
Khafre	64	128	más iteraciones
Gost	64	256	32variable
RC5	64	variable	variable
SAFER 64	64	64	8
Akelarre	variable	variable	variable
FEAL	64	64	32

Cifrado de disco y archivos

Métodos, opciones y herramientas

Aplicaciones criptográficas para cifrado en disco

- TrueCrypt
- BitLocker
- Steganos
- PGPDisk
- FileVault
- Symantec Endpoint Encryption
- Check Point Full Disk Encryption
 - (Pointsec)



- Algunas ligas interesantes:

- <http://encryption-software-review.toptenreviews.com/>
- http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software
- <http://www.sans.org/windows-security/2009/08/17/how-to-choose-the-best-drive-encryption-product>

¿Qué deseo proteger?

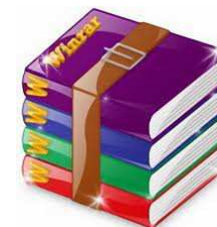
- Un archivo
- Todo el disco duro
- Contenido unidad almacenamiento

Protegiendo archivos

- Puede tratarse de un conjunto de archivos o de un solo archivo.
- Puntos a considerar:
 - ¿La herramienta borra el archivo original?
 - En caso de envío del archivo por algún medio, ¿es necesario que el receptor cuente con la herramienta para descifrar el archivo?
 - ¿Se requiere un elemento de hardware para descifrar a información?

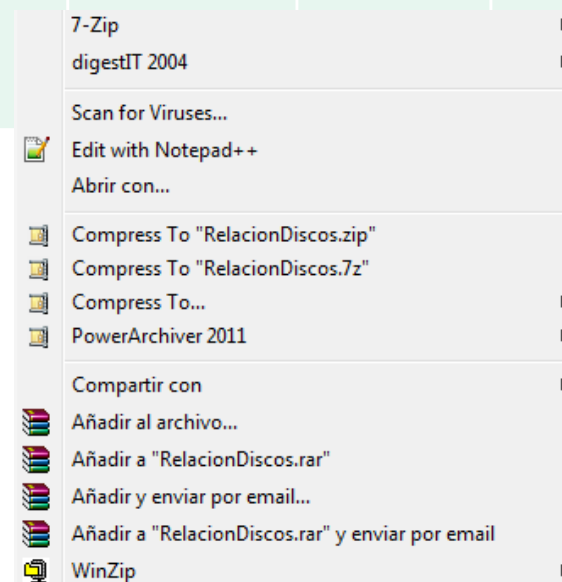
¿Y algo mas “sencillo”?

- Problema software cifrado
 - Emisor y receptor deben contar con el mismo software.
 - Posible que emisor genere un archivo autoejecutable
 - No es posible el envío por correo.
- Opción: utilizar la opción de cifrado de los programas de comprensión más utilizados en el mercado.
 - Solución simple y que proporciona un nivel de seguridad de acuerdo a la contraseña seleccionada.
 - Una segunda capa: utilizar las opciones de seguridad del aplicativo con que fue creado el documento a asegurar.



Un comparativo sencillo

Producto	Cifrado	Nombre oculto	Licencia	Acción vence licencia	Long. Comp.	Long. Cifrado	Cifrado y Nombre
7 Zip	AES-256	Si	Freeware	N/A	173	202	246
WinRAR	AES-128	Si	Shareware	Mensaje	138	147	180
WinZip	AES-128 AES-256 ZIP 2.0	No	Shareware	Espera	246	180	N/A
PowerArchiver	PK v2.04 AES 128 AES 192 AES 256	Solo en formato .pae	Shareware	Bloqueo	176	226	365



Archivo original: 203 bytes, solo texto.

Protección disco

- Se cifra todo el disco o solo una partición del disco.
- ¿En realidad es un cifrado o es una carpeta donde se colocan archivos y esta se cifra?
 - Capacidad de almacenamiento en la carpeta.
 - ¿Se puede modificar la capacidad sin tener que extraer la información?
- A tomar en cuenta: desempeño del sistema
 - Sugerencia: contar con varias particiones, algunas se cifran y otras no.

- Medios móviles
 - CD, DVD, **HUB**
- A tomar en cuenta
 - Datos a descifrar en cualquier computadora o en una sola computadora.
 - Independiente de cualquier sistema operativo.



- USB Disk Guard Pro
- Cryptoloop
- TrueCrypt
- FreeSecurity
- Bcrypt
- Challenger



Desventajas llave secreta

- Distribución de llaves
 - Usuarios tienen que seleccionar llave en secreto antes de empezar a comunicarse
 - KDC: Key Distribution Problem
- Manejo de llaves
 - Red de n usuarios, cada pareja debe tener su llave secreta particular,
- Sin firma digital
 - No hay posibilidad, en general, de firmar digitalmente los mensajes

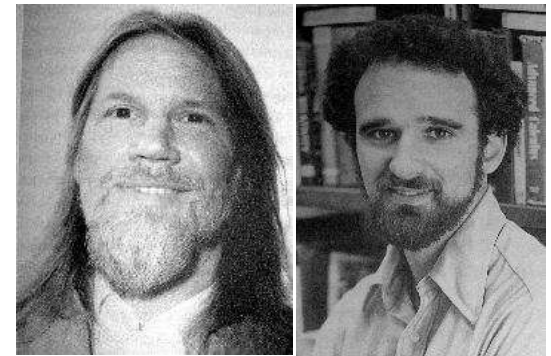


Criptosistema Diffie Hellman

Algoritmo intercambio llaves

Diffie-Hellman

- Primer algoritmo de llave pública (1976)
 - Williamson del CESG¹ UK, publica un esquema idéntico unos meses antes en documento clasificado
 - asegura que descubrió dicho algoritmo varios años antes
- Varios productos comerciales utilizan esta 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 en la dificultad para calcular logaritmos discretos
 - i.e. el problema del logaritmo discreto



El problema del logaritmo discreto

- Dados g , x y p en la formula:

$$y = g^x \text{ mod } p$$

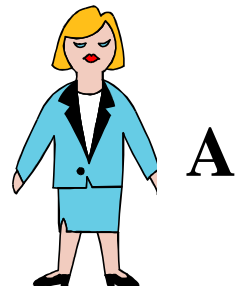
- el valor de y se puede obtener fácilmente
- Sin embargo dado y, g y p es computacionalmente difícil calcular x , como el logaritmo discreto
- Por ejemplo
 - dado $y = 7^8 \text{ mod } 13$ calcular y es fácil,
 - pero $3 = 7^x \text{ mod } 13$ calcular x es muy difícil
- Conclusión:
 - es muy fácil calcular exponentes mod un primo
 - es muy pesado calcular un logaritmo discreto

Algoritmo de Diffie-Hellman

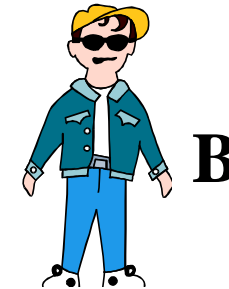
1. Los dos usuarios A y B seleccionan públicamente un grupo multiplicativo finito, G , de orden n y un elemento de G
2. A genera un número aleatorio X_a , calcula Y_a en G y transmite este elemento a B
3. B genera un número aleatorio X_b , calcula Y_b en G y transmite este elemento a A
4. A recibe Y_b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

Esquema Diffie Hellman

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



La llave de A y B es **K**

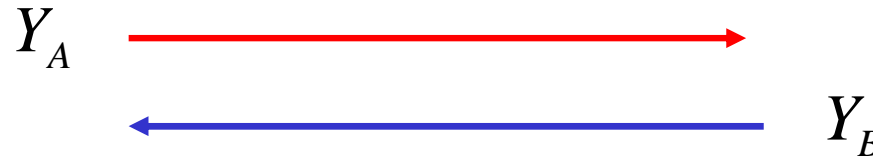


Selecciona val. priv: X_A ($X_A < q$)

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

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

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



Generando llave secreta A

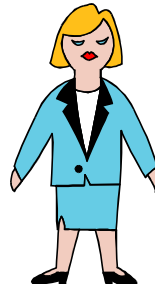
$$K = (Y_B)^{X_A} \text{ mod } q$$

Generando llave secreta B

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

Ejemplo Diffie Hellman

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



A



La llave de A y B es 21



B

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

Calcula valor pub: $Y_A = 2^{29} \bmod 53$
 $= 45 \bmod 53$

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

Calcula valor pub: $Y_B = 2^{19} \bmod 53$
 $= 12 \bmod 53$

Y_A (45)



Y_B (12)

Generando llave secreta A

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

Generando llave secreta B

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

Características y ejemplos



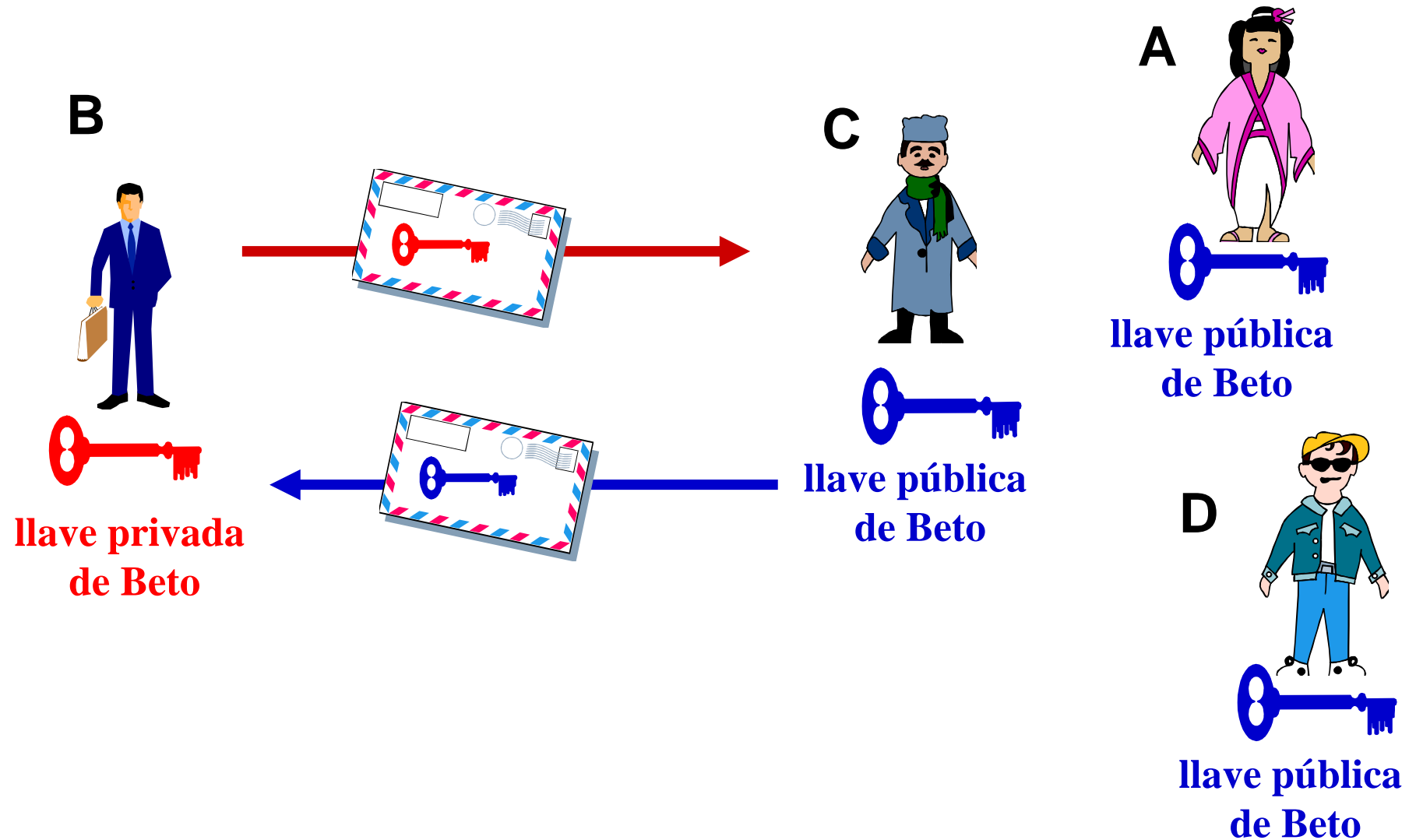
Background

- 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.

Antecedentes

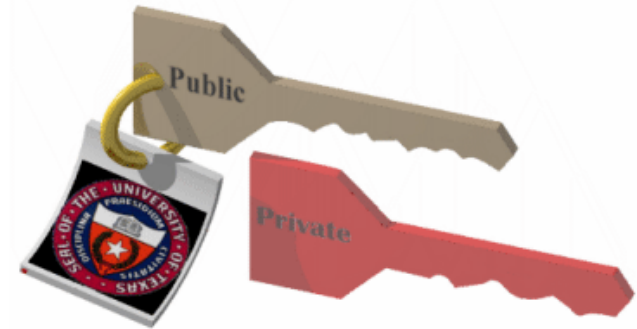
- Algunos algoritmos solo son buenos para distribución de llaves.
- Otros solo son buenos para encriptación.
- Algunos más solo son buenos para firmas digitales.
- Solo tres algoritmos son buenos para encriptación y firmas digitales:
 - RSA,
 - ElGamal
 - Rabin.
- Los tres algoritmos son más lentos que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

Criptograma llave pública (asimétrico)

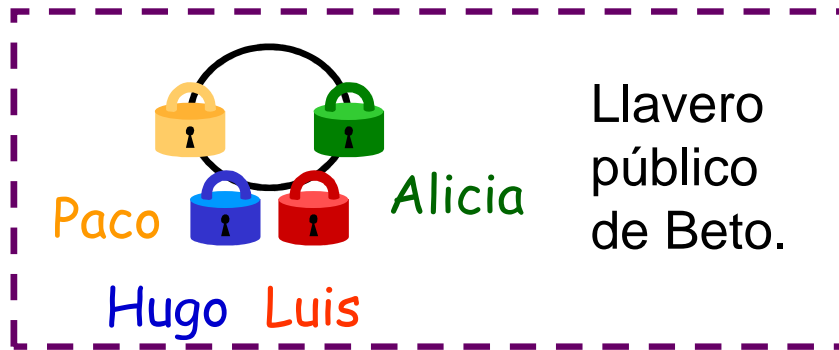


Encriptando con llave pública

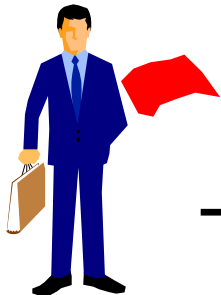
- Emisor no usa sus llaves
- Necesario contar con la llave pública del receptor
- Llaves relacionadas matemáticamente
 - teoría de números
 - funciones unidireccionales con puerta trasera
- Dos funciones usadas
 - producto de números enteros, cuya inversa es la factorización del número obtenido (RSA)
 - la exponenciación discreta, cuya inversa es el logaritmo discreto (problema logaritmos discretos, El Gamal)



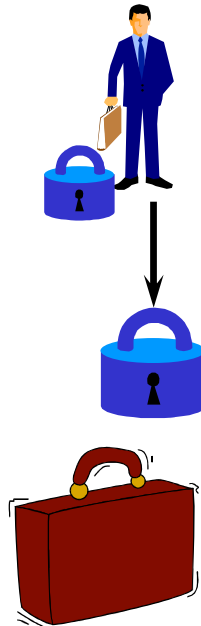
Encriptación con llave pública



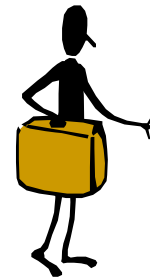
1. Beto escribe documento



2. Beto coloca el documento en la caja fuerte

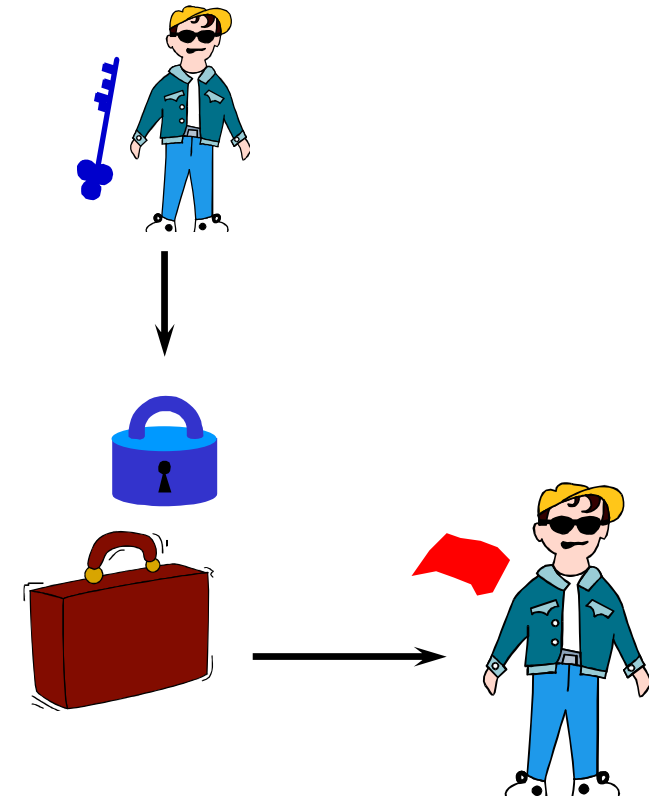


3. Beto asegura la caja con el candado de Hugo



4. La caja se transporta hacia Hugo

5. Hugo desasegura la caja con un su llave secreta



6. Hugo obtiene el documento.

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 .

Ejemplo suma modular 10

- $5 + 5 = 10 \text{ mod } 10 = 0$
- $3 + 9 = 12 \text{ mod } 10 = 2$
- $2 + 2 = 4 \text{ mod } 10 = 4$
- $9 + 9 = 18 \text{ mod } 10 = 8$

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

Encriptación usando suma modular

- Suma modulo 10 puede usarse como esquema de encriptación de dígitos.
- Encriptación:
 $\text{digito} + \langle \text{constante} \rangle \bmod 10$
- Se mapea cada dígito decimal a uno diferente de tal forma que es reversible.
- La constante es la llave secreta
- Decriptación:
 $\text{digito} - \langle \text{constante} \rangle \bmod 10$
si el resultado es menor a cero \Rightarrow sumar 10

Ejemplo encriptación suma modular

- Llave secreta: 5
- Encriptación:
 - $7 + 5 = 12 \bmod 10 = 2$
 - $8 + 5 = 13 \bmod 10 = 3$
 - $3 + 5 = 8 \bmod 10 = 8$
- Decripción:
 - $2 - 5 = -3 + 10 = 7$
 - $3 - 5 = -2 + 10 = 8$
 - $8 - 5 = 3$

Encriptación con inversa aditiva de x

- Aritmética regular:
 - substraer x puede hacerse sumando $-x$
- Inversa aditiva de x
 - número que se le tiene que sumar a x para obtener 0
- Por ejemplo:
 - inversa aditiva de 4 es 6
 - aritmética mod 10: $4 + 6 = 10 \text{ mod } 10 = 0$
- Si la llave pública es 4:
 - para encriptar se añade 4 mod 10
 - para decriptar se añade 6 mod 10

Ejemplo encriptación inversa aditiva

- Llave pública: 4
- Encriptación:
 $7 + 4 \bmod 10 = 11 \bmod 10 = 1$
 $8 + 4 \bmod 10 = 12 \bmod 10 = 2$
 $3 + 4 \bmod 10 = 7 \bmod 10 = 7$
- Decripción (llave privada: 6)
 $1 + 6 \bmod 10 = 7 \bmod 10 = 7$
 $2 + 6 \bmod 10 = 8 \bmod 10 = 8$
 $7 + 6 \bmod 10 = 13 \bmod 10 = 3$



Llave encriptación:

4



Llave decriptación:

6

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

Encriptación con multiplicación modular

- Multiplicación modular: mismo principio que la suma:
 - $7 * 4 \bmod 10 = 8$
 - $3 * 9 \bmod 10 = 7$
 - $2 * 2 \bmod 10 = 4$
 - $9 * 9 \bmod 10 = 1$

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

¿Cómo decriptar?

- No es posible aplicar el mismo principio de encriptación que en la suma
- 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
- ¿Cuáles números se pueden elegir para encriptar y decriptar?

¿Es posible usar el 5 y el 8?

Encriptando con 5

- $1 * 5 \bmod 10 = 5$
- $2 * 5 \bmod 10 = 0$
- $3 * 5 \bmod 10 = 5$
- $4 * 5 \bmod 10 = 0$
- $5 * 5 \bmod 10 = 5$
- $6 * 5 \bmod 10 = 0$
- $7 * 5 \bmod 10 = 5$
- $8 * 5 \bmod 10 = 0$
- $9 * 5 \bmod 10 = 5$

Encriptando con 8

- $1 * 8 \bmod 10 = 8$
- $2 * 8 \bmod 10 = 6$
- $3 * 8 \bmod 10 = 4$
- $4 * 8 \bmod 10 = 2$
- $5 * 8 \bmod 10 = 0$
- $6 * 8 \bmod 10 = 8$
- $7 * 8 \bmod 10 = 6$
- $8 * 8 \bmod 10 = 4$
- $9 * 8 \bmod 10 = 2$

¿Entonces cuales se pueden usar?

*	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 sustitución uno a uno de los dígitos
- Problema: **¿Cómo decriptar?**

Ejemplos inversos multiplicativos

- Se van a usar los números que cuenten con un inverso multiplicativo: $\{1,3,7,9\}$
- Ejemplo 1:
 - 7 es el inverso multiplicativo de 3
 - $3 \times 7 \bmod 10 = 21 \bmod 10 = 1$
 - Entonces: encriptación con 3 y decriptación con 7

Encriptación

$$7 * 3 \bmod 10 = 1$$

$$8 * 3 \bmod 10 = 4$$

$$3 * 3 \bmod 10 = 9$$

Decriptación

$$1 * 7 \bmod 10 = 7$$

$$4 * 7 \bmod 10 = 8$$

$$9 * 7 \bmod 10 = 3$$

En general

- Criptosistema:
 - 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 criptosistema ya que:
 - se puede multiplicar por x mod n para encriptar
 - se puede multiplicar por x^{-1} mod n para decriptar

Primera observación

- No es tan simple encontrar un inverso multiplicativo mod n , especialmente si n es muy grande,
- Si $n = 100$ dígitos
 - no es lógico realizar una búsqueda de fuerza bruta para encontrar un inverso multiplicativo
- Algoritmo ecludiano
 - permite encontrar inversos mod n , dado x y n encuentra y tal que:

$$x * y \text{ mod } n = 1 \text{ (si existe)}$$

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, i.e. $\text{mcd}(1,10) = 1$
 - 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

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

El mcd y los números relativamente primos a n

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

- Para poder determinar si un número cuenta con un inverso multiplicativo en aritmética modular n, es necesario encontrar el máximo común denominador, mcd, entre dos números a y b.
- Posible usar el algoritmo de Euclides para lo anterior

La función totient de Euler

- ¿Cuántos 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

Como se calcula el inverso de a en el cuerpo n

- Teorema de Euler/Fermat
 - basado en la función totient de Euler
- Algoritmo extendido de Euclides
 - es el método más rápido y práctico
- Teorema del Resto Chino TRC

**ESTAMOS LISTOS PARA DISEÑAR UN
ALGORITMO DE ENCRIPCION...**

Criptosistema RSA

- Primera realización del modelo de Diffie-Hellman
- Realizado por Rivest, Shamir y Adleman en 1977 y publicado por primera vez en 1978
 - Se dice que un método casi idéntico fue creado por Clifford Cocks en 1973
- Podría considerarse un criptosistema de bloque
 - Texto claro y criptograma son enteros entre 0 y $n-1$ para algún valor de n
 - Concepto bloque diferente al de criptosistemas simétricos en bloques
- Dos etapas
 1. Creación de las llaves
 2. Cifrado/descifrado del mensaje

La creación de llaves

- La creación de llaves

1. Cada usuario elige un número $n = p*q$ (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 llave pública e ($e < n$) y que cumpla:

$$\text{mcd} [e, \phi(n)] = 1.$$

5. Cada usuario calcula la llave privada que cumpla:

$$d = \text{inv} [e, \phi(n)].$$

6. Se hace público el número n y la llave e .

$$K_{\text{pub}} = (e, n)$$

7. Se guarda en secreto la llave d .

$$K_{\text{priv}} = (d, n)$$

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

Cifrado y descifrado de mensajes

- Tomando en cuenta que las llaves son:

Llave pública: (e, n)

Llave privada: (d, n)

- Si se desea encriptar un mensaje M :

- se tiene que cumplir: $M < n$

- es necesario usar la llave pública (e, n) :

$$C = M^e \bmod n$$

- Para descifrar el criptograma C es necesario usar la llave privada (d, n)

$$M = C^d \bmod n$$

Ejemplo generación llaves RSA

- Alicia desea generar sus llaves
 1. Elige un número $n = 7 * 13 = 91$
 2. 7 y 13 permanecen secretos
 3. $\phi(n) = \phi(7*13) = (7-1)(13-1) = 72$
 4. Se elige una llave pública $e=5$ ($5 < 91$) que cumple:
 $\text{mcd}[e, \phi(n)] = \text{mcd}[5,72] = 1$
 5. Se calcula una llave privada
 $d = \text{inv}[e, \phi(n)] = \text{inv}[5,72] = 29$
 6. Se envía a Beto la llave pública (5,91)
 7. Permanece en secreto 29



Alicia

Ejemplo encriptación/decriptación RSA

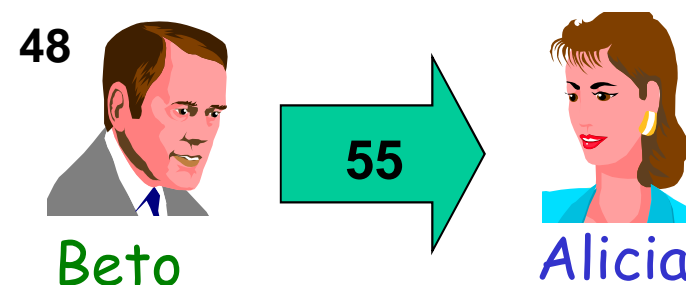
- Mensaje a encriptar: $M=48$
- Para encriptar M , Beto toma la llave pública $(5,91)$

$$C = M^e \text{ mod } n$$

$$C = 48^5 \text{ mod } 91$$

$$C = 5245.803.968 \text{ mod } 91$$

$$C = 55$$



- Se envía el mensaje 55 al receptor
- Para decriptar C , Alicia toma la llave privada $(29, 91)$

$$M = C^d \text{ mod } n$$

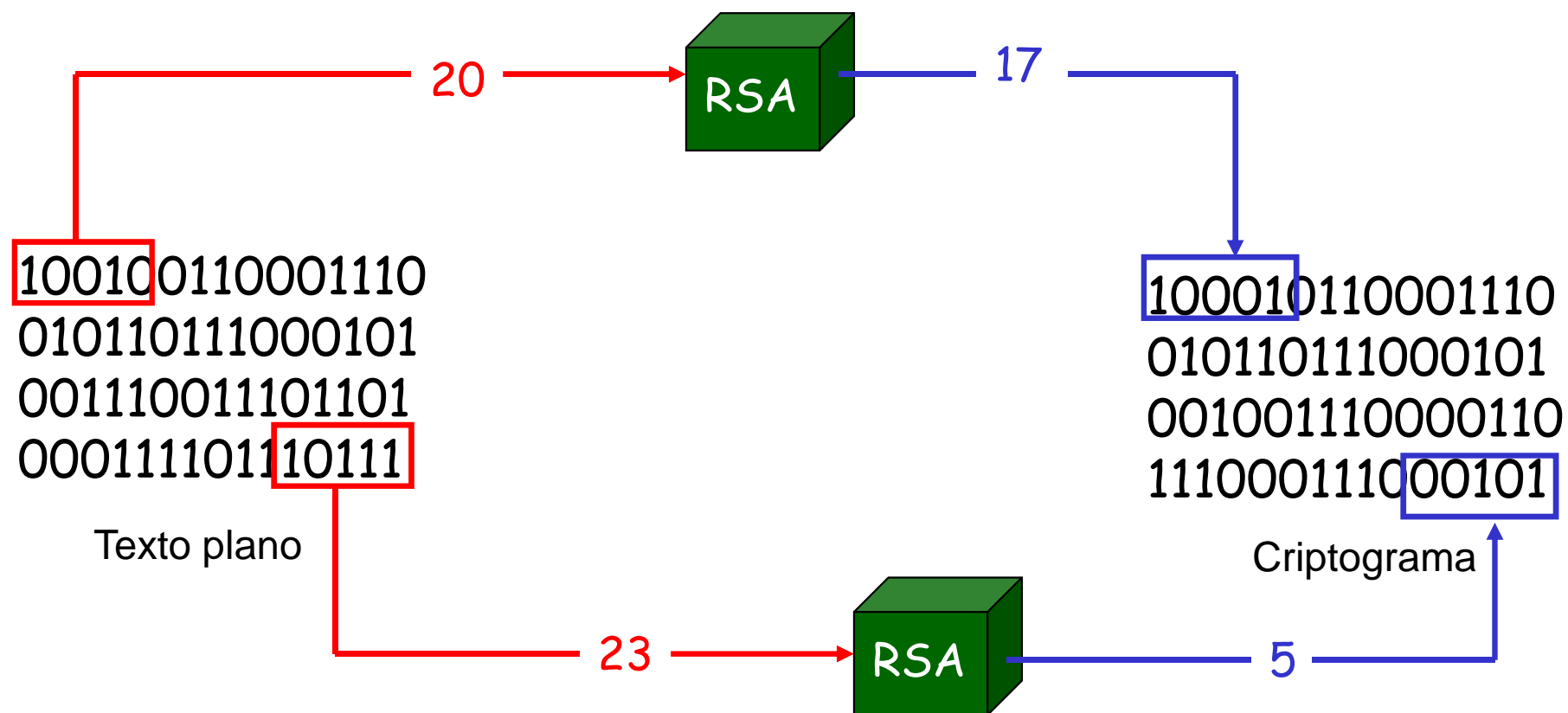
$$M = 55^{29} \text{ mod } 91$$

$$M = 2.954 \times 10^{50} \text{ mod } 91$$

$$M = 48$$

RSA como un criptosistema de bloques

- Texto claro y criptograma son enteros entre 0 y $n-1$ para algún valor de n
- Concepto bloque diferente a criptosistemas simétricos en bloques
- Por ejemplo: tomando en cuenta un valor de $n = 32 \Rightarrow 5$ bits



Factorización y RSA

- Fuerza Bruta
 - intentar todas las llaves posibles
- Ataques matemáticos
 - la llave privada de RSA es el inverso multiplicativo de un número en aritmética modular $\Phi(n)$
 - un atacante solo conoce la llave pública
 - (e, n)
 - si se factoriza n en dos números primos, se obtiene p y q , y con estos $\Phi(n)$, para después calcular la llave secreta

$$\Phi(n) = (p - 1)(q - 1)$$

$$d = e^{-1} \text{ mod } \Phi(n)$$

Tiempos factorización

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 2×10^{13} instrucciones ejecutadas. Un Pentium 200 MHz equivale aprox. a una máquina de 50 MIPS

El problema de factorización

- En 1977 se lanzó un reto matemático
- Artículo *A New Kind of Cipher that Would Take Millions of Years to break*
- Columna *Mathematical Games* en *Scientific American*
- Criptosistema encriptado con la 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 tomó aproximadamente 4000 a 6000 MIPS años de cómputo sobre un período de seis a ocho meses.

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"

¿Y hoy en día?

<http://www.rsa.com/rsalabs/node.asp?id=2093>

RSA Laboratories



- ▶ PUBLICATIONS
- ▶ RESEARCH AREAS
- ▶ STANDARDS INITIATIVES
- ▼ OTHER ACTIVITIES
 - ▼ Cryptographic Challenges
 - ▶ The RSA Factoring Challenge
 - The RSA Laboratories Secret-Key Challenge
 - DES Challenge III
 - ▶ CT-RSA 2007
- ▶ STAFF & ASSOCIATES

Home: Other Activities: Cryptographic Challenges: The RSA Factoring Challenge

The RSA Challenge Numbers

A link to each of the eight RSA challenge numbers is listed below. The numbers are designated "RSA-XXXX", where XXXX is the number's length, in bits. The values are presented as decimal strings, with the most significant digit first. Also listed are the number of digits, the decimal sum of the digits and the dollar amount to be awarded for a successful factorization.

Each challenge number may be downloaded as an ASCII text file. The entire challenge list may be downloaded, in ASCII text format, using the link below.

Challenge Number	Prize (\$US)	Status	Submission Date	Submitter(s)
RSA-576	\$10,000	Factored	December 3, 2003	J. Franke et al.
RSA-640	\$20,000	Factored	November 2, 2005	F. Bahr et al.
RSA-704	\$30,000	Not Factored		
RSA-768	\$50,000	Not Factored		
RSA-896	\$75,000	Not Factored		
RSA-1024	\$100,000	Not Factored		
RSA-1536	\$150,000	Not Factored		
RSA-2048	\$200,000	Not Factored		

The RSA Factoring Challenge

- The RSA Challenge Numbers
- The RSA Factoring Challenge FAQ
- Factorization Submission Form
- RSA-640 is factored!
- RSA-200 is factored!
- RSA-576 is factored!
- RSA-160 is factored!
- RSA-155 is factored!
- RSA-140 is factored!

Home: Historical: Cryptographic Challenges: The RSA Factoring Challenge

RSA-576 is factored!

On December 3, 2003, a team of researchers in Germany and several other countries reported a successful factorization of the challenge number [RSA-576](#). According to the announcement by J. Franke:

The factors [verified by RSA Laboratories] are

39807508642406493739712550055038649119906436234252
6708406385189575946388957261768583317

and

47277214610743530253622307197304822463291469530209
7116459852171130520711256363590397527

Lattice sieving was done by J. Franke and T. Kleinjung using Hardware of the Scientific Computing Institute and the Pure Mathematics Institute at Bonn University, of the Max Planck Institute for Mathematics in Bonn, and of the Experimental Mathematics Institute in Essen.

Home: Historical: Cryptographic Challenges: The RSA Factoring Challenge

RSA-640 is factored!

The factoring research team of F. Bahr, M. Boehm, J. Franke, T. Kleinjung continued its productivity with a successful factorization of the challenge number [RSA-640](#), reported on November 2, 2005. The factors [verified by RSA Laboratories] are:

16347336458092538484431338838650908598417836700330
92312181110852389333100104508151212118167511579

and

1900871281664822113126851573935413975471896789968
515493666638539088027103802104498957191261465571

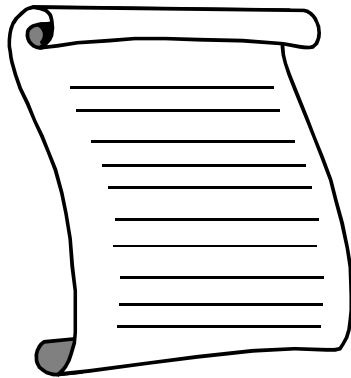
The effort took approximately 30 2.2GHz-Opteron-CPU years according to the submitters, over five months of calendar time. (This is about half the effort for [RSA-200](#), the 663-bit number that the team factored in 2004.)

Sistemas Híbridos

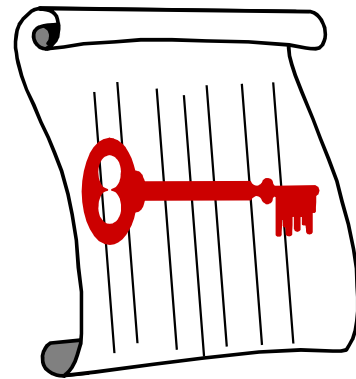
- Un algoritmo simétrico con una llave de sesión aleatoria es usada para encriptar un mensaje.
- Un algoritmo de llave pública es usado para encriptar la llave de sesión aleatoria.

Encriptación sistema híbrido

1. Escribir
mensaje a
enviar



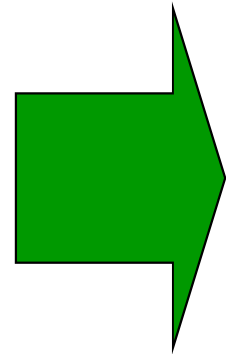
2. Generar una
llave simétrica
aleatoria



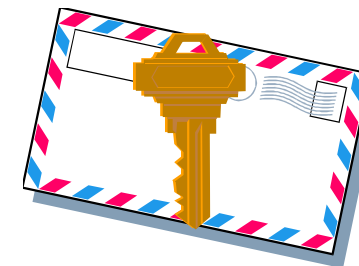
3. Encriptar
mensaje
con llave
simétrica



5. Poner
mensaje
y llave
encriptados
en un
solo
mensaje y
enviarlo

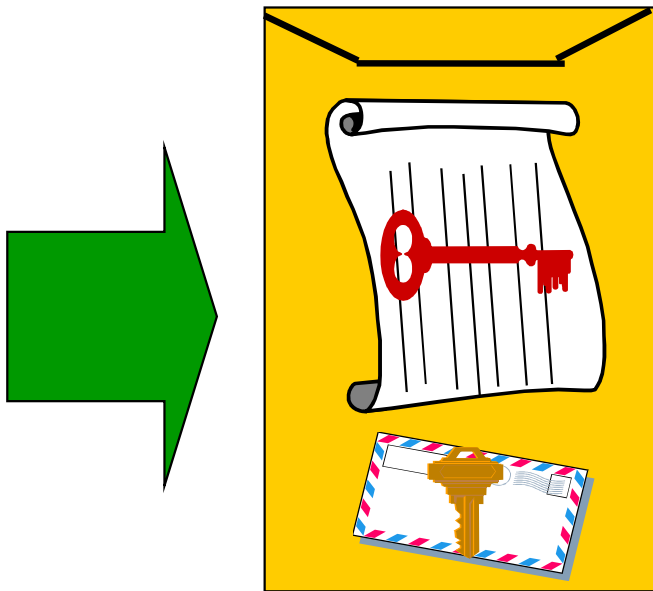


4. Tomar llave
pública destinatario
y encriptar llave
simétrica

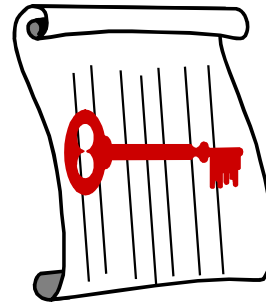


Decripción sistema hibrido

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

¿Hash?



???



H



Definición función hash

- Una función hash es una función $f\{0,1\}^* \rightarrow \{0,1\}^n$
- El tamaño de la salida n , es una propiedad de la función
- Una transformación de un mensaje de longitud arbitraria en un número de longitud fija es conocida como función hash.
- Nombres alternos
 - Huella digital
 - Compendio de un mensaje
 - Funciones de un solo sentido.
 - Digestivo

Ejemplo salida funcion hash

```
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>
```

rogomez@armagnac:467>more toto

ULTRA SECRETO

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

Atte

RGC

rogomez@armagnac:468>hash toto

MD5 (toto) = 30a6851f7b8088f45814b9e5b47774da

rogomez@armagnac:469>

Propiedades de una función hash

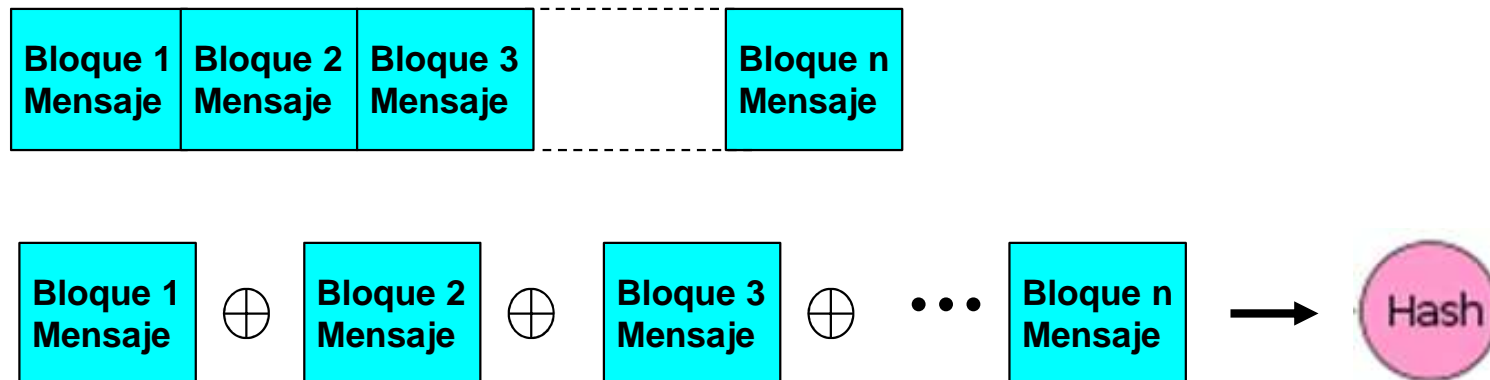
1. Debe ser posible calcular de forma eficiente el valor hash $x=H(m)$ de un mensaje m .
2. Dado el valor hash $x=H(m)$, debe ser computacionalmente imposible encontrar m . Una función con esta propiedad se conoce como función de un solo sentido.
3. La salida es única, si la información es cambiada (aún en sólo un bit) un valor completamente diferente es producido
4. Dado un mensaje m , debe ser imposible encontrar otro mensaje m' tal que $H(m)=H(m')$.
5. Debe ser imposible encontrar dos mensajes m y m' tal que $H(m)=H(m')$

Propiedad 4 se conoce como resistencia a una colisión débil

Propiedad 5 se conoce como resistencia a una colisión fuerte

¿Cómo se calcula un hash?

- Una forma sencilla es:
- Dividir el mensaje en bloques del mismo tamaño (añadir un pad/relleno si es necesario).
- Llevar a cabo un xor entre todos los bloques.
- El resultado final es el hash

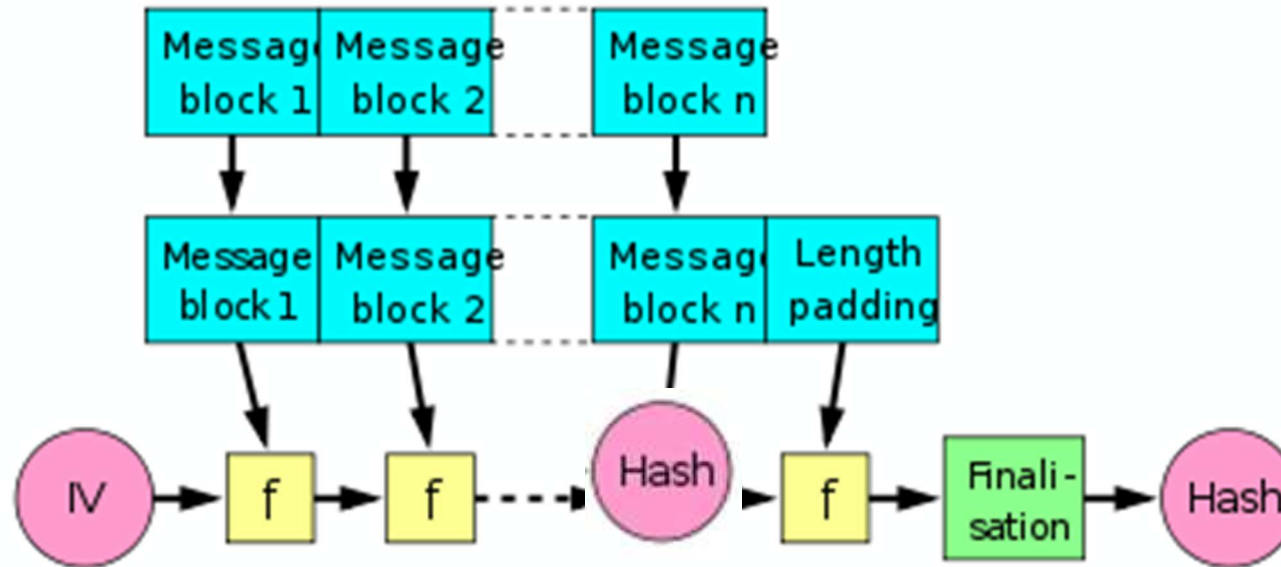


Pseudocódigo

```
main(int argc, char *argv[])
{
    unsigned long hash[4] = {0, 0, 0, 0}, data[4];
    FILE *fp;    int i;

    if ((fp = fopen(argv[1], "rb")) != NULL) {
        while ( fread(data, 4, 4, fp) != NULL)
            for (i=0; i<4; i++)
                hash[i] ^= data[i];
        fclose(fp);
        for (i=0; i<4; i++)
            printf("%08lx",hash[i]);
        printf("\n");
    }
}
```

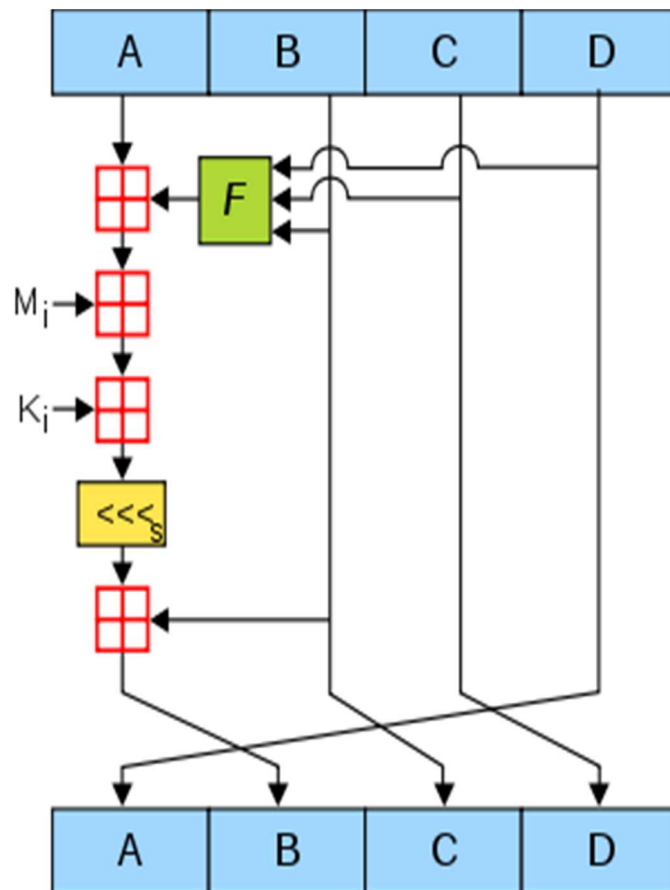
Merkle-Damgard



- Entrada dividida en bloques de igual tamaño y será la entrada a funciones de compresión.
- Añadir relleno: $1000\dots0 \parallel \text{longitud mensaje}$
- Finalisation: Opcional.
- Usado en todas las funciones hash anteriores al 2004
 - MD4, MD5, RIPE-MD, RIPE-MD160, SHA0, SHA1, SHA2

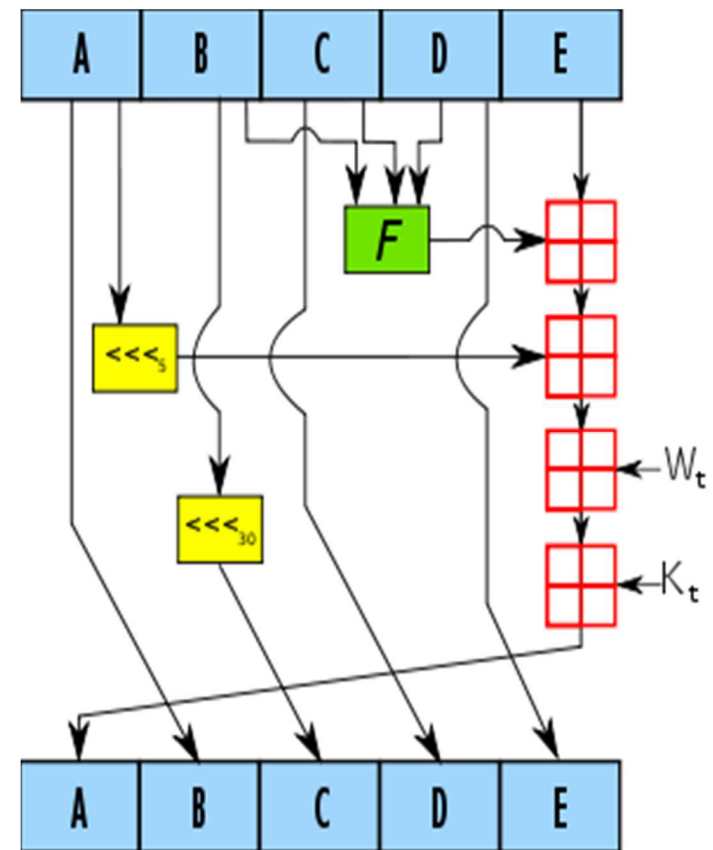
MD5 y SHA-1

64 rounds of:



128 bits

80 rounds of:



160 bits

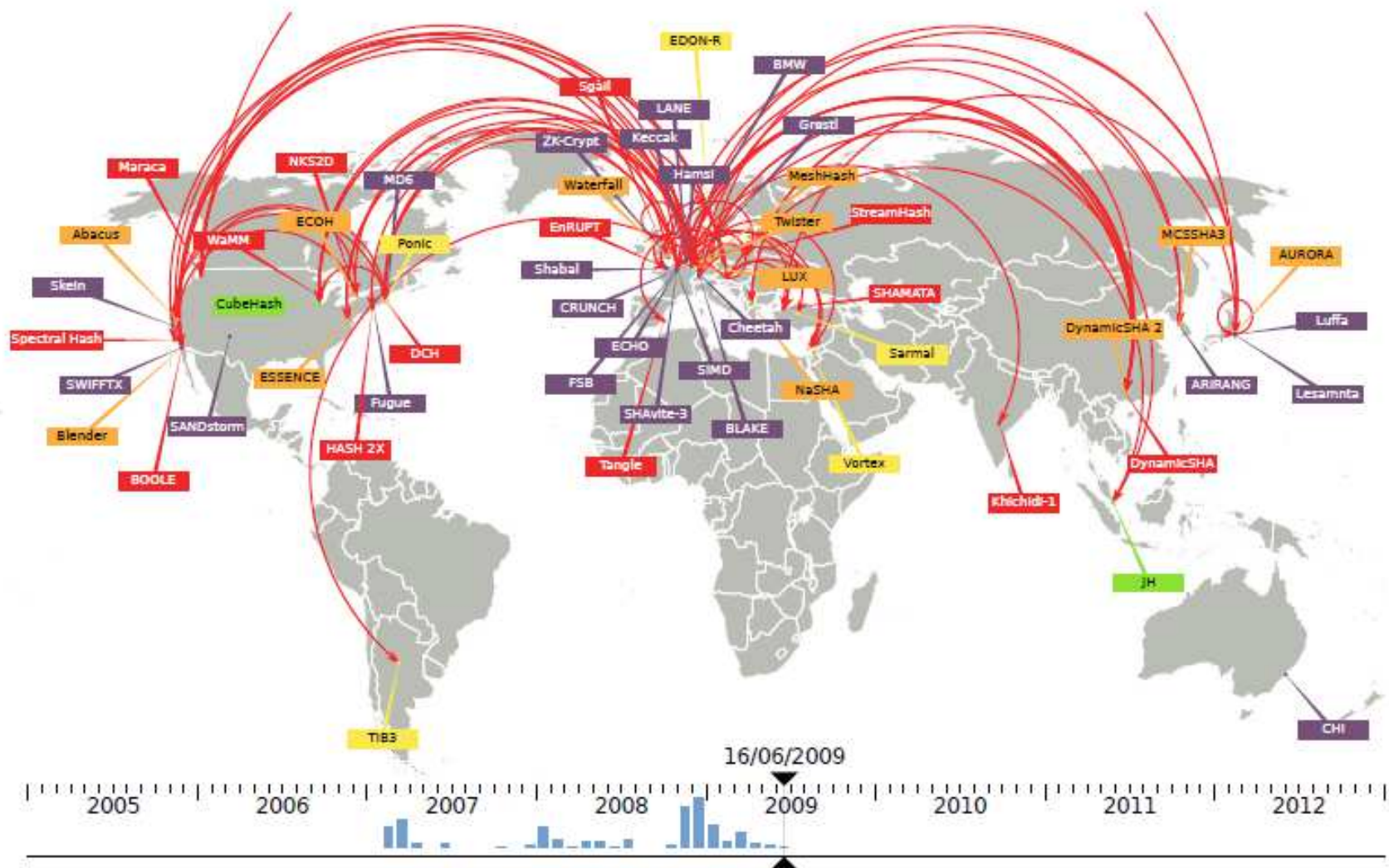
Ataques a funciones hash



- 2004: SHA-0 roto (Joux et al.)
- 2004: MD5 roto (Wang et al.)
- 2005: ataque práctico en MD5 (Lenstra et al., and Klima)
- 2005: SHA-1 teóricamente roto (Wang et al.)
- 2006: SHA-1 además roto (De Cannière and Rechberger)
- 2007: NIST lanzo un llamado para un SHA-3

¿Quién respondió al llamado del NIST?

El campo de batalla



Cortesía de Christophe De Canniere

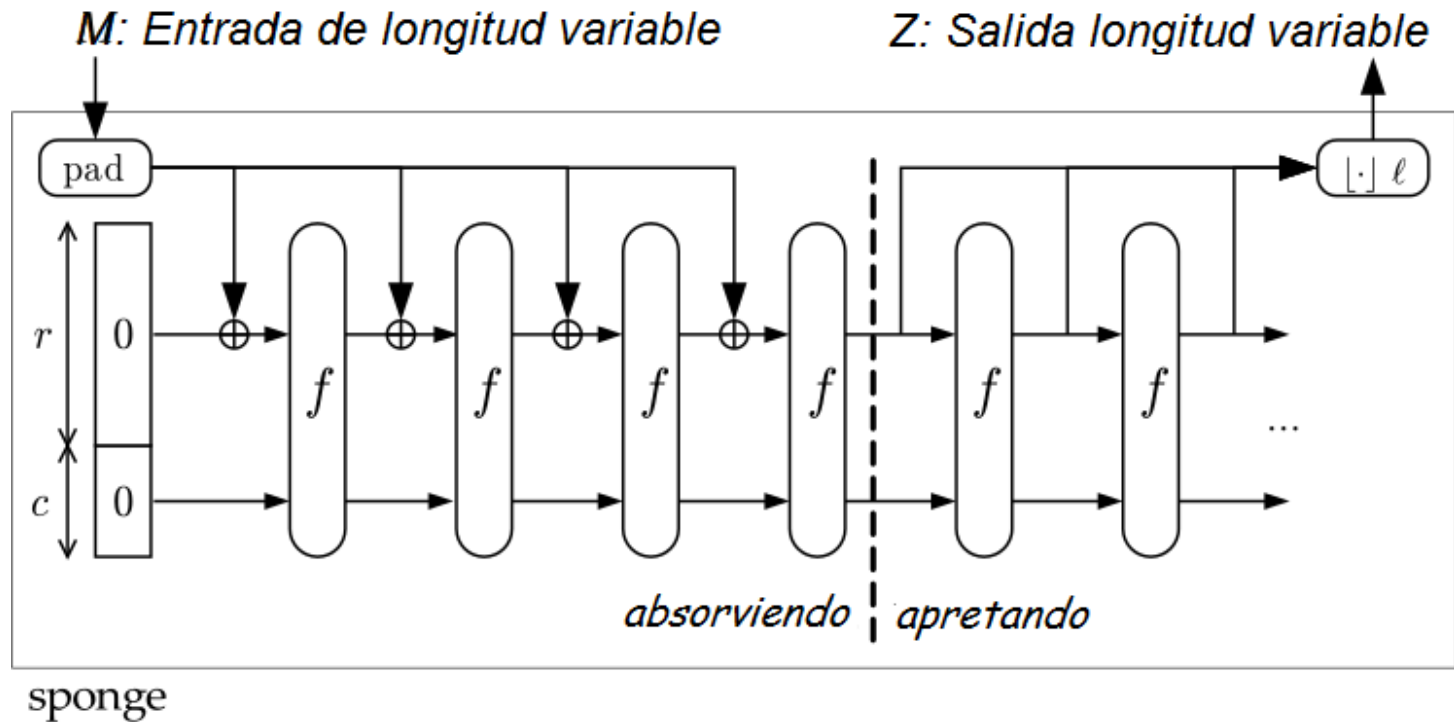
La selección



- 2007: SHA-3 llamado inicial
- 2008: deadline para someter una propuesta
- 2009: primera conferencia SHA-3
- 2010: segunda conferencia SHA-3 conference
- 2010: los finalistas son Blake, Grøstl, JH, Keccak and Skein
- 2012: conferencia final SHA-3
- Oct. 2, 2012: Keccak gana!

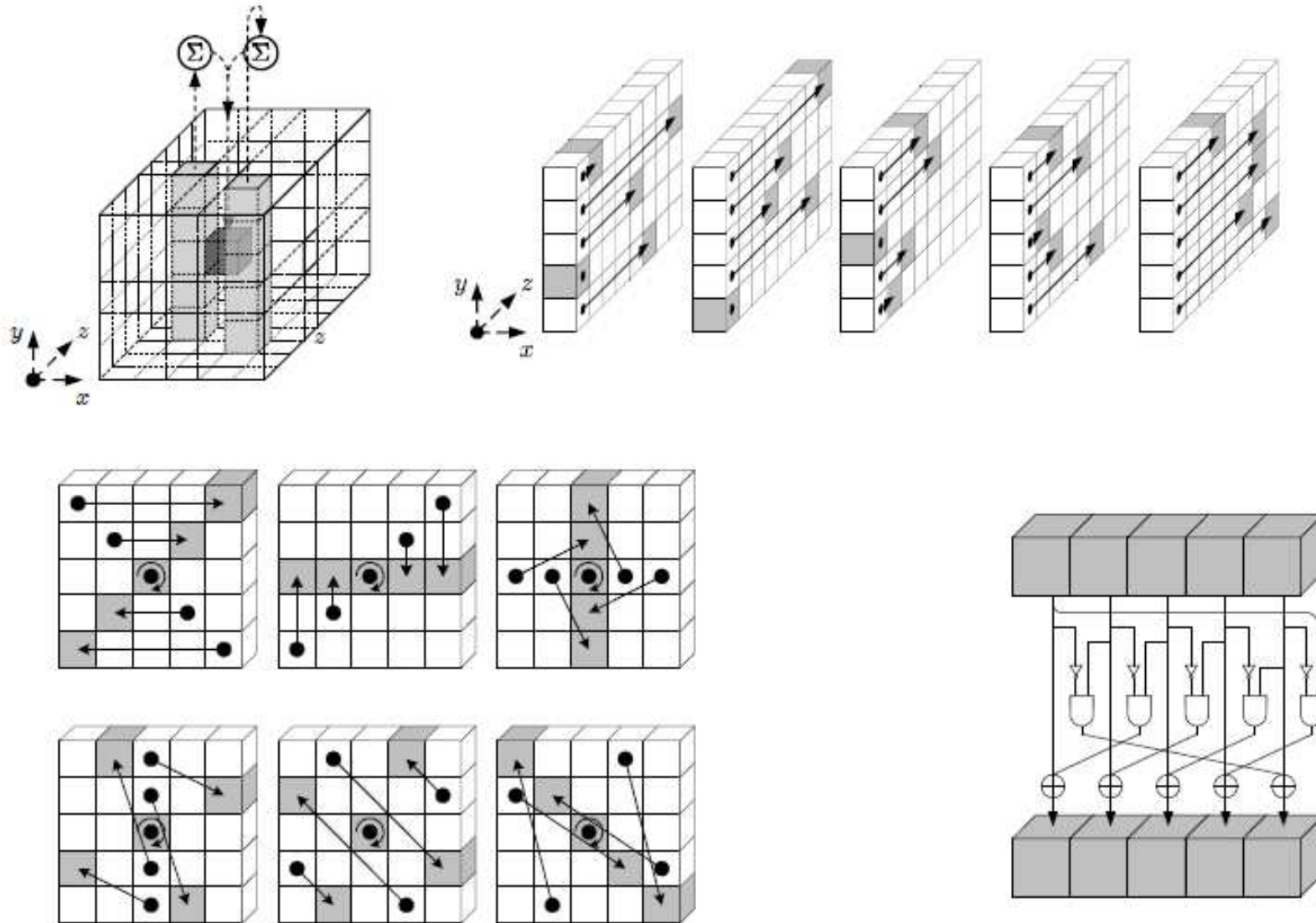
Participantes: 64 ! 51 ! 14 ! 5 ! 1

Keccak: función esponja



- Longitud entrada y salida variable.
- Parámetros
 - Estado compuesto de b bits, donde r de dichos bits son de velocidad (rate) y c son de capacidad.
- Usa una función de permutación.

Permutaciones en Keccak

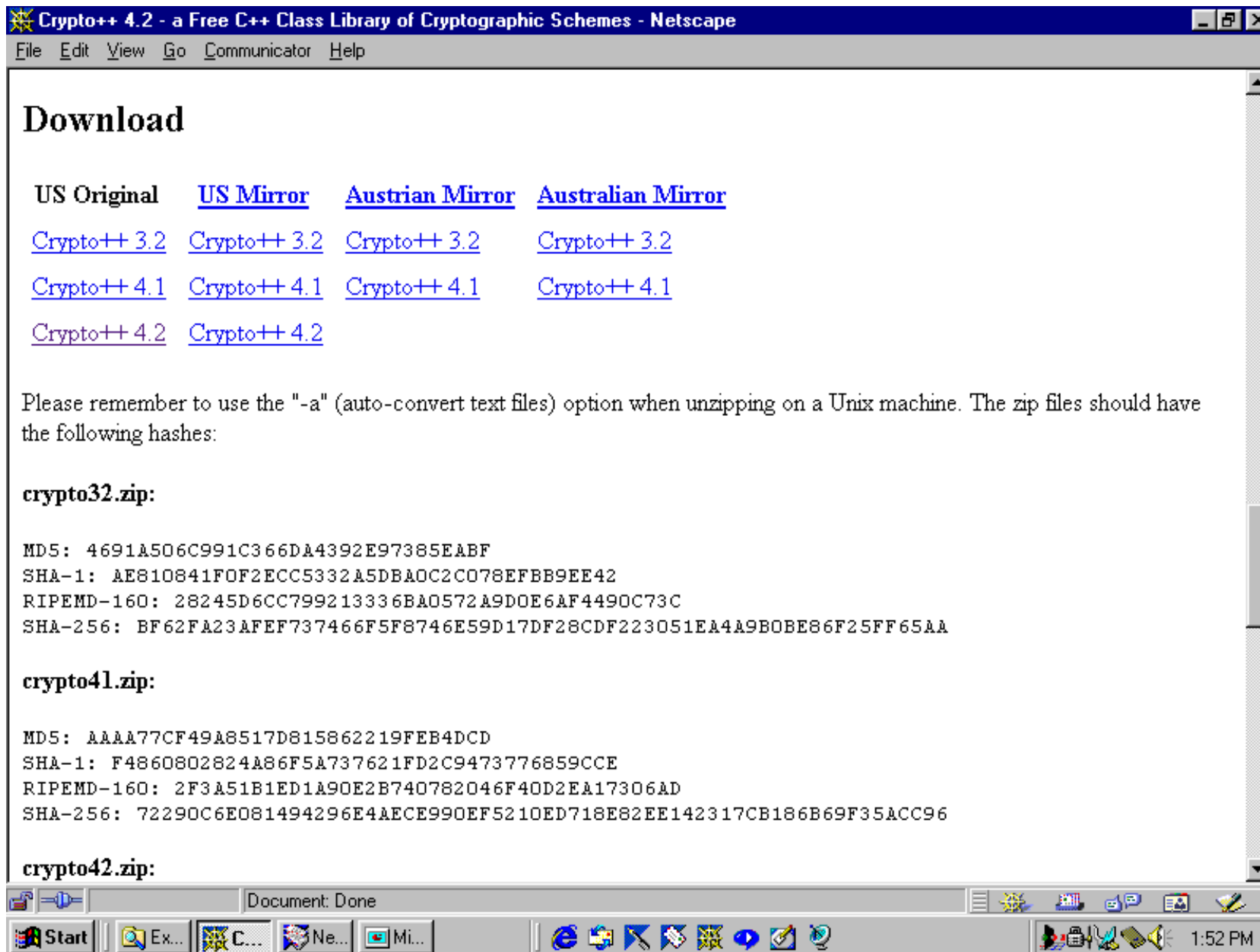


¿Porqué gano?

- Margen de seguridad alto
- Un calidad de análisis alto
- Diseño elegante, limpio
- Excelente desempeño a nivel hardware
- Buen desempeño global
- Diferente diseño de SHA2

Comparativo funciones hash

Algoritmo	Tamaño bloque	Tamaño salida
MD4	512	128
MD5	512	128
PANAMA	256	256
RIPEMD	512	128
RIPEMD-128/256	512	128/256
RIPEMD-160/320	512	160/320
SHA-0	512	160
SHA-1	512	160
SHA2 - 256/224	512	256/224
SHA2 - 512/384	1024	512/384
SHA3 – 224	1152	224
SHA3 – 256	1088	256
SHA3 – 384	832	384
SHA3 – 512	576	512



Crypto++ 4.2 - a Free C++ Class Library of Cryptographic Schemes - Netscape

File Edit View Go Communicator Help

Download

[US Original](#) [US Mirror](#) [Austrian Mirror](#) [Australian Mirror](#)

[Crypto++ 3.2](#) [Crypto++ 3.2](#) [Crypto++ 3.2](#) [Crypto++ 3.2](#)

[Crypto++ 4.1](#) [Crypto++ 4.1](#) [Crypto++ 4.1](#) [Crypto++ 4.1](#)

[Crypto++ 4.2](#) [Crypto++ 4.2](#)

Please remember to use the "-a" (auto-convert text files) option when unzipping on a Unix machine. The zip files should have the following hashes:

crypto32.zip:

```
MD5: 4691A506C991C366DA4392E97385EABF
SHA-1: AE810841F0F2ECC5332A5DBAOC2C078EFBB9EE42
RIPEMD-160: 28245D6CC799213336BA0572A9DOE6AF4490C73C
SHA-256: BF62FA23AFEF737466F5F8746E59D17DF28CDF223051EA4A9BOBE86F25FF65AA
```

crypto41.zip:

```
MD5: AAAA77CF49A8517D815862219FEB4DCD
SHA-1: F4860802824A86F5A737621FD2C9473776859CCE
RIPEMD-160: 2F3A51B1ED1A90E2B740782046F40D2EA17306AD
SHA-256: 72290C6E081494296E4AECE990EF5210ED718E82EE142317CB186B69F35ACC96
```

crypto42.zip:

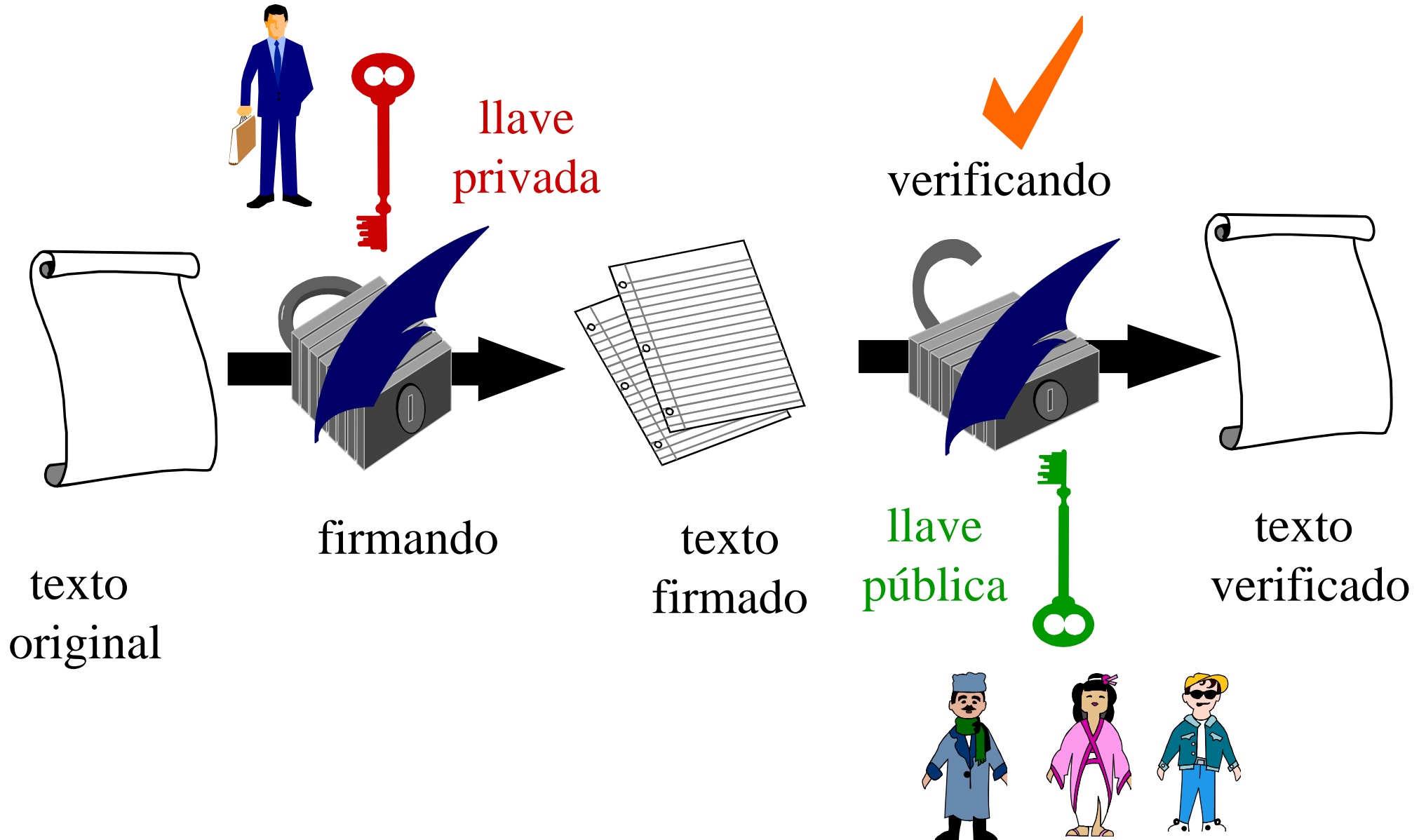
Document: Done

Start | Ex... | C... | Ne... | Mi... | 1:52 PM

¿Cómo se puede autenticar una comunicación?

- **Encriptación 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

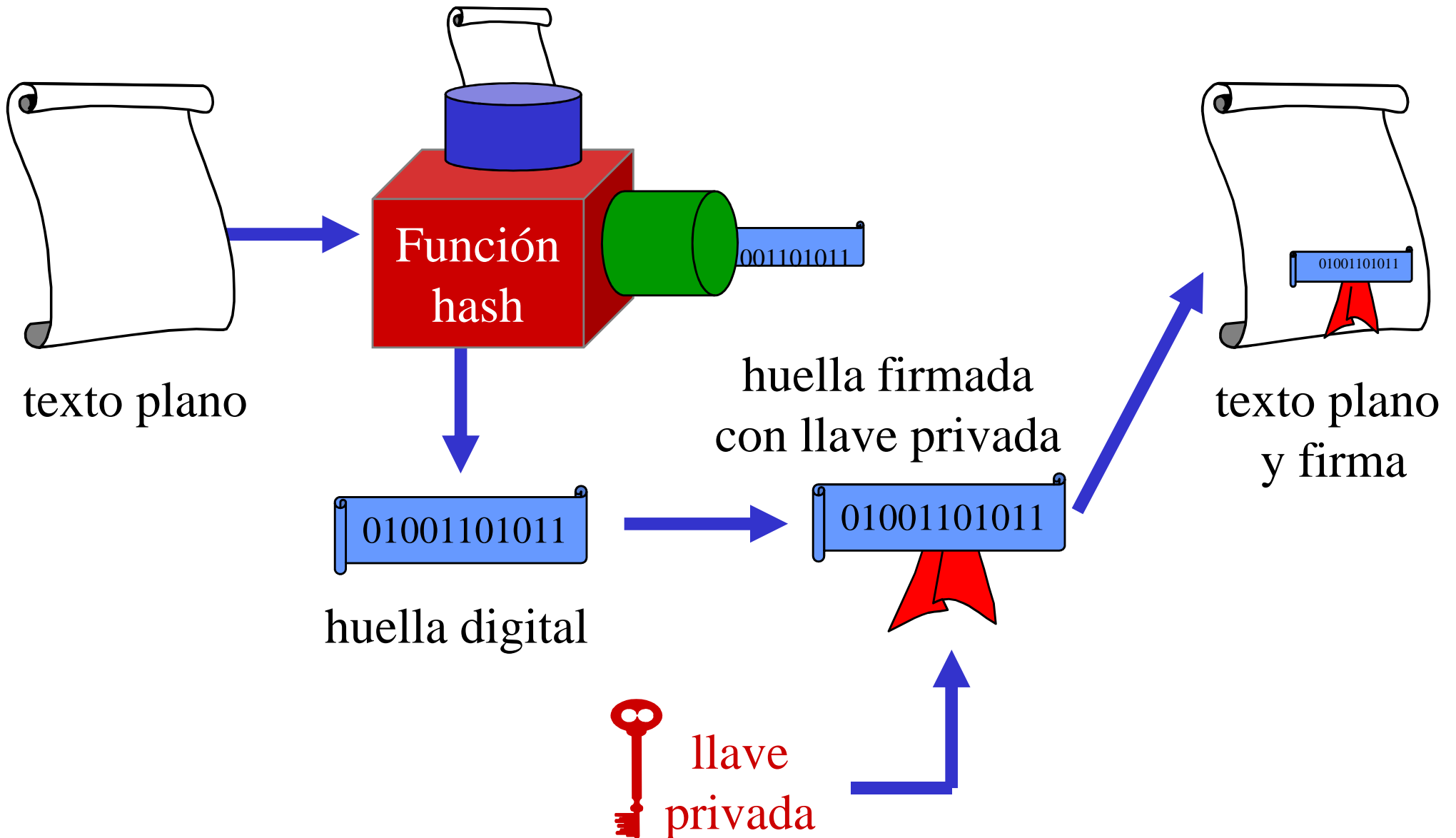
Un esquema de autenticación



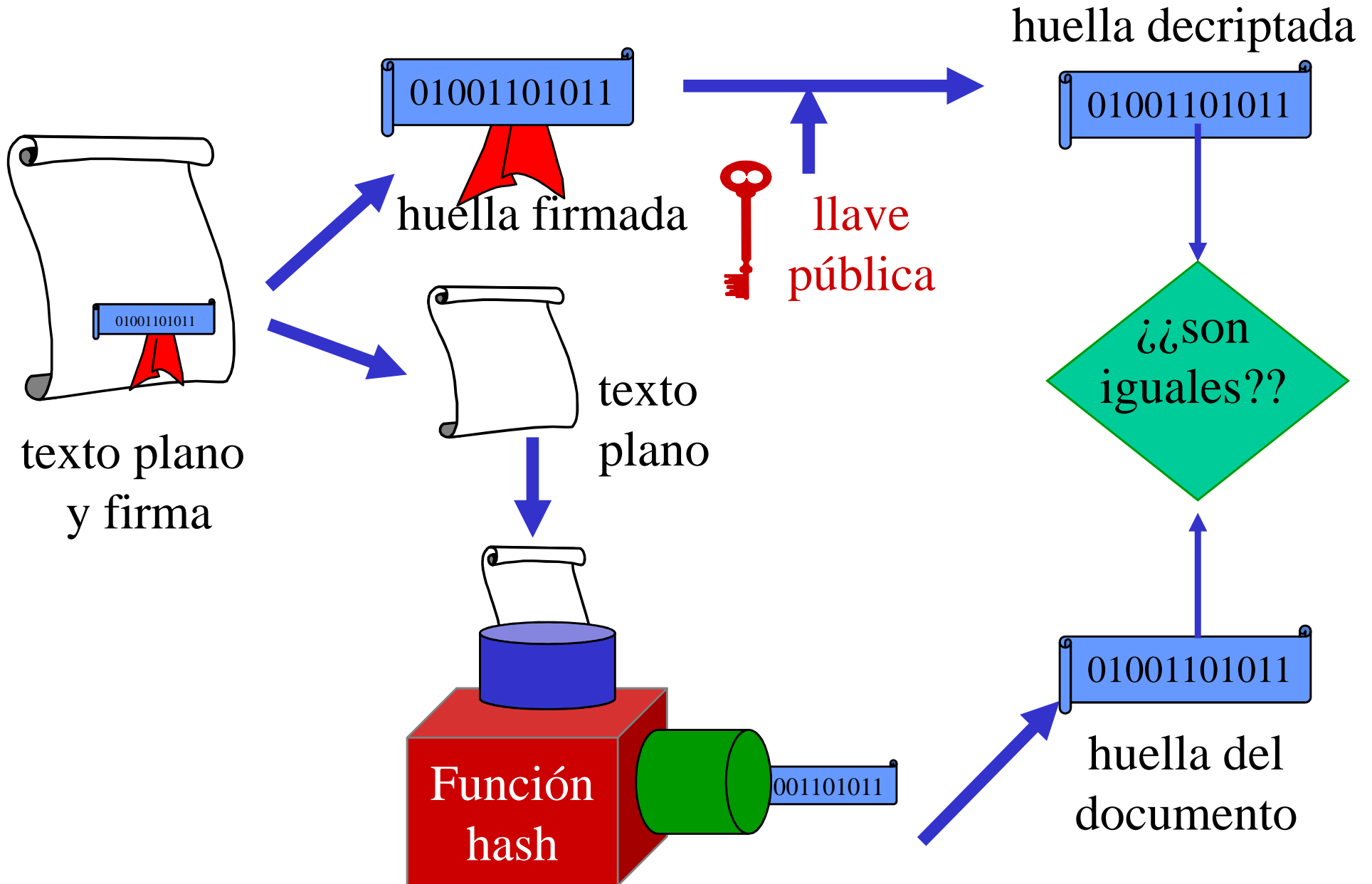
Firmas digitales

- Es posible usar una huella digital 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

Firma digital segura (envío)



Firma digital segura (recepción)



Estándares firmas digitales

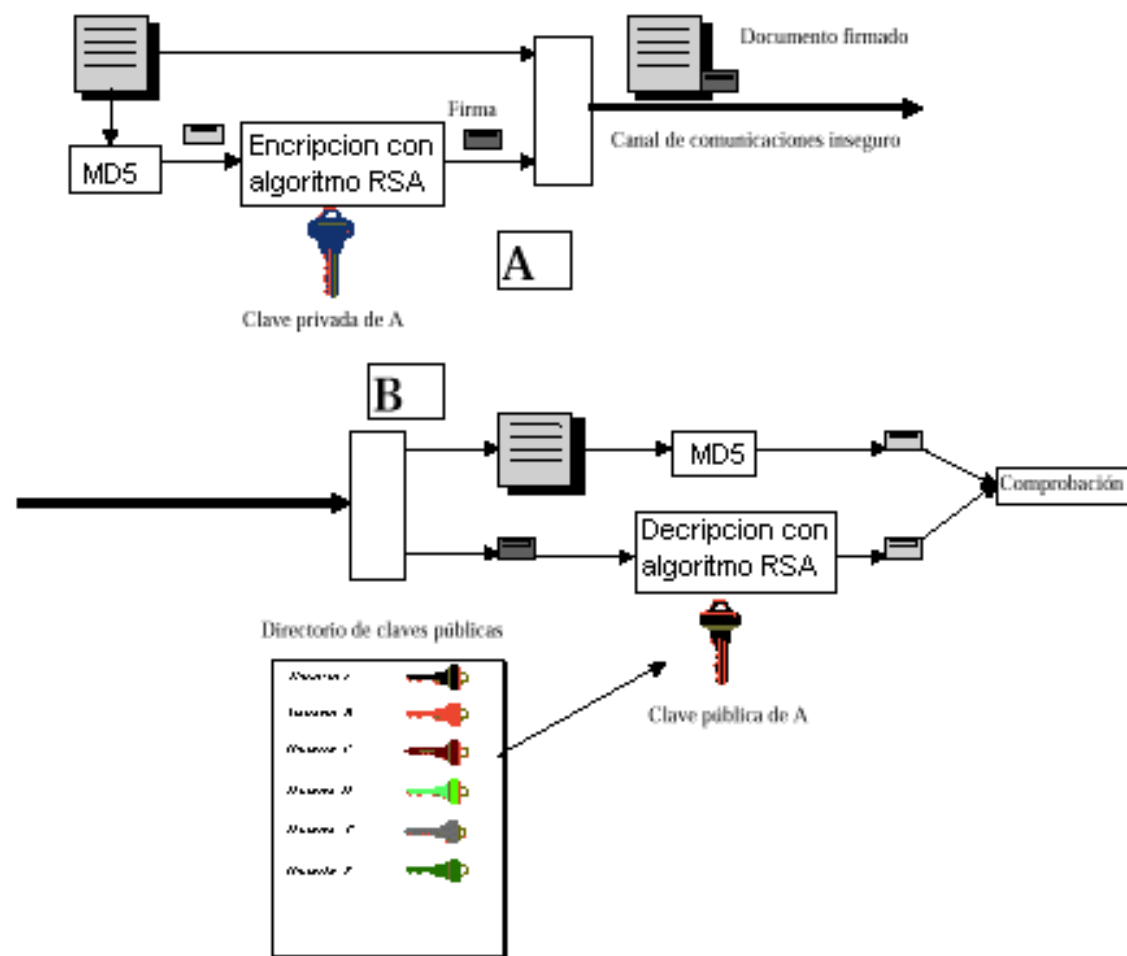
- Existen tres algoritmos aprobados como FIPS para producir una firma digital
 1. Digital Signature Algorithm (DSA)
 2. RSA (ANSI X9.31) y
 3. Elliptic Curve DSA (ECDSA -ANSI X9.62).

Diferencias RSA y DSS

	RSA	DSS
Algoritmo para cálculo del hash	MD5	SHA-1
Algoritmo de cifrado/descifrado	RSA	DSA
Desarrollador	RSA	NIST

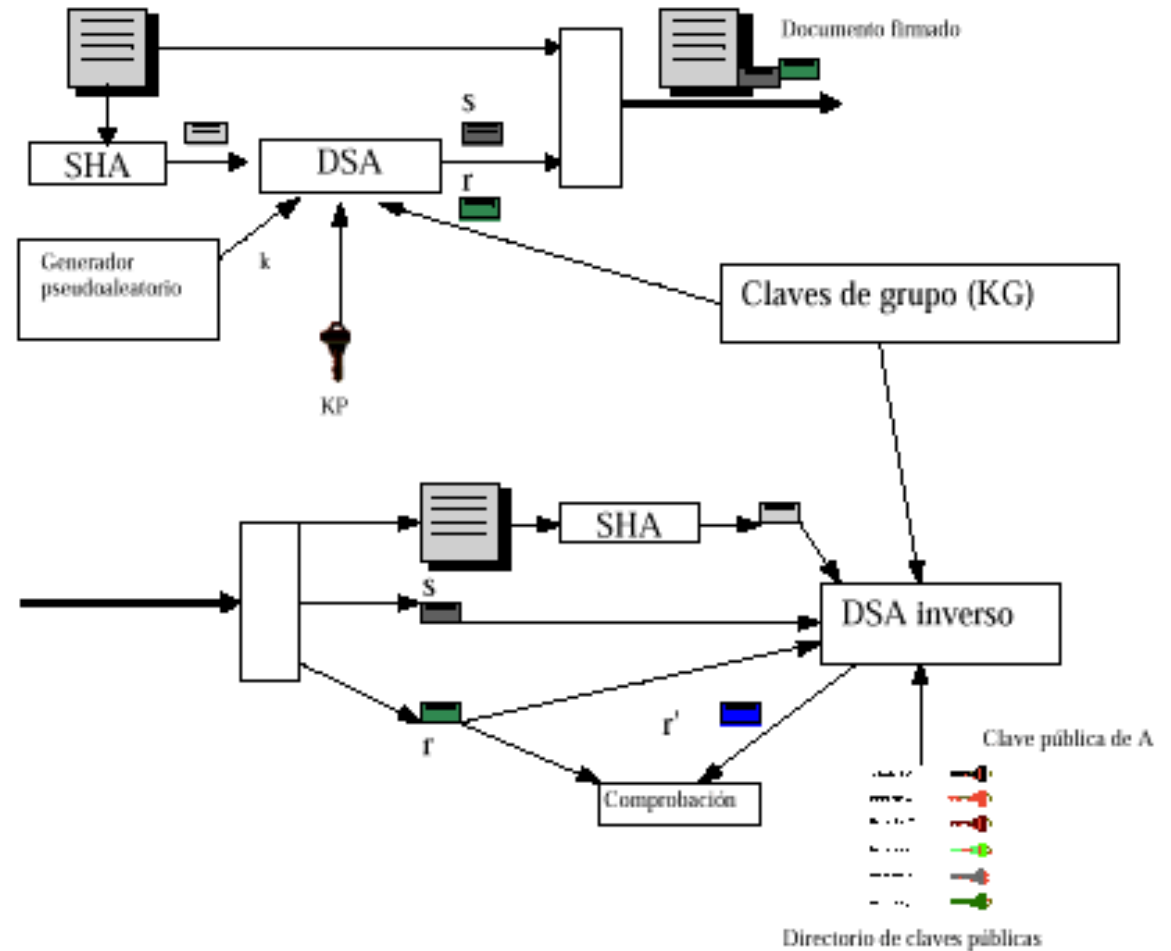
Algoritmo firma digital RSA

- Mismo principio de la firma
 - Algoritmo huella digital: MD5
 - Algoritmo encriptación/decriptación: RSA



Algoritmo firma digital DSS

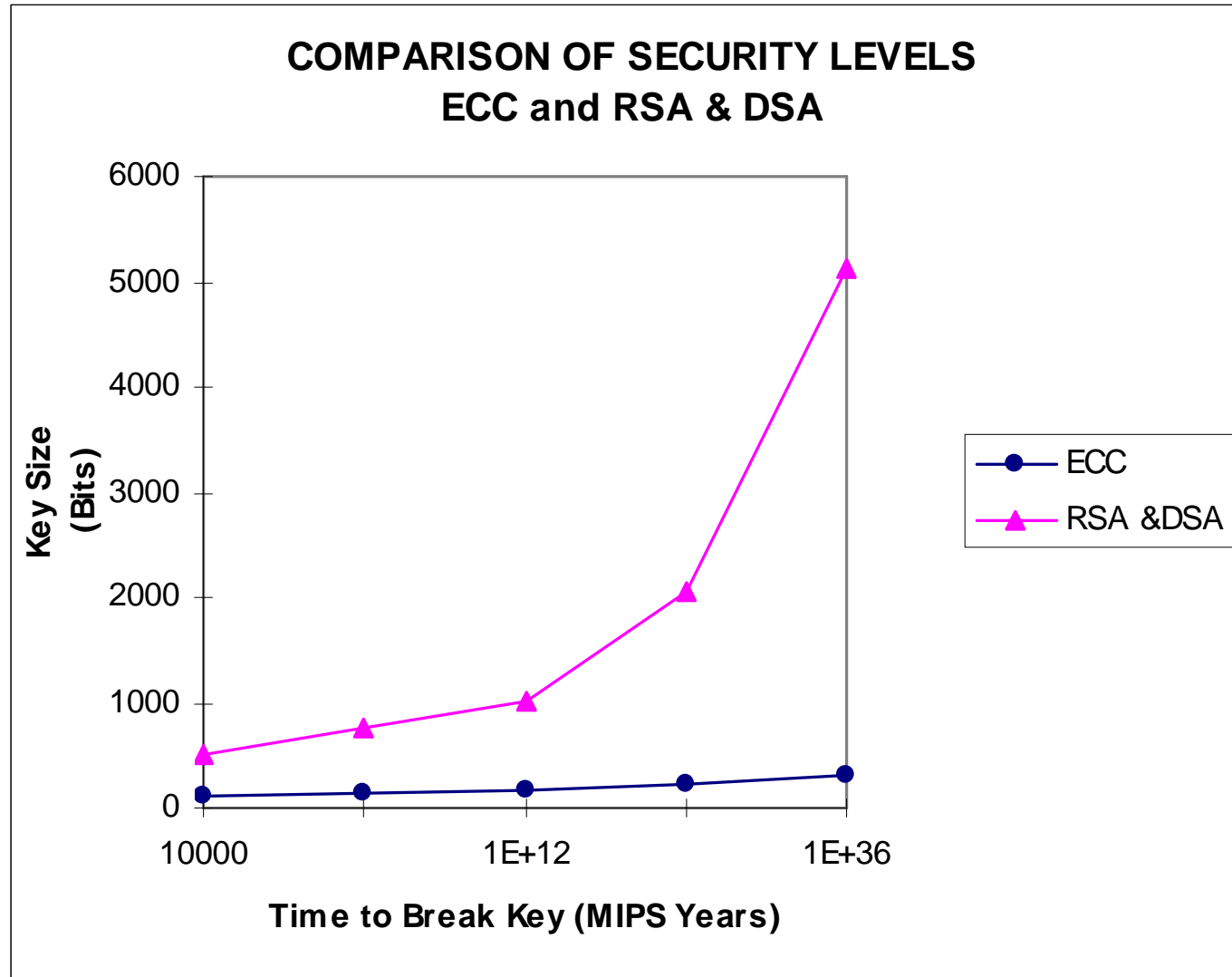
- Huella Digital
 - SHA-1
- Encriptación/decriptación
 - DSA



Firma digital y curvas elípticas

- ECDSA: Elliptic Curve DSA
- Modificación de algunos pasos en el algoritmo DSS en la selección de los números a usar
- El algoritmo de hash es el mismo
 - SHA-1
- El 15 febrero del 2000, NIST anuncia la publicación del FIPS 186-2, que substituye al FIPS 186-1 así como:
 - la aprobación del ECDSA
 - lista de curvas elípticas recomendadas para uso gubernamental

¿Porqué las curvas elípticas?



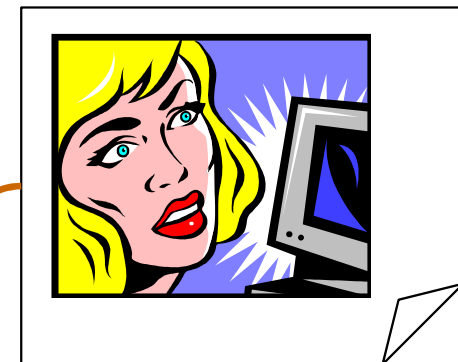
Referencia: Certicom white paper. Remarks on the Security of The Elliptic Curve Cryptosystem. Certicom. 1997

Algunos problemas de la criptografía de llave pública

¿Cómo estar
seguro de que esta
llave pública
pertenece a Alicia?

¿Cómo
obtengo la
llave pública
de Alicia?

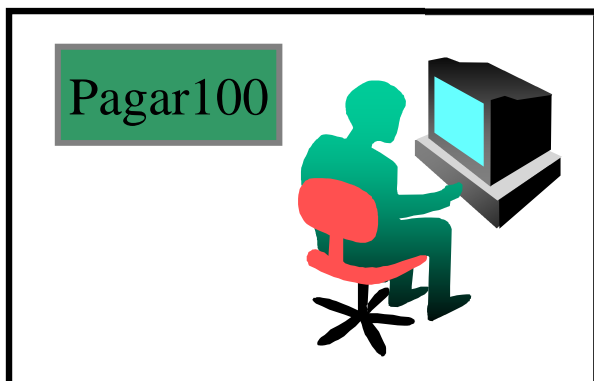
¿Cómo estar
seguro de que la
llave pública es
aún válida?



Solicitando una llave pública

Alicia

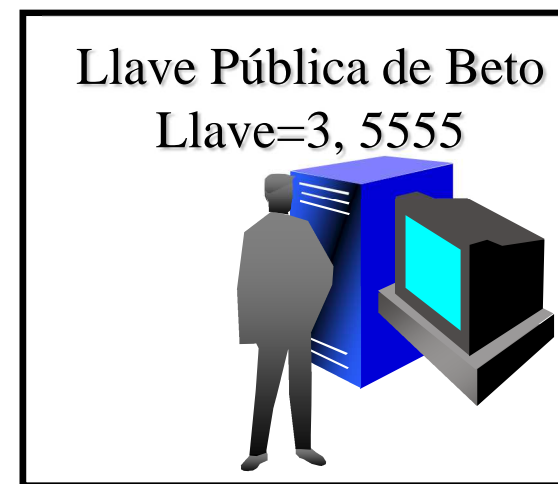
Alicia va a pagarle
100 pesos a Beto



“Solicita la Llave
Pública de Beto”

Entregando llave
pública de Beto
Llave=3, 5555

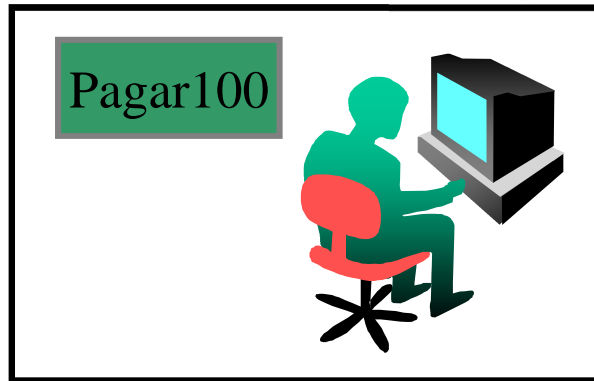
Beto



El ataque “Man in the Middle” (MIM)

Alicia

Alicia va a pagarle
100 pesos a Beto

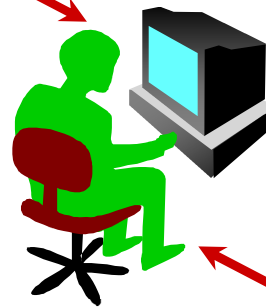


“Solicita la Llave
Pública de Beto”

Llave=3, FFFF

Cambiando
Llave=3, FFFF por
Llave=3, 5555

Sergio
“El Cambiador”



“Solicita la Llave
Pública de Beto”

Llave=3, 5555

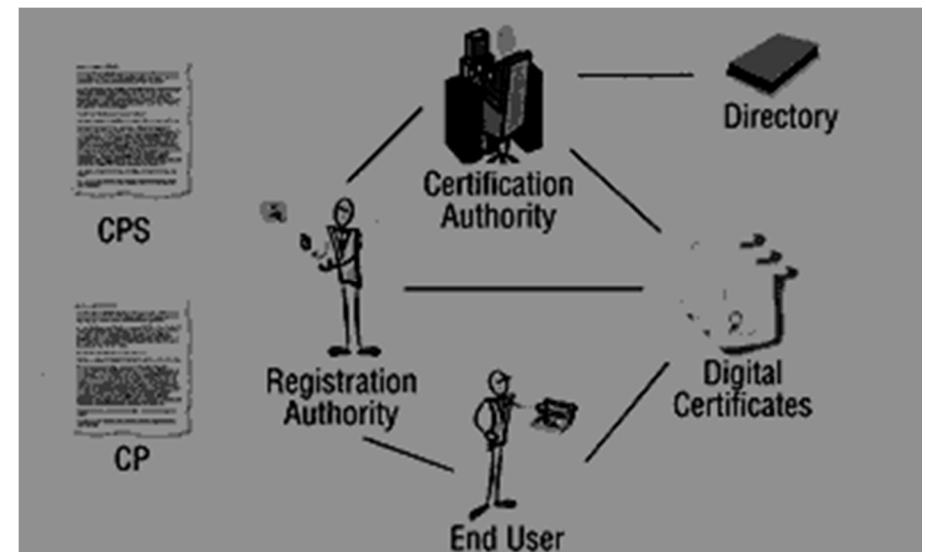
Beto



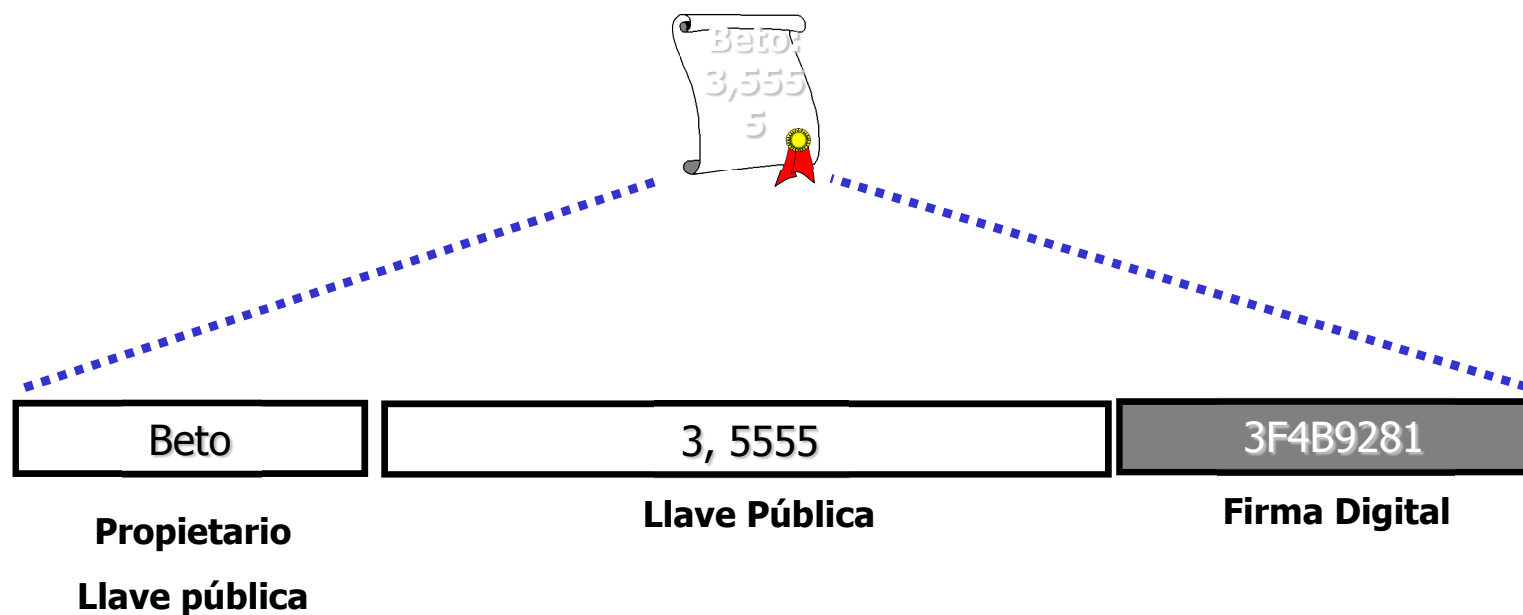
- Solución:
 - Intercambio de llaves públicas firmadas digitalmente con la llave privada de una 3a persona.
 - 3a. persona de confianza que de a conocer su llave pública.
- Certificado digital:
 - Archivo o estructura de datos que funciona como una identificación para el propietario.
 - Amarra la llave pública del usuario a su identidad.
 - Emitido por una autoridad certificadora (CA), que:
 - contiene una llave pública
 - identifica al dueño de la llave,
 - especifica la vigencia del certificado e
 - incluye la firma digital de la CA.
 - Propósito: mostrar que una llave pública pertenece en verdad a una persona.

Autoridades Certificadoras (CAs)

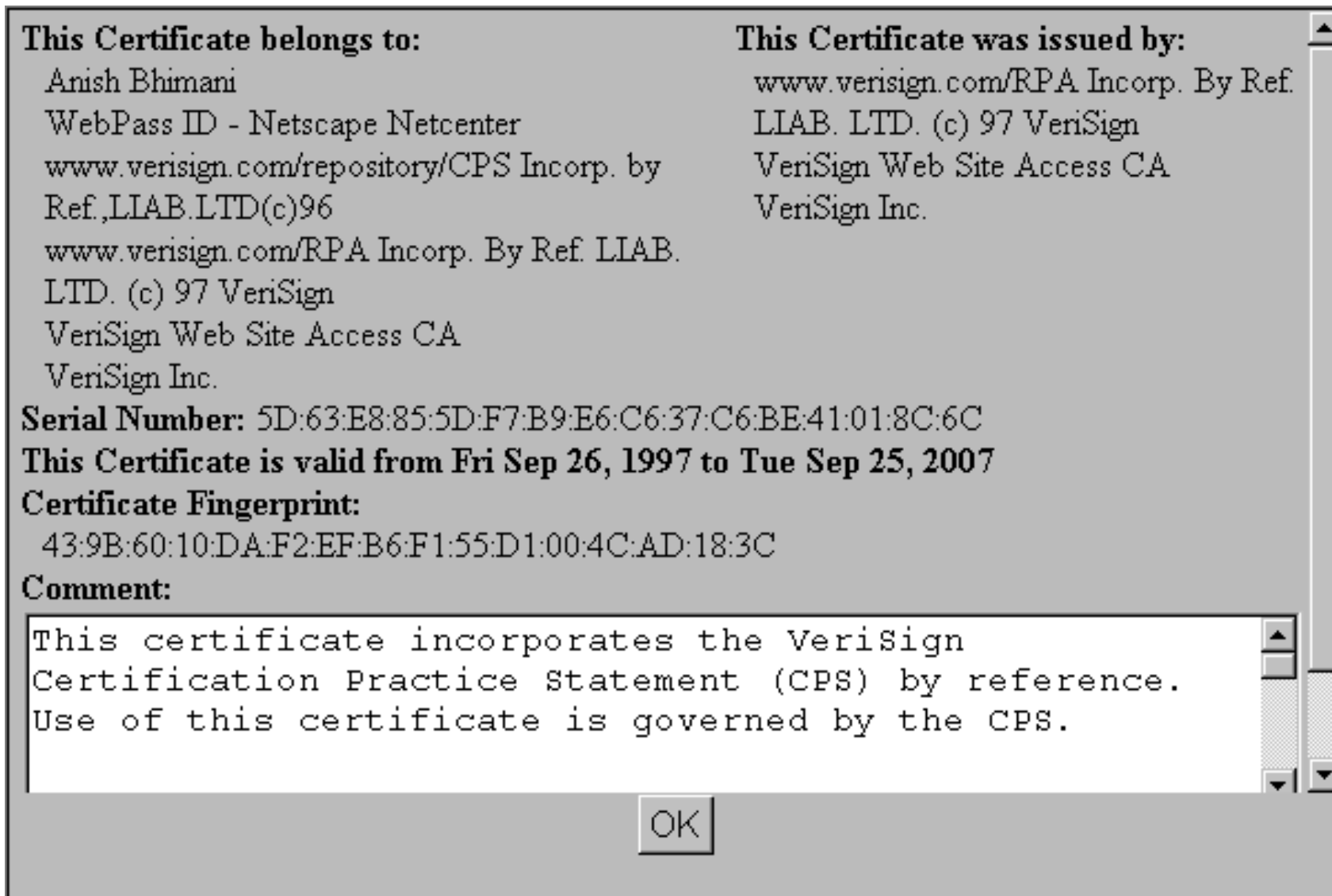
- Certificados son expedidos por autoridades confiables conocidas como Autoridades Certificadoras.
- Organismo interno confiable o tercera parte también confiable que respalda (vouches) la identidad de un dispositivo o individuo, mediante la emisión de un certificado y la llave privada correspondiente.
- Se responsabiliza por la gente a la cual emitió el certificado:
 - Compañía a sus empleados
 - Universidad a sus estudiantes
 - CA Pública (Verisign) a sus clientes



El contenido de un Certificado Digital



Ejemplo Certificado Digital



This Certificate belongs to:
Anish Bhimani
WebPass ID - Netscape Netcenter
www.verisign.com/repository/CPS Incorpor. by
Ref.,LLAB.LTD(c)96
www.verisign.com/RPA Incorpor. By Ref. LLAB.
LTD. (c) 97 VeriSign
VeriSign Web Site Access CA
VeriSign Inc.

This Certificate was issued by:
www.verisign.com/RPA Incorpor. By Ref.
LLAB. LTD. (c) 97 VeriSign
VeriSign Web Site Access CA
VeriSign Inc.

Serial Number: 5D:63:E8:85:5D:F7:B9:E6:C6:37:C6:BE:41:01:8C:6C

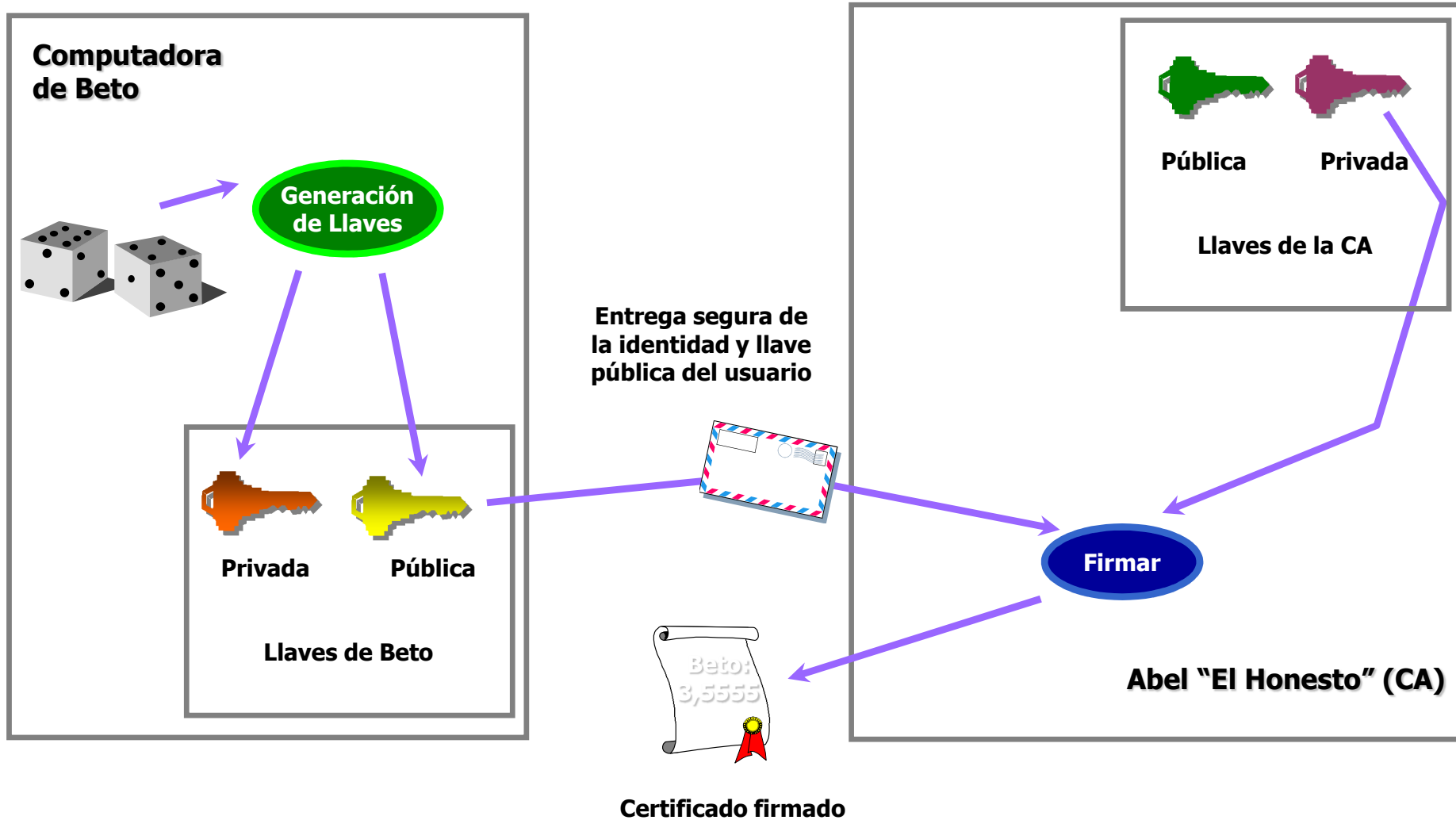
This Certificate is valid from Fri Sep 26, 1997 to Tue Sep 25, 2007

Certificate Fingerprint:
43:9B:60:10:DA:F2:EF:B6:F1:55:D1:00:4C:AD:18:3C

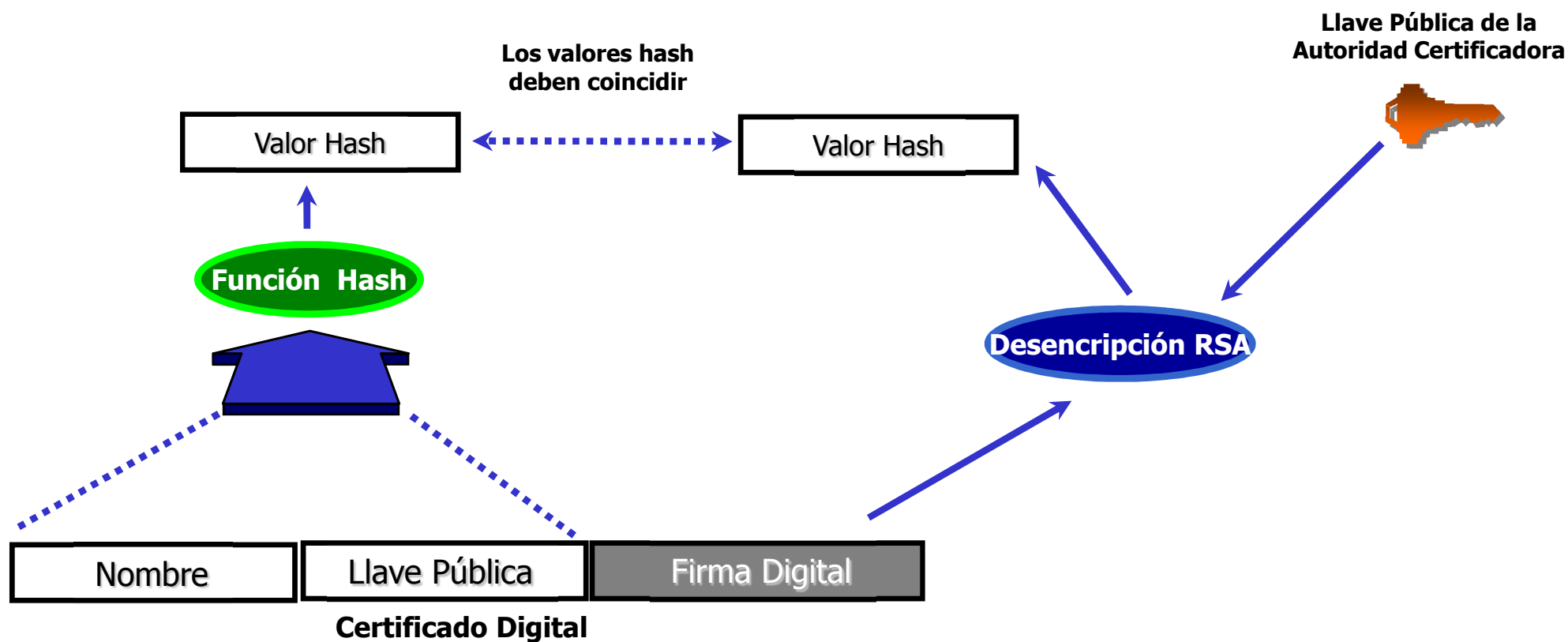
Comment:
This certificate incorporates the VeriSign
Certification Practice Statement (CPS) by reference.
Use of this certificate is governed by the CPS.

OK

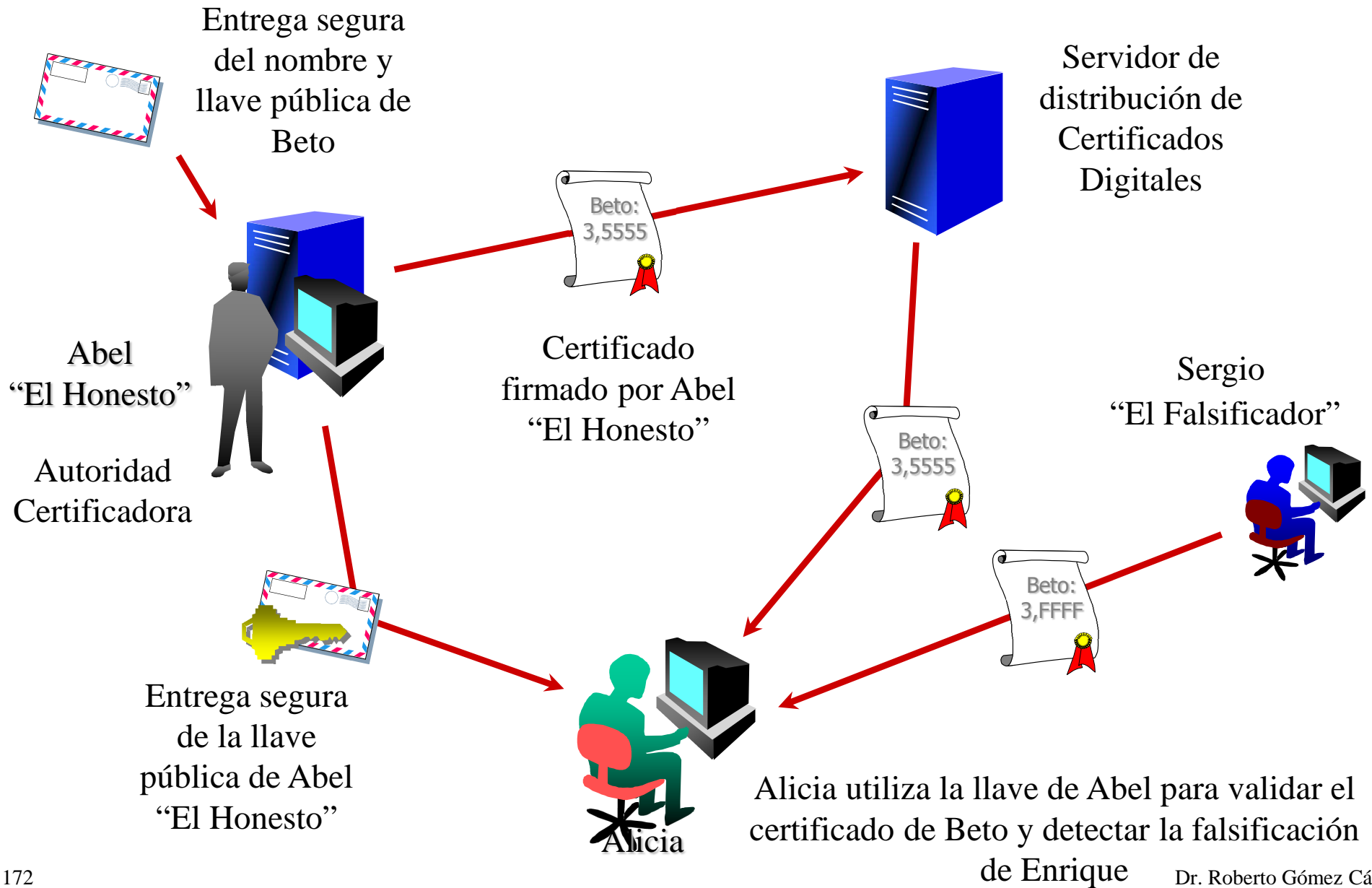
La generación de un certificado digital



La validación de un certificado digital



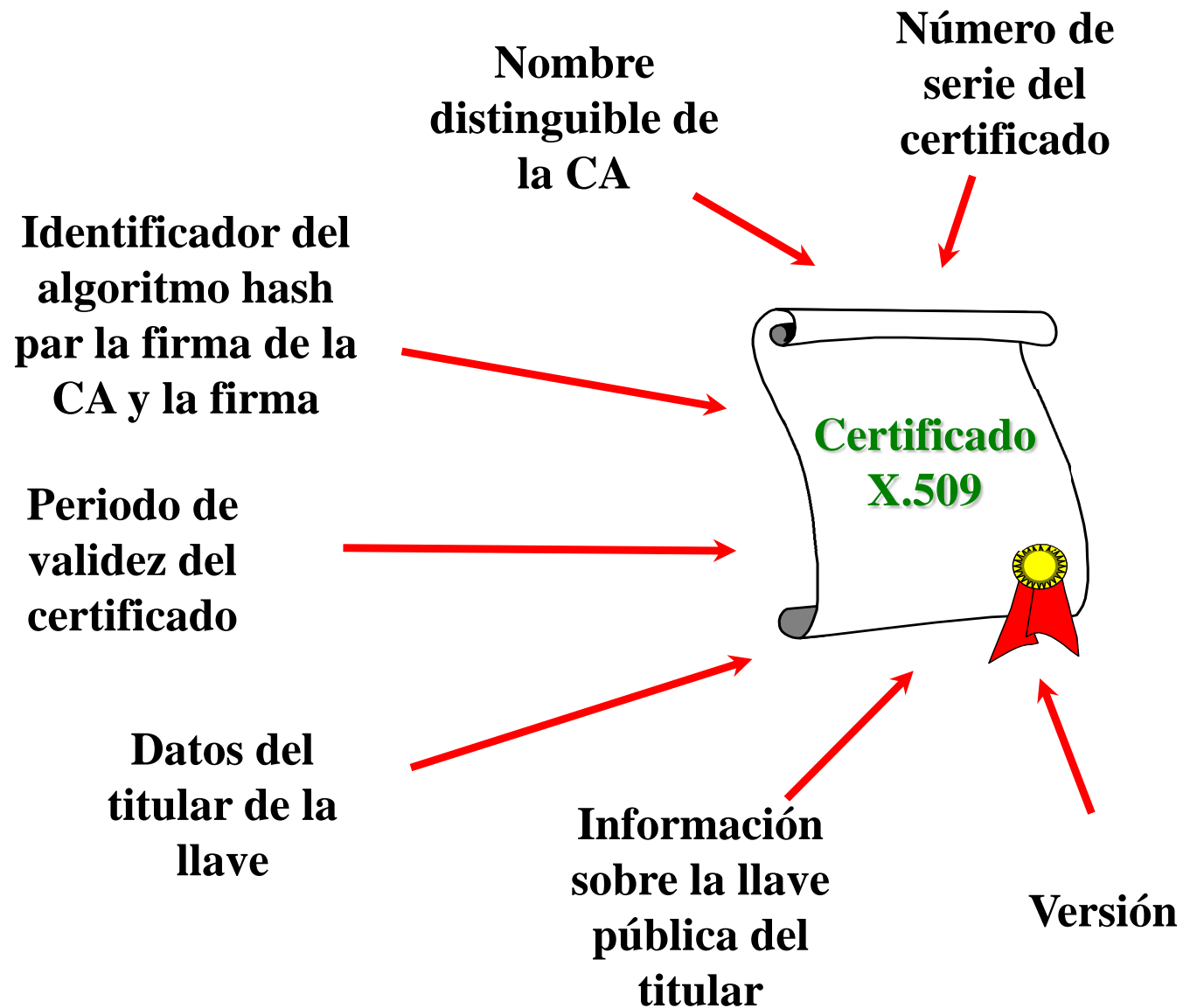
¿Cómo funciona todo?



El formato X.509

- El estándar base es el ITU-T X.509
 - Alineado con el ISO/IEC 9594-8
- Forma parte del servicio de directorios X.500 (UIT-T)
- Debe contener información tanto de la entidad que lo solicitó como de la Autoridad Certificadora que lo expidió.
 - Tres versiones: v1, v2, v3
- Define un entorno de trabajo para provisión de servicio de autenticación:
 - Formato de certificado.
 - Protocolo de autenticación basado en clave pública.

Elementos estándar X.509



Contenido de un certificado

Data:

Version: 1 (0x0)

Serial Number: 18 (0x12)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ES, ST=Madrid, L=Madrid, O=Lexus, OU=TI, CN=Lexus Certificate Server

Validity

Not Before: Jan 7 13:02:39 2000 GMT

Not After : Jan 6 13:02:39 2001 GMT

Subject: C=ES, L=Madrid, O=Lexus, OU=Ventas, CN=Javier Gallego/Email=jgallego@lexus.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (512 bit)

Modulus (512 bit):

00:98:59:ab:d9:7e:a3:40:21:60:ee:54:a5:a4:54:

d2:29:fd:50:82:c1:28:05:25:0a:6b:aa:61:aa:e0:

19:3b:d7:5e:18:f2:14:60:ed:58:f6:87:eb:4c:61:

fc:9e:ed:9d:b2:19:d4:73:25:cc:d4:63:88:54:f4:

49:2a:ba:ce:7b

Exponent: 65537 (0x10001)

Signature Algorithm: md5WithRSAEncryption

7a:df:8a:aa:b5:23:5b:c6:ff:f3:02:73:65:bb:0f:05:7a:fd:

f4:68:ee:b9:fe:92:72:53:bb:f2:31:9e:38:92:69:b3:04:22:

d7:be:f5:18:42:7a:c0:9b:e2:1e:04:a4:66:02:80:76:79:0e:

f6:c3:7e:25:2d:ec:00:01:fb:f7

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 cuánto tiempo es válida esta lista y cuando obtener la siguiente.

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 cuánto tiempo es válida esta lista y cuando obtener la siguiente.

Tipos certificados y autoridades certificadoras

- Existen diferentes tipos de certificados
 - Certificado personal
 - Certificado servidor
 - Certificado correo seguro
 - Certificado autoridad certificadora
 - Certificados código
- Existen diferentes formas en que las CA ofrecen sus servicios:
 - CA interna
 - CA externa de empleados
 - CA externa de clientes
 - CA de terceros (cross-certification)

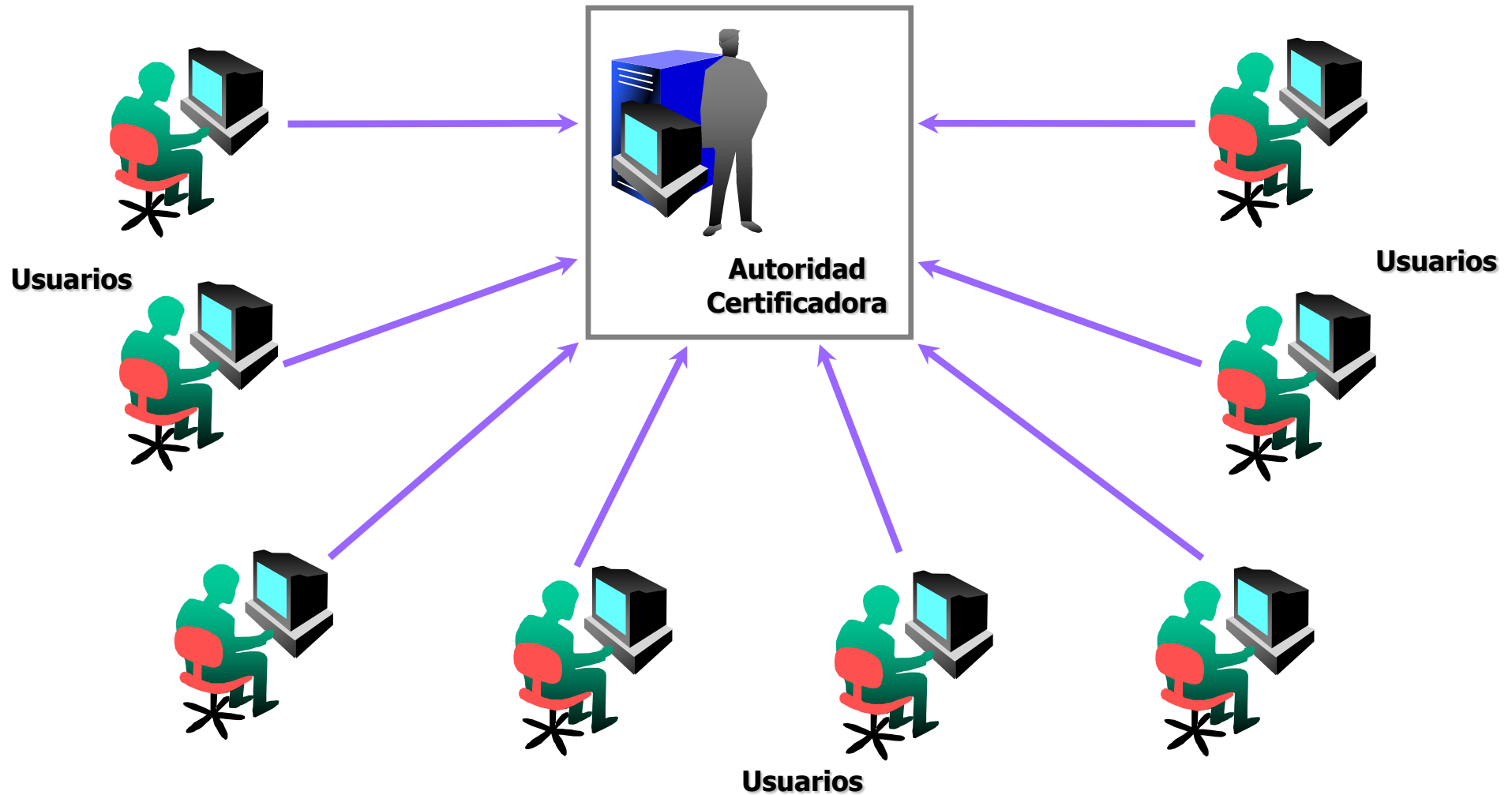


**Ese momento desafortunado cuando 2
cybernautas se encuentran cara a cara**

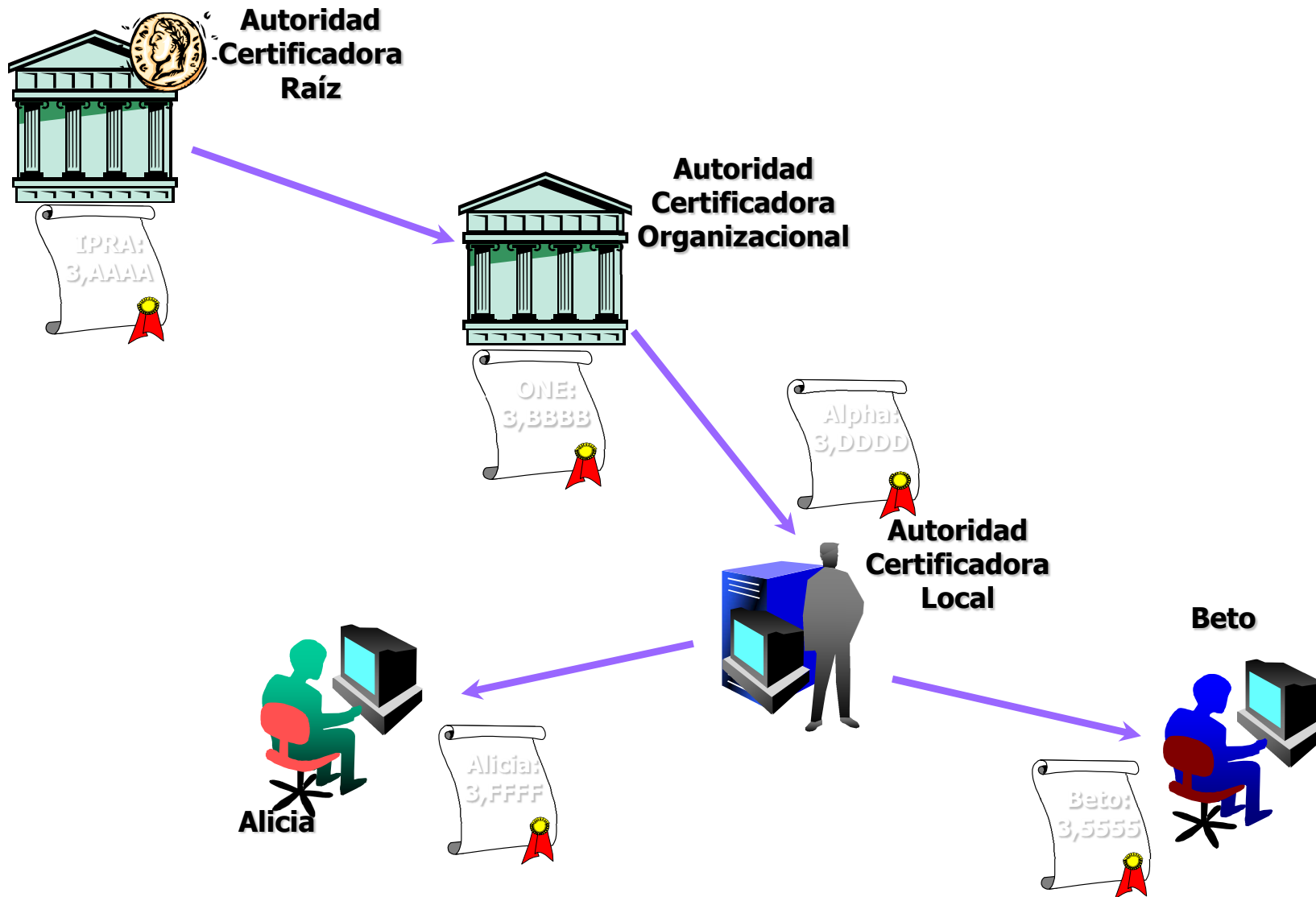
Modelos de confianza

- La entidad “A” confía en la entidad “B” cuando “A” supone y asume que “B” se comportará exactamente como “A” espera.
- Jerárquico
 - Basado en la relación Superior / Subordinado
 - Actualmente es la regla en ambiente de web
 - Mientras mas cercano al nivel root se comprometa una llave mayor será el impacto para la organización
- Distribuido
 - Es una red distribuida basada en una certificación cruzada “Cross Certification”
 - Mas flexible tanto en ambientes intra/inter organizacionales

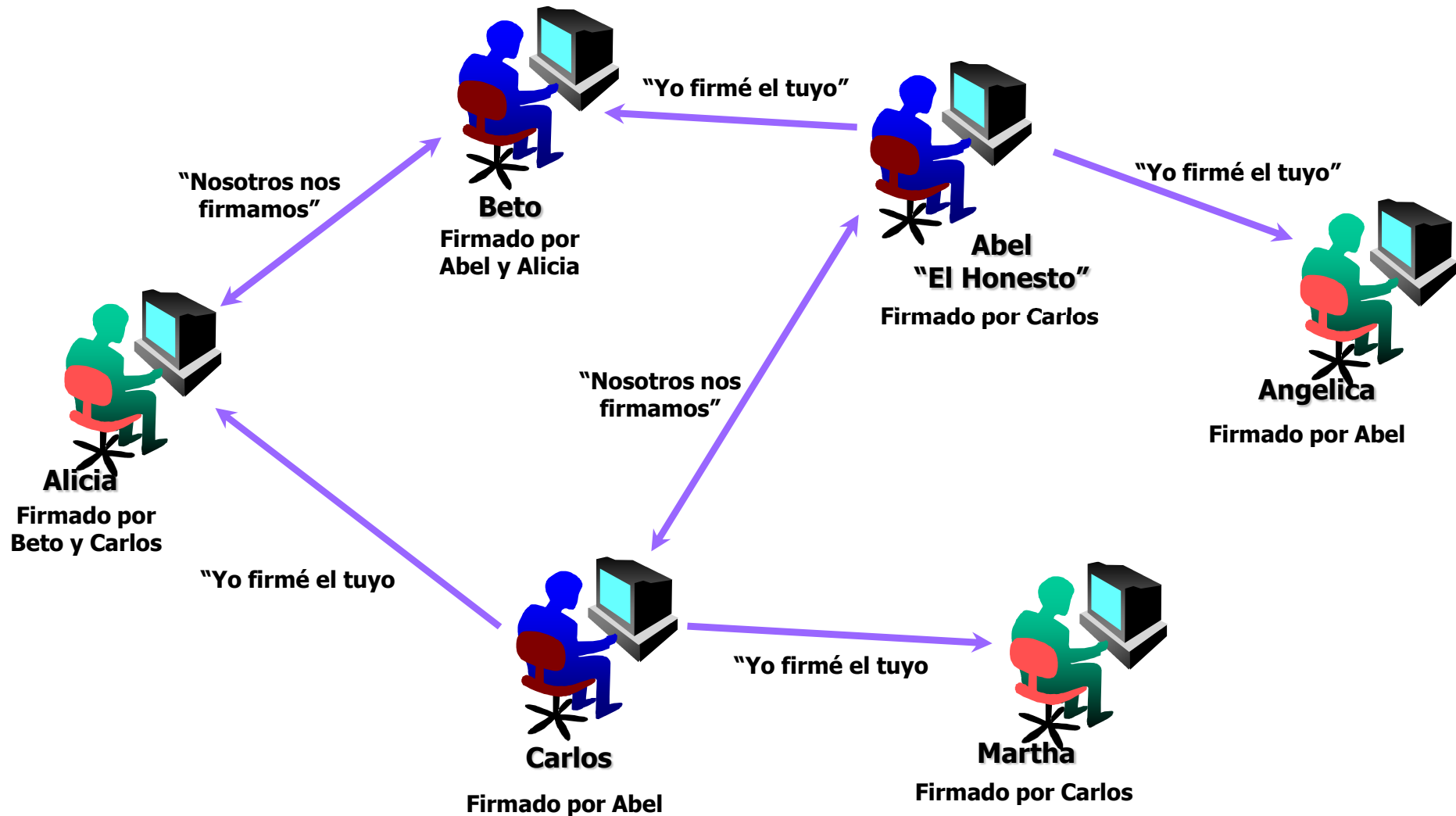
Modelo Centralizado



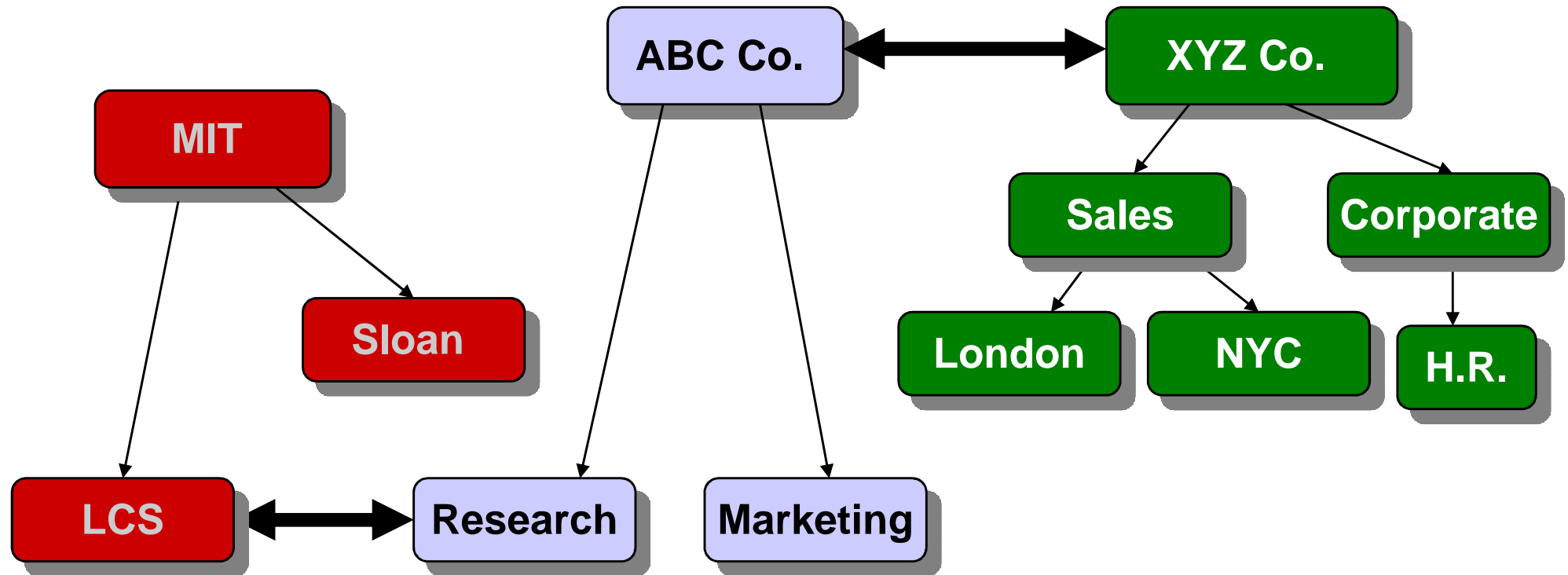
Modelo Jerárquico



“Web of Trust” de PGP



Ejemplo de Cross-Certification

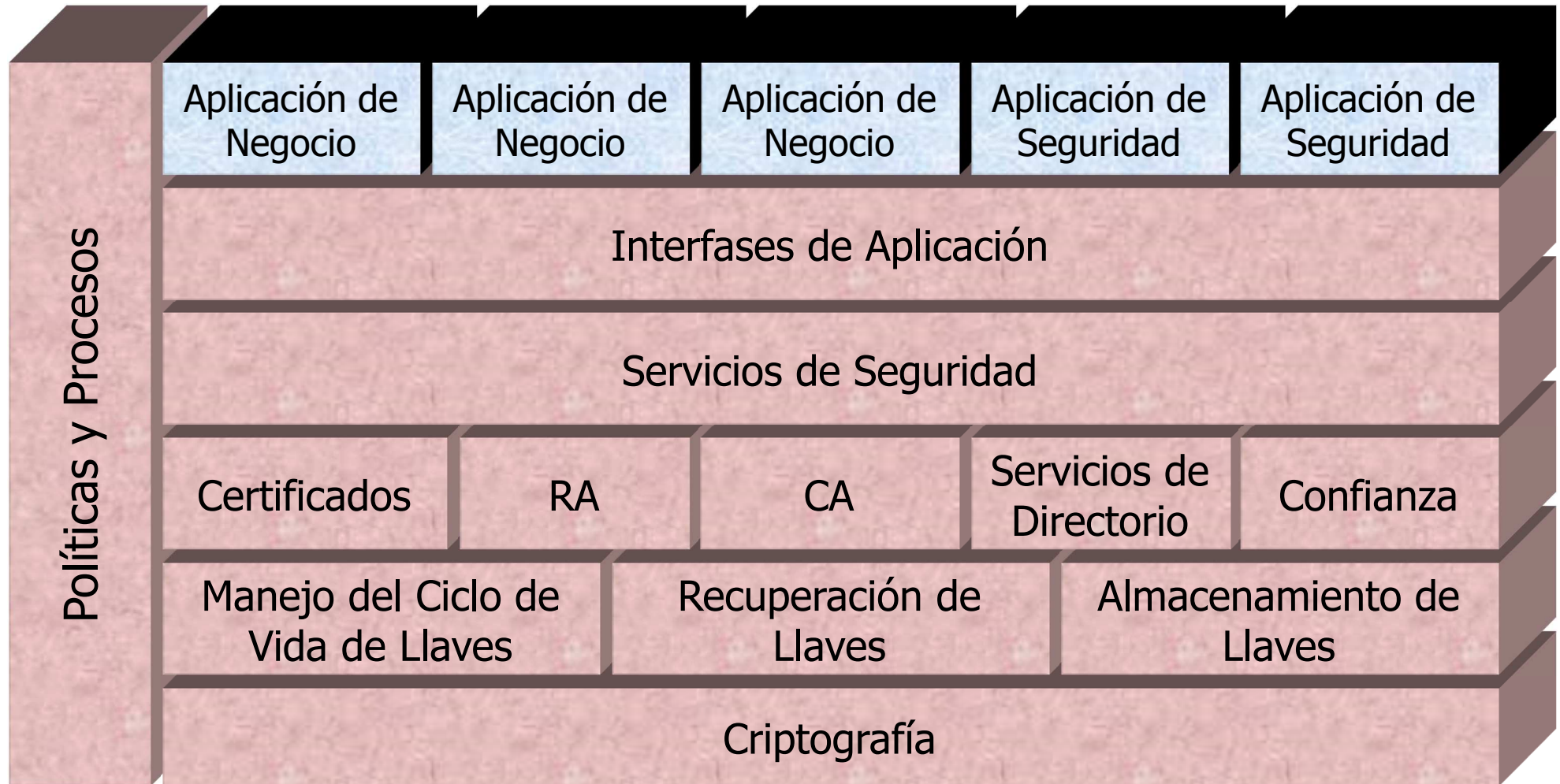


Infraestructura de llave pública (PKI)

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.

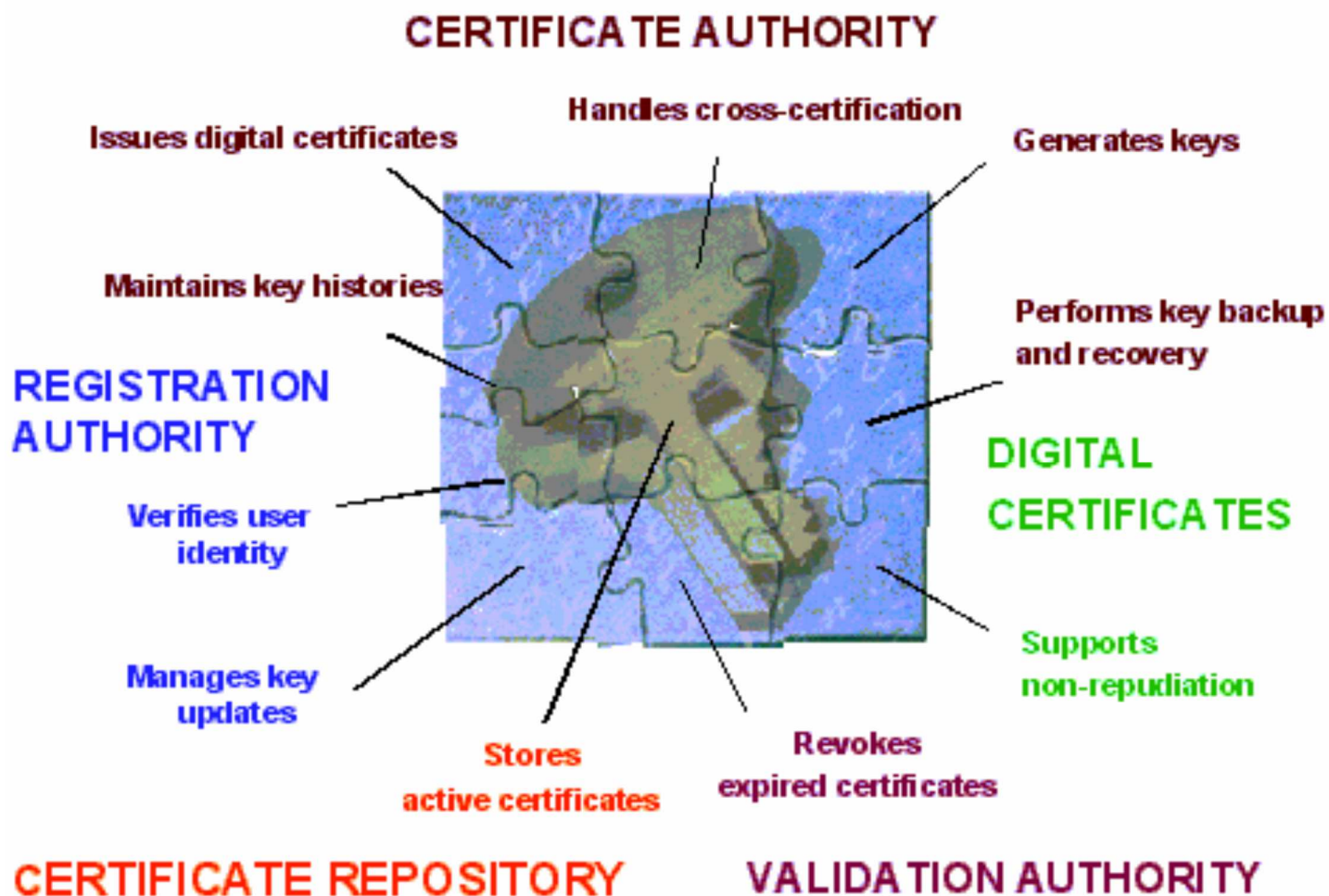
PKI's son 80% políticas y 20% tecnología

Componentes de una PKI

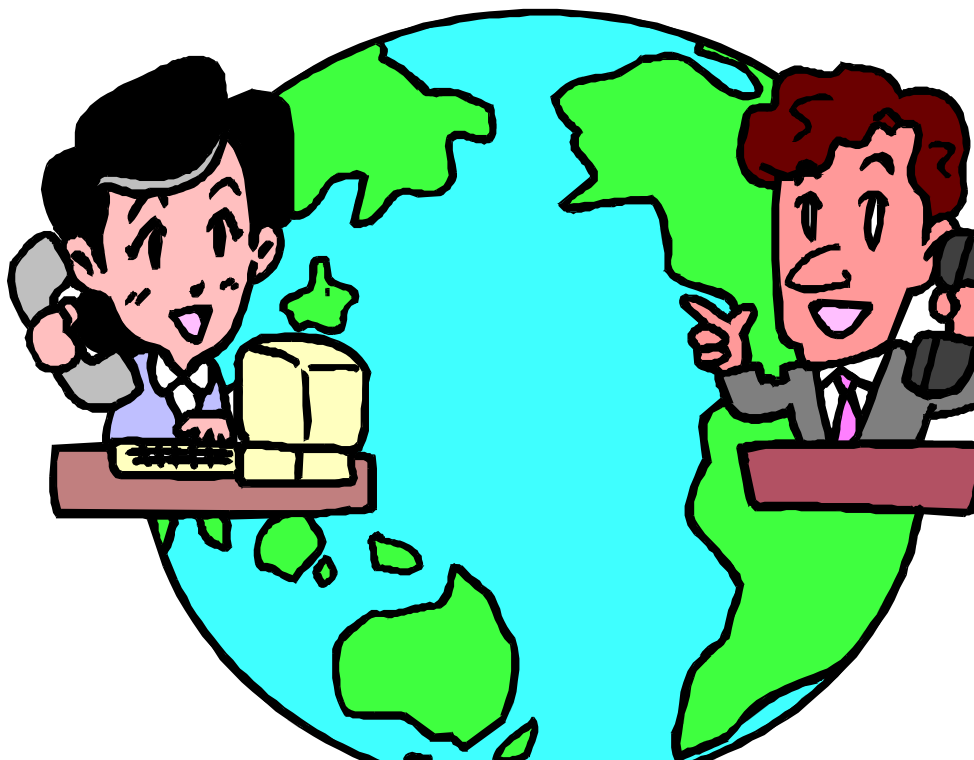


Componentes y funciones de una PKI

- Autoridad certificadora
- Certificados digitales
- Autoridad de validación
- Repositorio de certificados
- Autoridad de registro



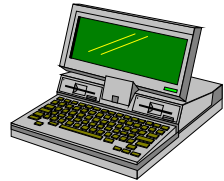
Protocolos de transmisión de datos seguros en Internet



SSL, PCT y TLS

- Protocolos criptográfico de propósito general para asegurar canales de comunicación bidireccionales
 - SSL: Secure Socket Layer
 - PCT: Private Communication Technology
 - TLS: Transport Layer Security
- Se utilizan comúnmente junto con el protocolo TCP/IP
- Sistema cifrado usado por navegadores como Netscape, Firefox, Safari e Internet Explorer

Criptografía y canales seguros



Cliente

Hola

Hola

Como estas

Muy bien



Quiero pagar

Toma mi llave pública

**Te envio una llave nueva
encriptada con tu llave pública**



Servidor

No hay autenticación
ni privacidad, ni
encriptación

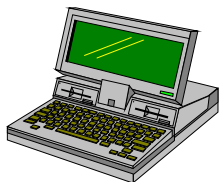
Hablemos en forma
segura



Generando
llave
simétrica

Comunicación encriptada con la llave enviada por el cliente

Otro posible escenario



Cliente

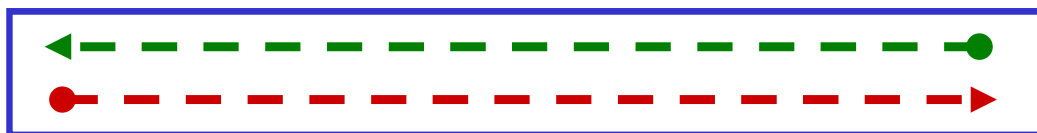


Servidor

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

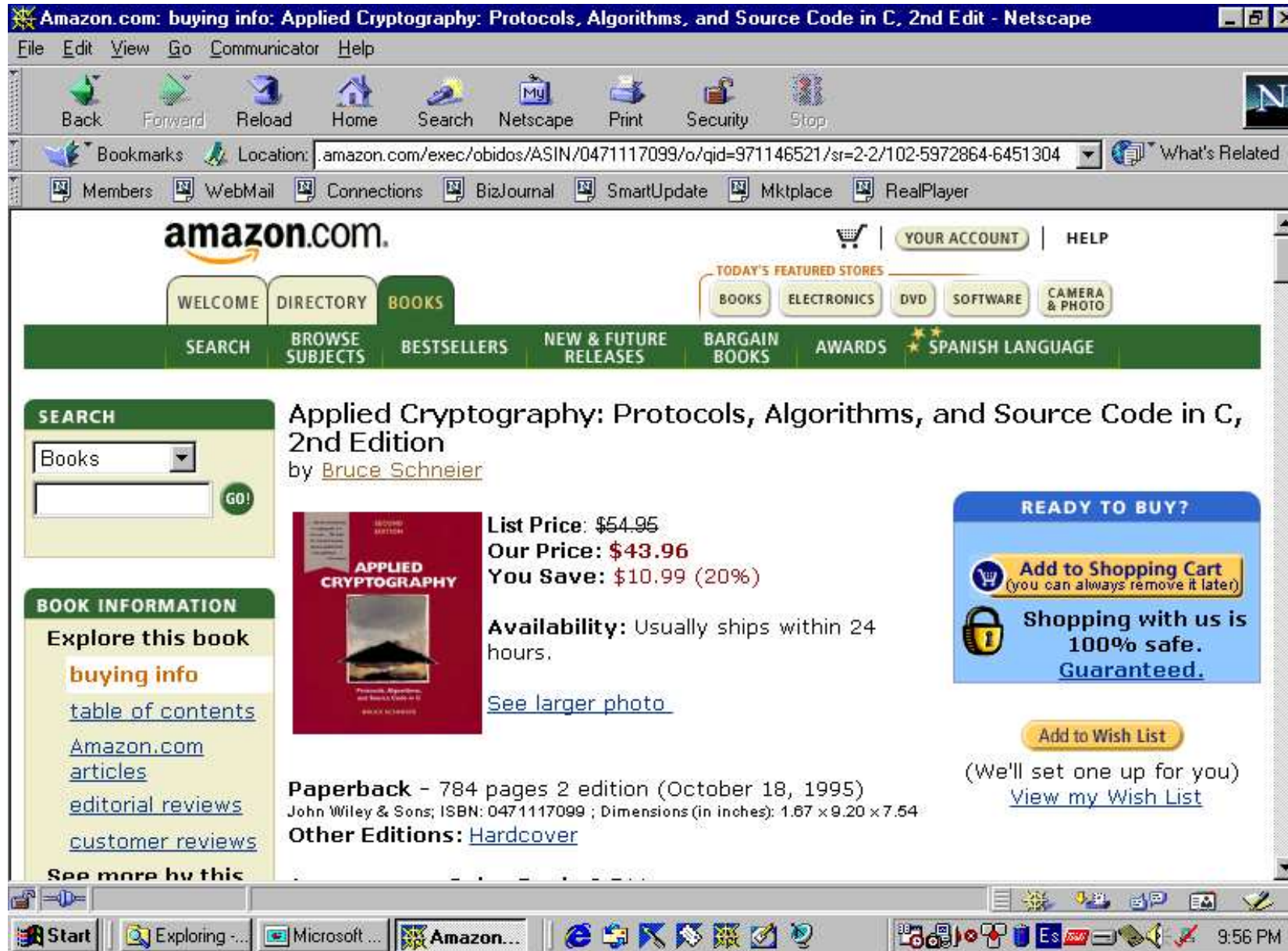
**Escogo este protocolo y criptosistema. Aquí
esta mi llave pública, un certificado digital y
un número random**

**Usando tu llave pública encripte una
llave simétrica aleatoria**



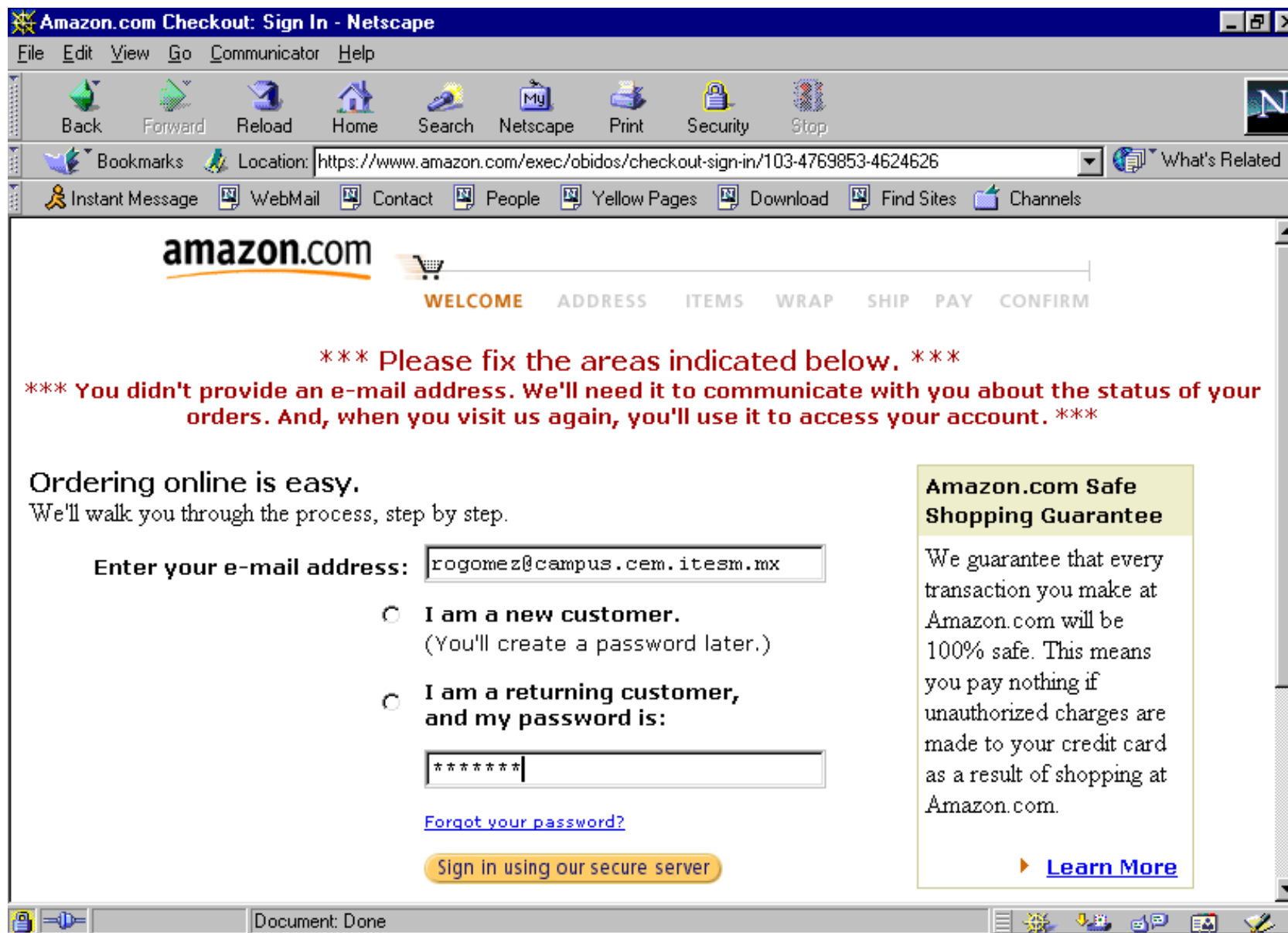
*Comunicación encriptada con la llave enviada por el cliente
y un hash para autenticación de mensajes*

Ejemplo protocolo seguro (1er. paso)



The screenshot shows a Netscape browser window displaying the Amazon.com product page for the book "Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition" by Bruce Schneier. The browser's address bar shows the URL: `amazon.com/exec/obidos/ASIN/0471117099/o/qid=971146521/sr=2-2/102-5972864-6451304`. The page features a green navigation bar with categories like "WELCOME", "DIRECTORY", "BOOKS", "SEARCH", "BROWSE SUBJECTS", "BESTSELLERS", "NEW & FUTURE RELEASES", "BARGAIN BOOKS", "AWARDS", and "SPANISH LANGUAGE". The main content area includes a search box, a "BOOK INFORMATION" sidebar with links to "buying info", "table of contents", "Amazon.com articles", "editorial reviews", and "customer reviews", and a central product display. The product display shows the book cover, pricing (List Price: \$54.95, Our Price: \$43.96, You Save: \$10.99 (20%)), availability ("Usually ships within 24 hours"), and purchase options ("Add to Shopping Cart", "Add to Wish List"). The Windows taskbar at the bottom shows the Start button, open applications (Exploring, Microsoft, Amazon), and system tray icons.

Ejemplo protocolo seguro (2do.paso)




Amazon.com Checkout: Sign In - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Location: <https://www.amazon.com/exec/obidos/checkout-sign-in/103-4769853-4624626> What's Related

Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels

amazon.com 

WELCOME ADDRESS ITEMS WRAP SHIP PAY CONFIRM

***** Please fix the areas indicated below. *****

***** You didn't provide an e-mail address. We'll need it to communicate with you about the status of your orders. And, when you visit us again, you'll use it to access your account. *****

Ordering online is easy.
We'll walk you through the process, step by step.

Enter your e-mail address:

I am a new customer.
(You'll create a password later.)

I am a returning customer,
and my password is:

[Forgot your password?](#)

[Sign in using our secure server](#)

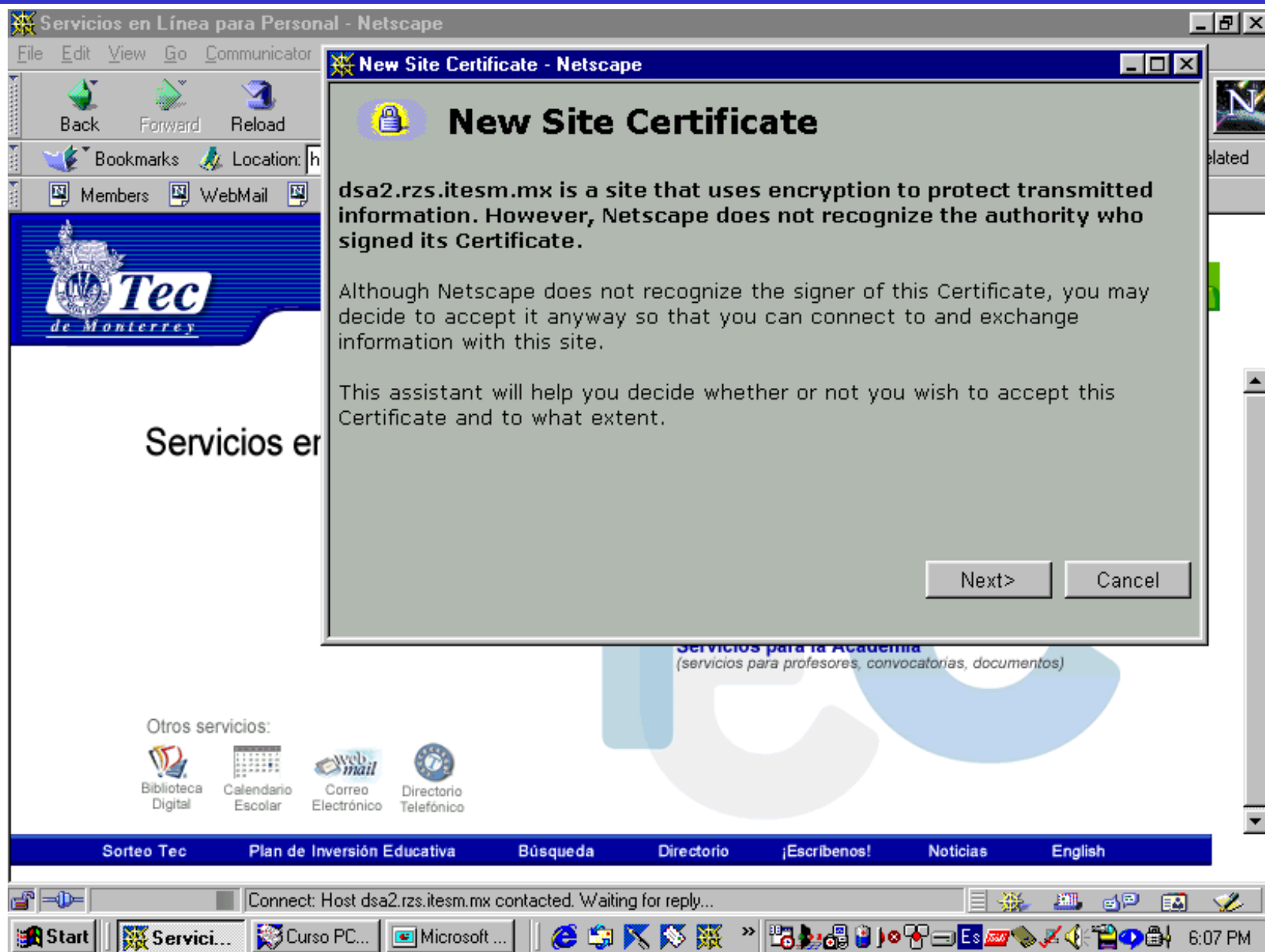
Amazon.com Safe Shopping Guarantee

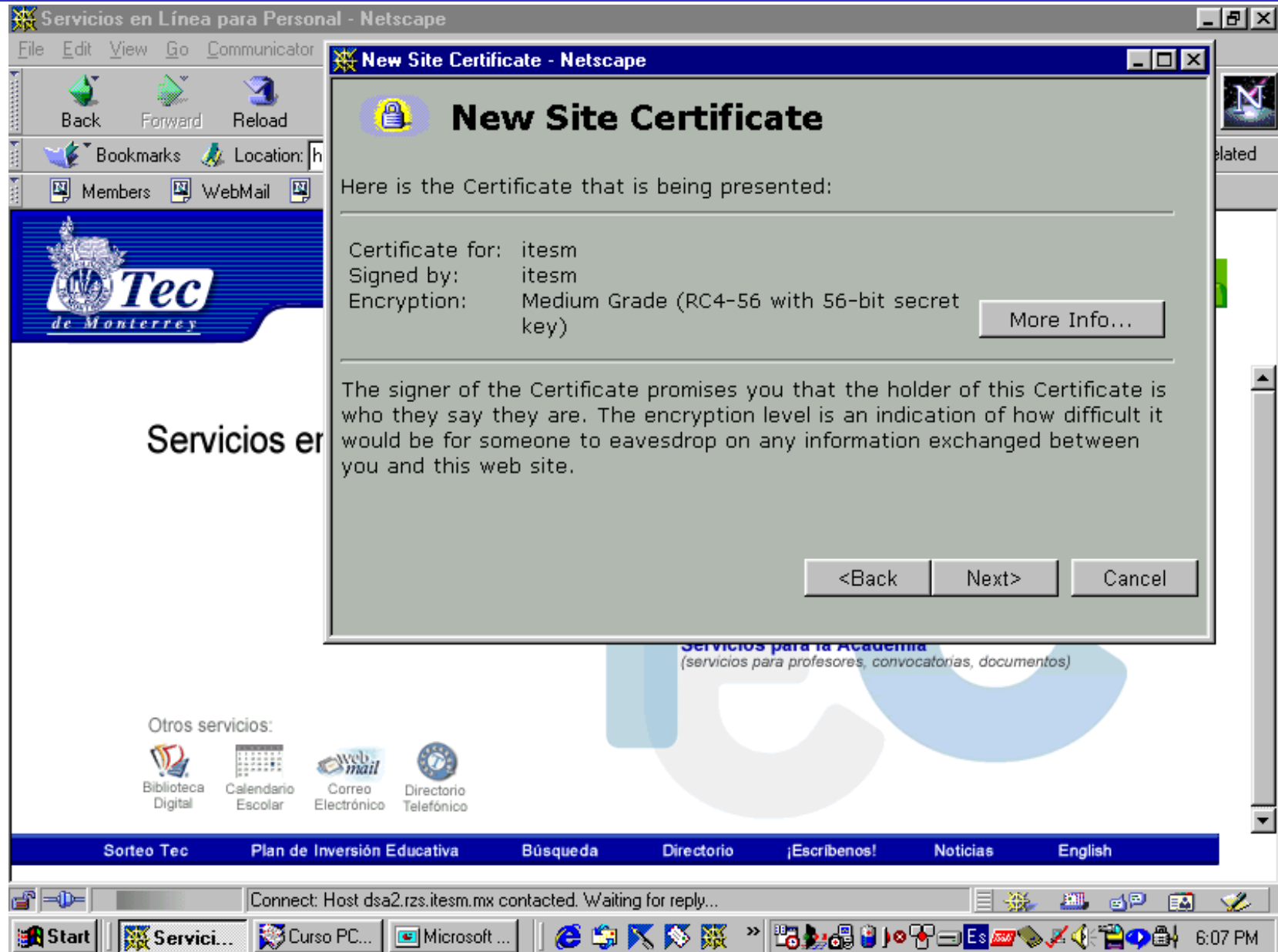
We guarantee that every transaction you make at Amazon.com will be 100% safe. This means you pay nothing if unauthorized charges are made to your credit card as a result of shopping at Amazon.com.

[Learn More](#)

Document: Done

Ejemplo certificado en una página





Servicios en Línea para Personal - Netscape

File Edit View Go Communicator

Back Forward Reload

Bookmarks Location: h

Members WebMail

Tec de Monterrey

Servicios en

New Site Certificate - Netscape

New Site Certificate

Here is the Certificate that is being presented:

Certificate for: itesm
Signed by: itesm
Encryption: Medium Grade (RC4-56 with 56-bit secret key)

More Info...

The signer of the Certificate promises you that the holder of this Certificate is who they say they are. The encryption level is an indication of how difficult it would be for someone to eavesdrop on any information exchanged between you and this web site.

<Back Next> Cancel

Servicios para la Academia
(servicios para profesores, convocatorias, documentos)

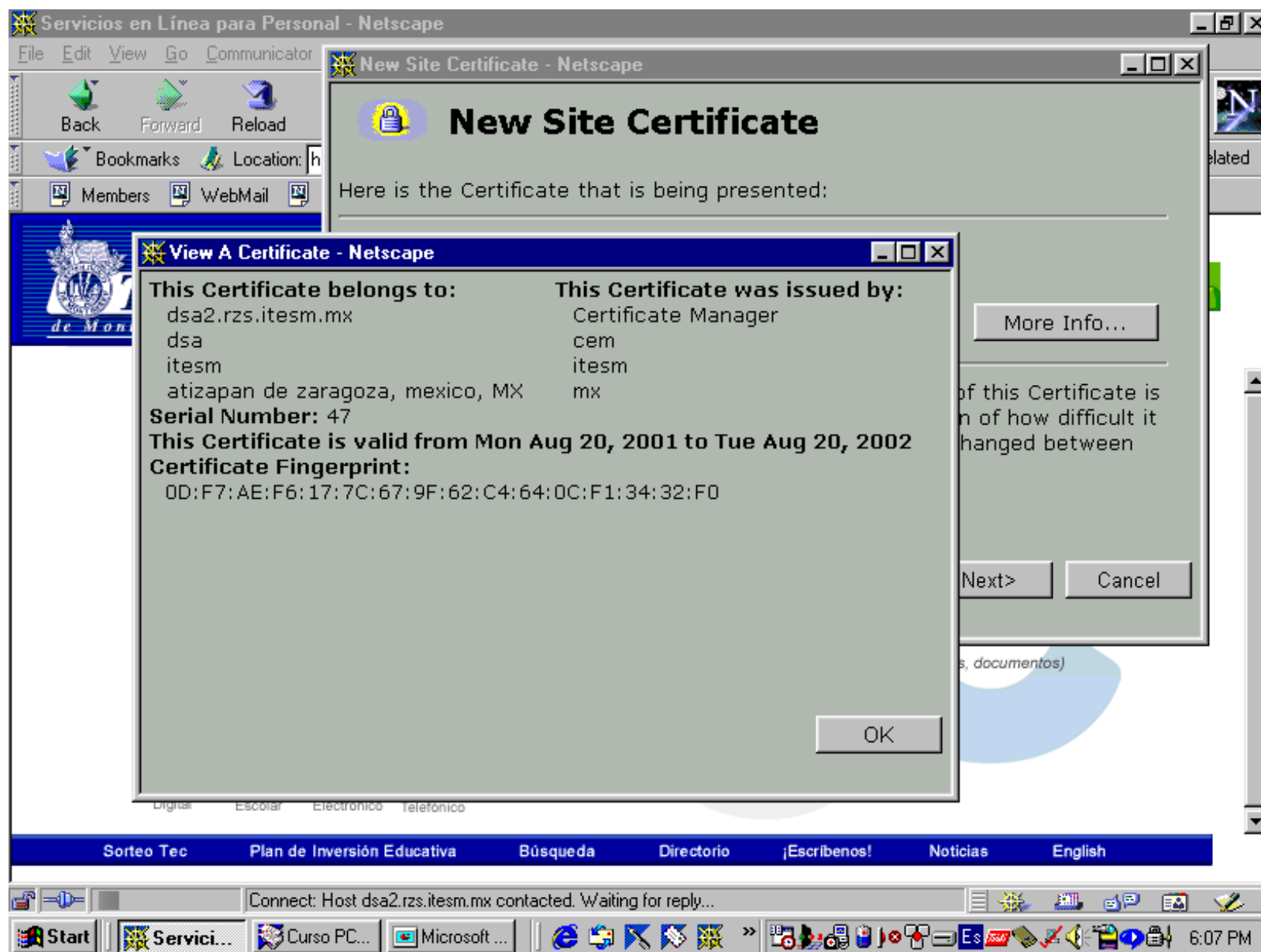
Otros servicios:

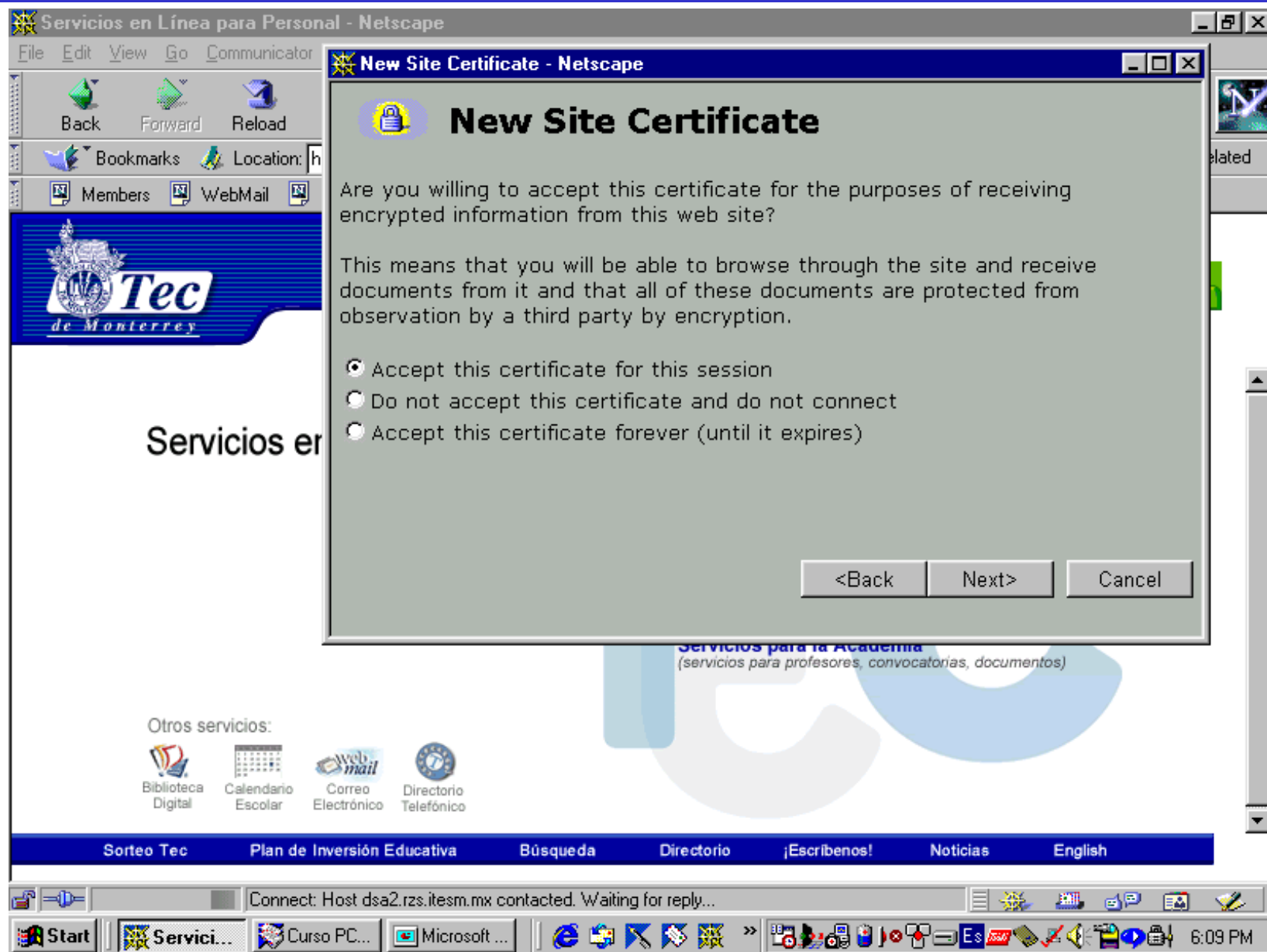
Biblioteca Digital Calendario Escolar Correo Electrónico Directorio Telefónico

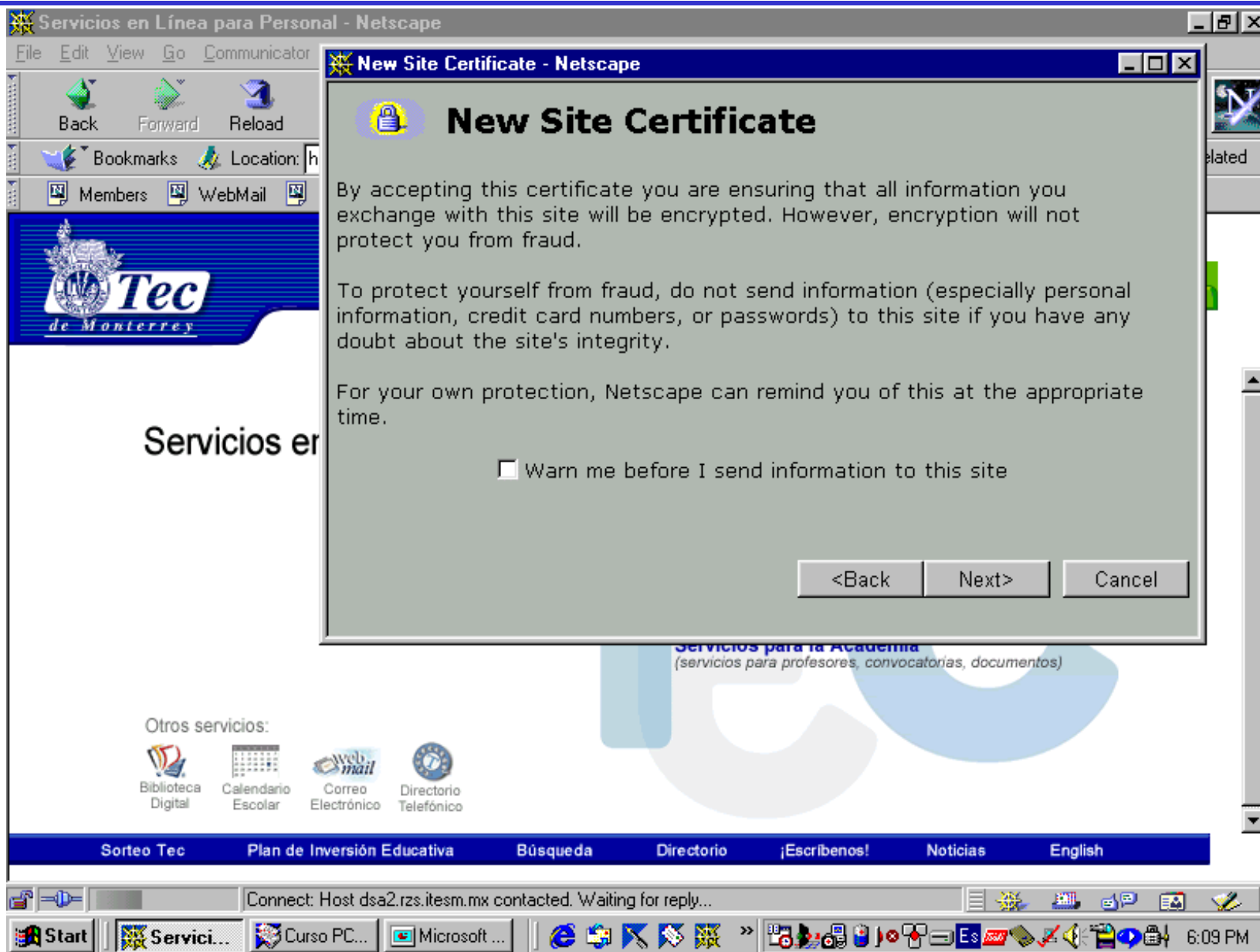
Sorteo Tec Plan de Inversión Educativa Búsqueda Directorio ¡Escribenos! Noticias English

Connect: Host dsa2.rzs.itesm.mx contacted. Waiting for reply...

Start | Servi... | Curso PC... | Microsoft ... | 6:07 PM







Servicios en Línea para Personal - Netscape

File Edit View Go Communicator

Back Forward Reload


Bookmarks Location: h

Members WebMail

Tec
de Monterrey

Servicios en

New Site Certificate - Netscape

 **New Site Certificate**

By accepting this certificate you are ensuring that all information you exchange with this site will be encrypted. However, encryption will not protect you from fraud.

To protect yourself from fraud, do not send information (especially personal information, credit card numbers, or passwords) to this site if you have any doubt about the site's integrity.

For your own protection, Netscape can remind you of this at the appropriate time.

Warn me before I send information to this site

<Back Next> Cancel

Servicios para la Academia
(servicios para profesores, convocatorias, documentos)

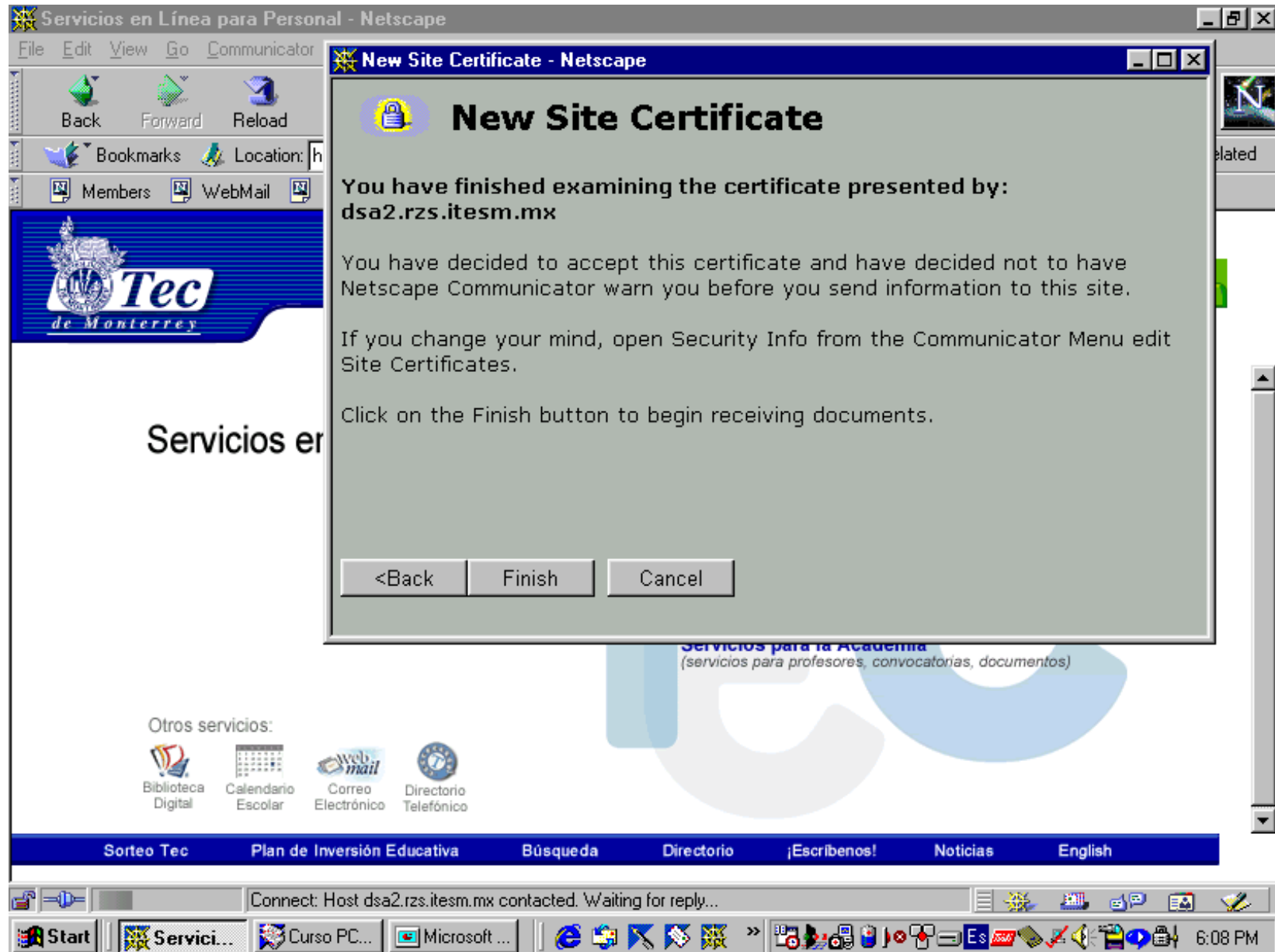
Otros servicios:

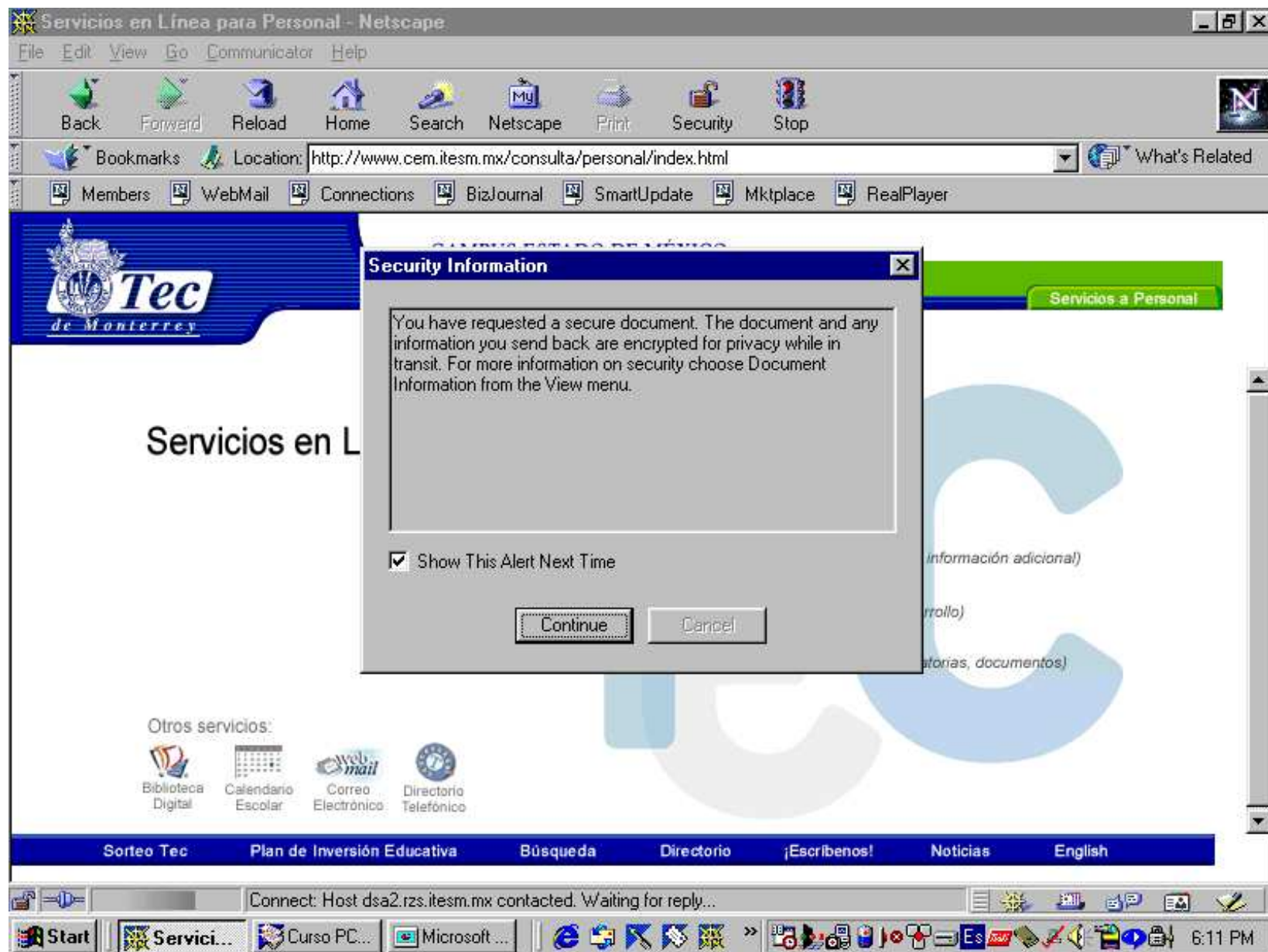
Biblioteca Digital Calendario Escolar Correo Electrónico Directorio Telefónico

Sorteo Tec Plan de Inversión Educativa Búsqueda Directorio ¡Escribenos! Noticias English

Connect: Host dsa2.rzs.itesm.mx contacted. Waiting for reply...

Start | Servi... | Curso PC... | Microsoft ... | 6:09 PM






ACM: Membership Type - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Historial Ir

Dirección http://www.acm.org/membership/L2-3/level_3_memtype.html

home feedback join go shopping search



Membership

The First Society in Computing

Membership

Please select your membership type

[Professional Membership](#)
[Professional Membership](#)


Last Updated




[HOME](#) || [ABOUT ACM](#) || [MEMBERSHIP](#) || [EDUCATION](#) || [EVENTS & CONFERENCES](#) || [AWARDS](#) || [CHAPTERS](#) || [COMPUTING & PUBLIC POLICY](#) || [PRESSROOM](#)

©2000 Association for Computing Machinery

https://www.acm.org/membership/L2-3/L3_pro_form.html

Alerta de seguridad

 La información que intercambie con este sitio no puede ser vista o cambiada por otros. No obstante, existe un problema con el certificado de seguridad del sitio.

-  El certificado de seguridad procede de una autoridad de certificación de confianza.
-  El certificado de seguridad ha caducado o todavía no es válido.
-  El nombre en el certificado de seguridad no coincide con el del sitio.

¿Desea continuar?

- Mi PC
- Mis sitios de red
- Papelera de reciclaje
- Página
- Tareas
- Cursos-Mat
- MaterialDS
- Varios
- Inbox

Priority

- Proporcionar integridad, confidencialidad, autenticidad y no repudio en el servicio de correo electrónico
- Cuatro opciones:
 - PEM
 - MOSS
 - S/MIME
 - PGP
 - GPG

S/MIME

- Secure Multipurpose Internet Mail Extensions
- Metodo para enviar correo seguro incorporado en diferente browsers y aplicaciones de correo
- Usa certificados X.509 entregados por una Autoridad de Certificación que los clientes de correo deben reconocer.
- Añade servicios de cifrado y firma en los clientes de correo (Outlook Express, Netscape Messenger, ...) en formato MIME.
- Crea una especie de sobre en el que se envuelven los datos cifrados y/o firmados.
- Usa plataformas de estándares PKCS
- Proporciona confidencialidad, autenticacion y no repudio usando criptografía asimetrica RSA, firmas electronicas y certificados X.509
- Referencia: <http://www.imc.org/smime-pgpmime.html>

Pretty Good Privacy



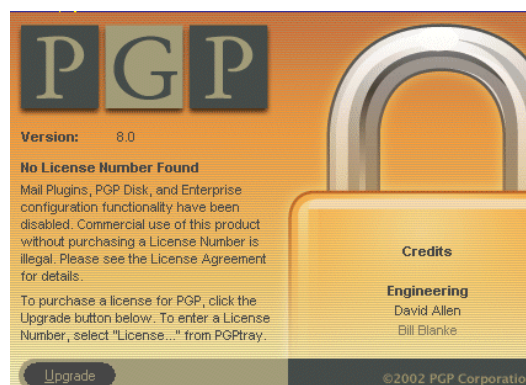
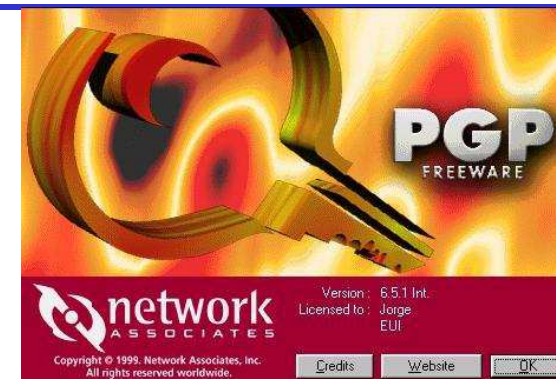
PGP

- Software acceso libre (<http://www.pgpi.org>).
- Desarrollado por Phil Zimmermann en 1994.
 - www.philzimmermann.com
- Protección de e-mail y de archivos de datos.
- Comunicación segura a través de canales inseguros.
- Administración de llaves.
- Firmas digitales.
- Compresión de datos.
- No es una herramienta esteganográfica



Versiones de PGP

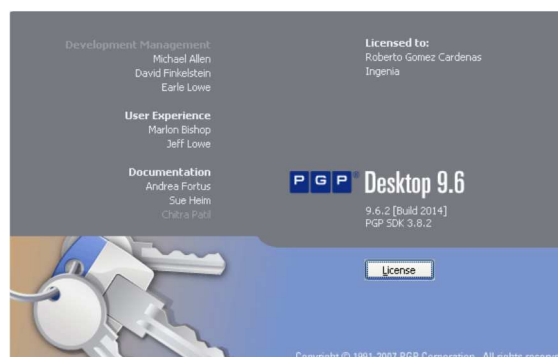
- PGP 6.5.8
 - comandos nivel consola en sistemas Unix
- PGP Freeware 7.0.3
 - Windows NT
 - Windows 2000
 - Windows Millenium
- PGP 8.0
 - Windows XP
- PGP 9.0
 - Windows Vista
 - MacOS



PGP 8.0



PGP 7.0.3



PGP 9.6

El llavero y las opciones de PGP

PGPkeys

Keys	Validity	Trust	Size	Description	Key ID	Creation	Expiration	ADK
agcampus <agregoc@campus.cem.ites...			2048/1024	DH/DSS public key	0xB721F189	27/04/2...	Never	
Alain GALLO Thoshiba <alain@ksc.th...			3072/1024	DH/DSS public key	0xAD38E5E0	28/02/1...	Never	
Allen Chamberland <allenc@ci.net>			2048/1024	DH/DSS public key	0x5AC4548A	06/12/1...	Never	
cachafas <cachafas@toto.com>			2048/1024	DH/DSS key pair	0x3284C932	09/10/2...	Never	
Erika Saucedo <esaucedo@campus...			2048/1024	Expired DH/DSS public key	0x082AD464	12/03/2...	12/03/2003	
Givalle <gdvalle1@hotmail.com>			2048/1024	DH/DSS public key	0xFF92E98B	13/05/2...	Never	
jose <jose@cinvestav.mx>			2048/1024	DH/DSS key pair	0x80B85B81	01/06/2...	Never	
Lucila Islas <lucilaislas@hotmail.com>			2048	RSA legacy public key	0xFA3993A3	25/06/2...	Never	
Lucila Islas <lucila.islas@mx.eyi.com>			2048	RSA legacy public key	0x3F16C0C9	25/06/2...	Never	
pepe le pu <lepu@francia.fr>			2048/1024	DH/DSS key pair	0x41A3E824	05/01/2...	Never	
PGP Security Employee Certification...			1024	Expired DH/DSS public key	0x1D018388	27/06/2...	30/06/2001	
PGP Security Software Release Key 2...			2048/1024	Expired DH/DSS public key	0x614239DC	07/09/2...	01/01/2001	
PGP Security Software Release Key 2...			1024	Expired DH/DSS public key	0x80C6598E	02/01/2...	01/01/2002	
Ricardo C. Lira P. <rlira@avantel.net>			2048/1024	DH/DSS public key	0x8C815E51	27/08/2...	Never	
Ricardo C. Lira P. <rlira@campus.ce...			2048/1024	DH/DSS public key	0x1130CFB6	28/08/2...	Never	
Roberto Gómez Cárdenas <rogomez...			2048/1024	DH/DSS key pair	0x94B2E825	28/05/2...	Never	
Teofilo Gonzalez <teogonzalez@hotmai...			2048/1024	Revoked DH/DSS key pair	0x8FE3AD84	18/08/2...	Never	
toto <toto@france.fr>			2048/1024	DH/DSS key pair	0x1F97B11D	10/05/2...	Never	

1 key(s) selected

PGP Desktop - All Keys

Name	Email	Verified	Size	Key ID	Trust	Cre...	Expir...	ADK	Enabled	Description
agcampus	agregoc@campus.cem.i...		2048/1024	0xB72...		4/27/2...	Never			DH/DSS public key
Alain BUI	alain.bui@univ-reims.fr		2048/1024	0xCBE...		2/13/2...	Never			DH/DSS public key
Andrés Velázquez	avelazquez@matica.com		2048/2048	0xB6F...		1/29/2...	1/1/2008			Disabled RSA p...
Ricardo C. Lira P.	rlira@avantel.net		2048/1024	0xB6C...		8/27/2...	Never			DH/DSS public key
Ricardo C. Lira P.	rlira@campus.cem.ites...		2048/1024	0x113...		8/28/2...	Never			DH/DSS public key
Roberto Gómez C...	rogomez@campus.cem...		2048/1024	0x94B...		5/28/2...	Never			DH/DSS key pair
Roberto Gomez C...	rogomez@itesm.mx		2048/2048	0x9A8...		6/23/2...	Never			RSA key pair

PGP Options

General | Files | Email | HotKeys | Servers | CA | Advanced

Options

- Always encrypt to default key
- Faster key generation
- Show PGPTray icon

Comment block (optional)

Single Sign-On

- Cache passphrase while logged on
- Cache passphrase for 00 : 02 : 00
- Do not cache passphrase
- Share passphrase cache among modules

File Wiping

Number of passes: 3 Warn before user-initiated wiping

PGP Wipe exceeds the media sanitization requirements of DoD 5220.22-M at 3 passes. Security continues to increase up to approximately 28 passes.

Automatically wipe on delete

Aceptar Cancelar Ayuda

PGP Options

General | Keys | Master Keys | Messaging | NetShare | Disk | Notifier | Advanced

PGP Tray

- Show PGP Icon in the Windows System Tray

My Passphrase

- Save my passphrase for the current Windows session only
- Save my passphrase for: 00 : 02 : 00 (hh:mm:ss)
- Do not save my passphrase

Product Language

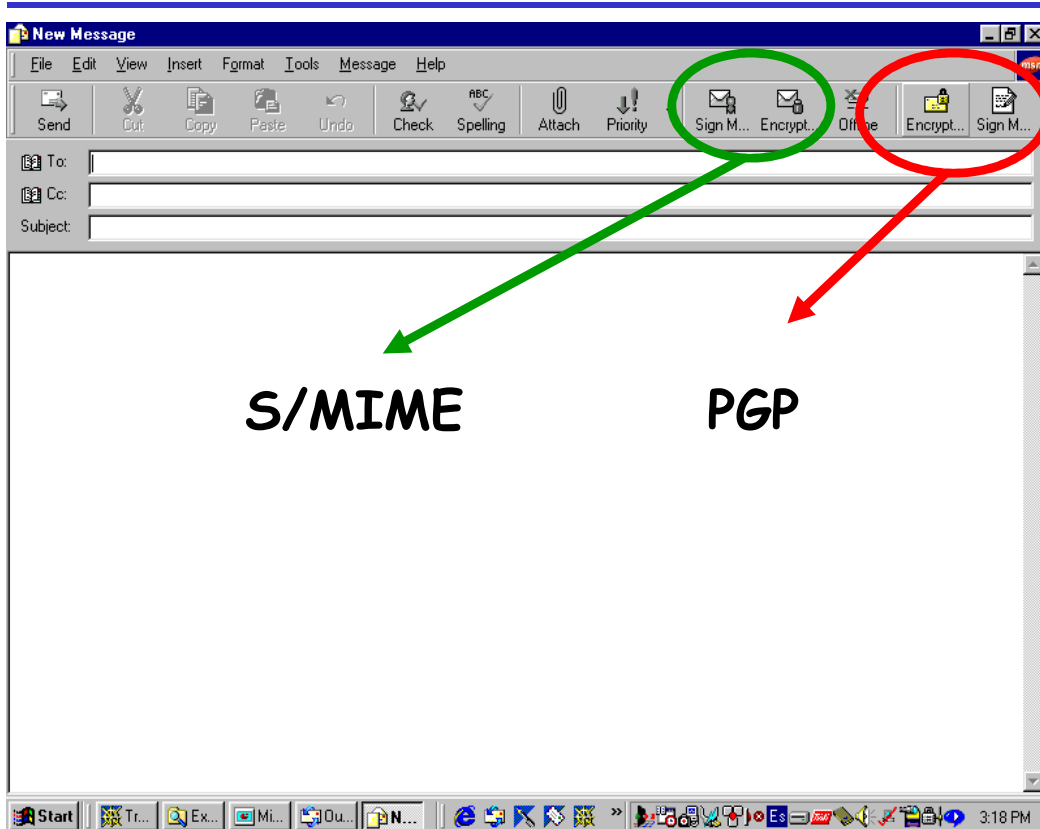
English

PGP Desktop Updates

- Check for updates every 0 days

OK Cancel Help

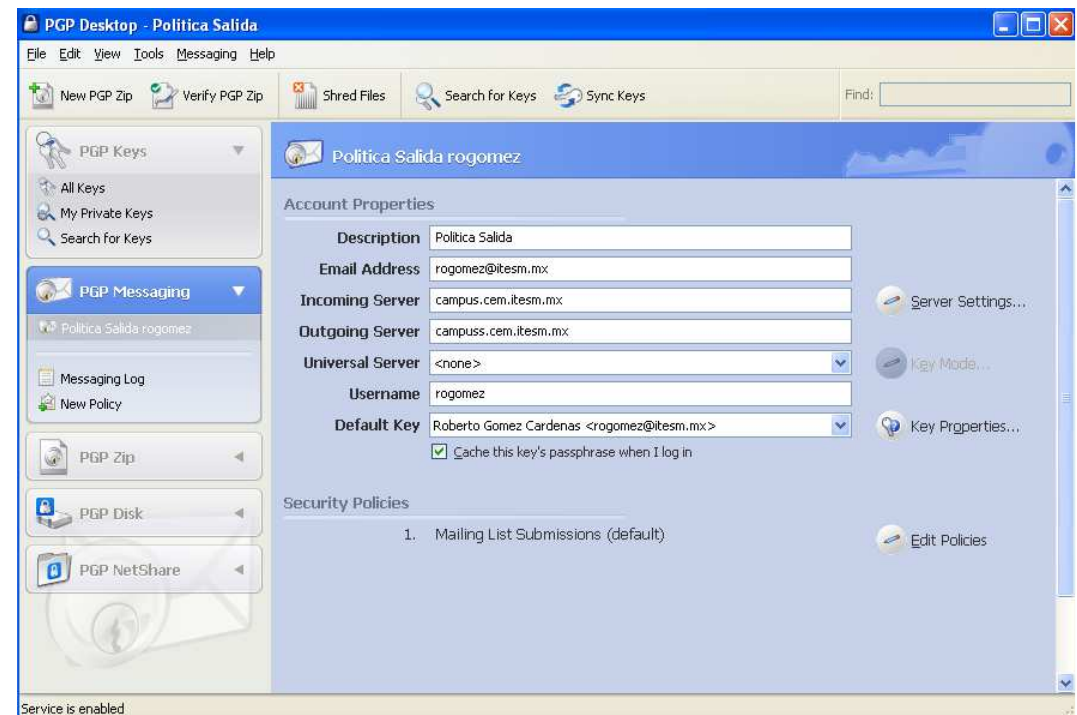
Integración con clientes de correos



S/MIME

PGP

Versiones posteriores a 9.0



Versiones anteriores a 9.0

OpenPGP

- PGP fue aceptado de tal forma por la comunidad que sirvió de base para el diseño de un estándar de encriptación para el correo electrónico: OpenPGP.
- Estándar definido por el OpenPGP Working Group (<http://www.openpgp.org>) del Internet Engineering Task Force (IETF) en el RFC 2440.
- La OpenPGP Alliance
 - grupo de compañías y otros organismos que implementan el estándar.
 - ña alianza trabaja para facilitar la interoperabilidad técnica y la sinergia de marketing entre las implementaciones de OpenPGP.

GPG

- GnuPG es un reemplazo completo y libre para PGP (<http://www.gnupg.org>).
- Debido a que no utiliza el algoritmo patentado IDEA, puede ser utilizado sin restricciones.
- GnuPG es una aplicación que cumple el RFC2440 (OpenPGP).
- La versión 1.0.0 fue liberada el 7 de septiembre de 1999.
- La versión estable actual (marzo 2004) es 1.2.4.
- GnuPG es software libre,
 - implica que puede ser utilizado, modificado y distribuido libremente bajo los términos de la GPL.

Criptoanálisis

Solo la teoría

Criptoanálisis académico

Breaking a cipher doesn't necessarily mean finding a practical way for an eavesdropper to recover the plaintext from just the ciphertext. In academic cryptography, the rules are relaxed considerably. Breaking a cipher simply means finding a weakness in the cipher that can be exploited with a complexity less than brute-force. Never mind that brute-force might require 2^{128} encryptions; an attack requiring 2^{110} encryptions would be considered a break. Breaks might also require unrealistic amounts of known or chosen plaintext -- 2^{56} blocks or unrealistic amounts of storage: 2^{80} . Simply put, a break can just be a "certificational weakness": evidence that the cipher does not perform as advertised.

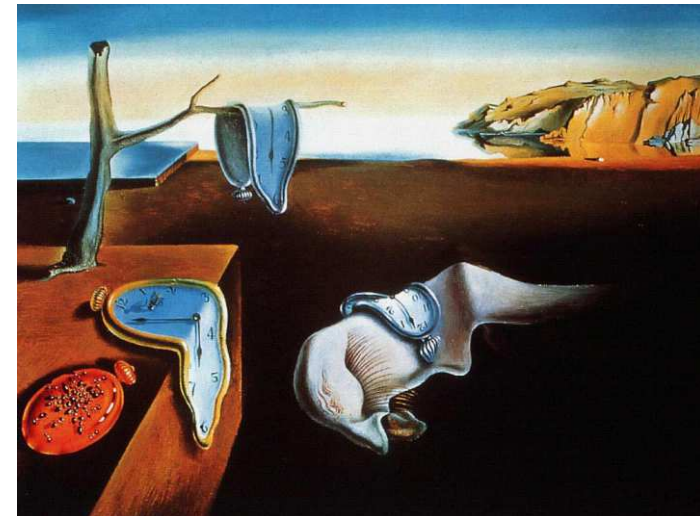
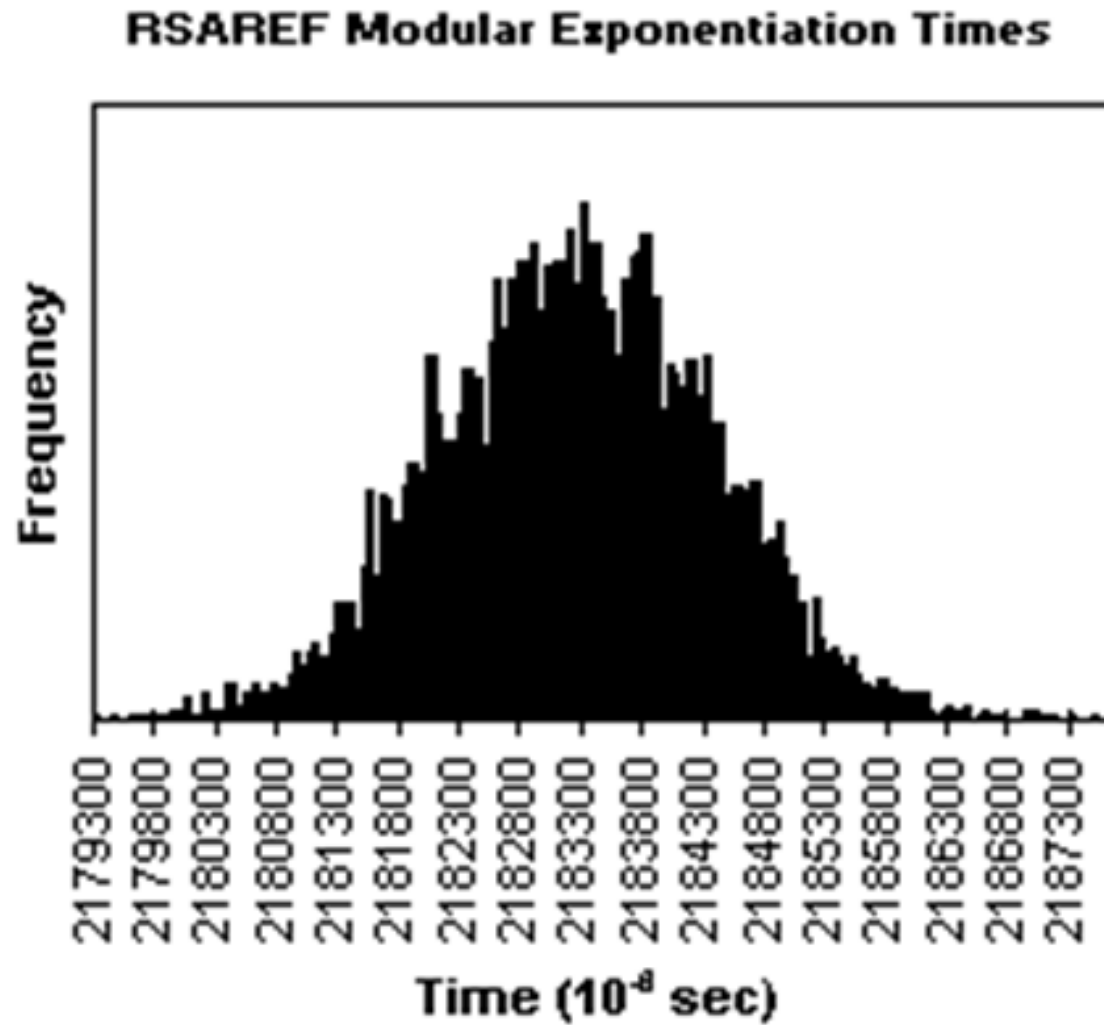
--Bruce Schneier;
from his "Self-Study Course in Block Cipher Cryptanalysis"

Tipos ataques criptográficos

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

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

Timing attack



Ataques sobre funciones de un solo sentido



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

Analogía con funciones un solo sentido



Ejemplo de colisión en MD5

- Archivos datos 1 (en hexadecimal)

d1	31	dd	02	c5	e6	ee	c4	69	3d	9a	06	98	af	f9	5c
2f	ca	b5	<u>87</u>	12	46	7e	ab	40	04	58	3e	b8	fb	7f	89
55	ad	34	06	09	f4	b3	02	83	e4	88	83	25	<u>71</u>	41	5a
08	51	25	e8	f7	cd	c9	9f	d9	1d	bd	<u>f2</u>	80	37	3c	5b
d8	82	3e	31	56	34	8f	5b	ae	6d	ac	d4	36	c9	19	c6
dd	53	e2	<u>b4</u>	87	da	03	fd	02	39	63	06	d2	48	cd	a0
e9	9f	33	42	0f	57	7e	e8	ce	54	b6	70	80	<u>a8</u>	0d	1e
c6	98	21	bc	b6	a8	83	93	96	f9	65	<u>2b</u>	6f	f7	2a	70

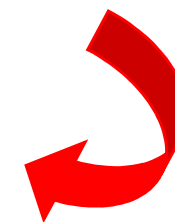
Hay hasta 24 bits diferentes

Los primeros 4 de 8 bits son distintos.

- Archivo datos 2 (en hexadecimal)

d1	31	dd	02	c5	e6	ee	c4	69	3d	9a	06	98	af	f9	5c
2f	ca	b5	<u>07</u>	12	46	7e	ab	40	04	58	3e	b8	fb	7f	89
55	ad	34	06	09	f4	b3	02	83	e4	88	83	25	<u>f1</u>	41	5a
08	51	25	e8	f7	cd	c9	9f	d9	1d	bd	<u>72</u>	80	37	3c	5b
d8	82	3e	31	56	34	8f	5b	ae	6d	ac	d4	36	c9	19	c6
dd	53	e2	<u>34</u>	87	da	03	fd	02	39	63	06	d2	48	cd	a0
e9	9f	33	42	0f	57	7e	e8	ce	54	b6	70	80	<u>28</u>	0d	1e
c6	98	21	bc	b6	a8	83	93	96	f9	65	<u>ab</u>	6f	f7	2a	70

Y la función hash MD5 es:



MD5 = 79 05 40 25 25 5f b1 a2 6e 4b c4 22 ae f5 4e b4

“Integridad” del código ejecutable

```
C:\TEMP> md5sum hello.exe
cdc47d670159eef60916ca03a9d4a007
C:\TEMP> .\hello.exe
Hello, world!

(press enter to quit)
C:\TEMP>
```

```
C:\TEMP> md5sum erase.exe
cdc47d670159eef60916ca03a9d4a007
C:\TEMP> .\erase.exe
This program is evil!!!
Erasing hard drive...1Gb...2Gb... just kidding!
Nothing was erased.

(press enter to quit)
C:\TEMP>
```

```
C:\OpenSSL\bin>openssl md5 hello.exe
MD5(hello.exe)= cdc47d670159eef60916ca03a9d4a007
C:\OpenSSL\bin>openssl md5 erase.exe
MD5(erase.exe)= cdc47d670159eef60916ca03a9d4a007
```

**Cálculo de hash
con OpenSSL**

Artículo de Peter Selinger

<http://www.mathstat.dal.ca/~selinger/md5collision/>

Alicia y su jefe

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

MD5=a25f7f0b 29ee0b39 68c86073 8533a4b9

May, 22, 2005

To Whom it May Concern:

Alice Falbala fulfilled all the requirements of the Roman Empire intern position. She was excellent at translating roman into her gaul native language, learned very rapidly, and worked with considerable independence and confidence.

Her basic work habits such as punctuality, interpersonal deoprtment, communication skills, and completing assigned and self-determined goals were all excellent.

I recommend Alice for challenging positions in which creativity, reliability, and language skills are required.

I highly recommend hiring her. If you'd like to discuss her attributes in more detail, please don't hesitate to contact me.

Sincerely,

Julius Caesar

May, 22, 2005

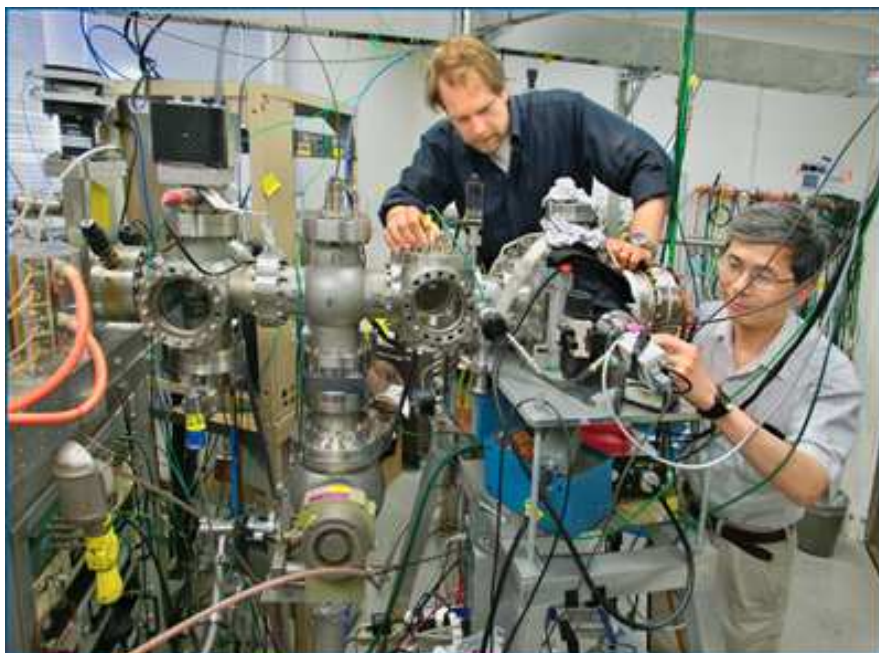
Order:

Alice Falbala is given full access to all confidential and secret information about GAUL.

Sincerely,

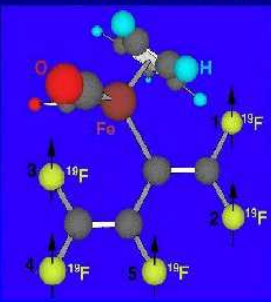
Julius Caesar

Quantum Computing

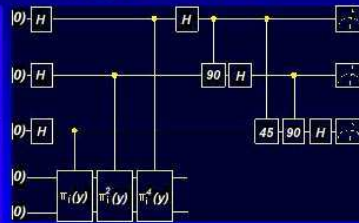


5 qubit 215 Hz Q. Processor

(Vandersypen, Steffen, Breyta Yannoni, Cleve, and Chuang, 2000)



• The Molecule



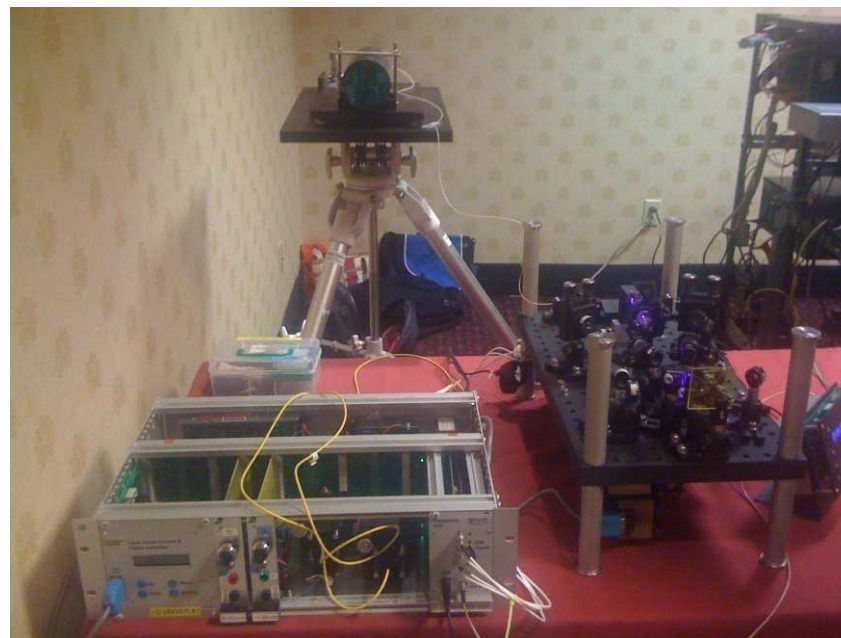
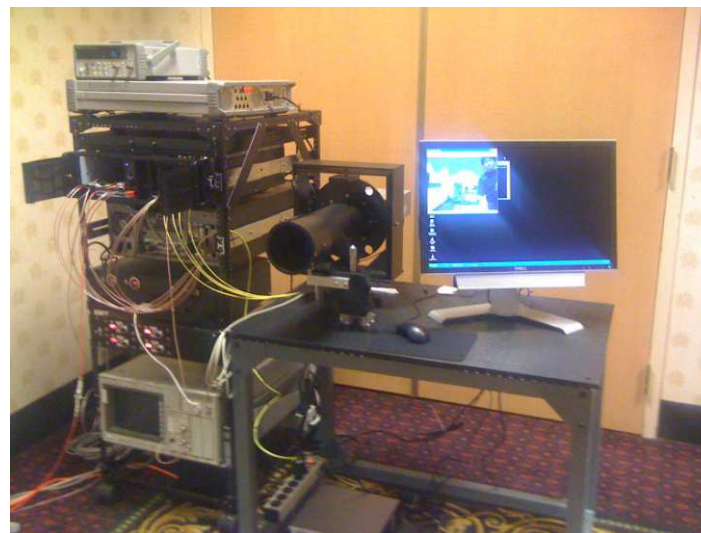
• Quantum Circuit

$T_2 > 0.3 \text{ sec} ; \sim 200 \text{ gates}$

Source: IBM, Hot Chips Conference, 2000



Quantum Cryptography (1)



Quantum Cryptography (2)



Otra opción a la criptografía...

ESTEGANOGRAFIA

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, dentro de información considerada como válida.
- La información puede esconderse de cualquier forma
 - diferentes métodos se han ido desarrollando



Algunos ejemplos históricos

- Herodoto:
 - 440 ac: Aristagoras de Milet usa esclavos calvos para la revuelta contra los persas
 - Demeratus envía mensaje (tablones cubiertos de cera) a Esparta para avisar de que Xerxes (rey de Persa) tenía intenciones de invadir Grecia.
- Tintas invisibles
 - naturales: jugo limón, leche, orina, sal de amoníaco
 - química: alumbre y vinagre, traspasar cáscara huevo duro
- Chinos: texto escrito sobre seda china



Ejemplo de Null Cipher

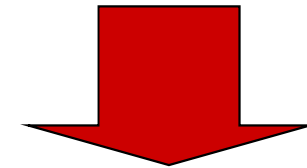
Tomando la primera letra de cada palabra

News Eight Weather: Tonight increasing snow.
Unexpected precipitation smothers eastern towns. Be
extremely cautious and use snowtires especially heading
east. The highways are knowingly slippery. Highway
evacuation is suspected. Police report emergency
situations in downtown ending near Tuesday.

Hidden Information !

Newt is upset because he thinks he is President.

Usando imágenes digitales



```
FlotC.txt - Bloc de notas
Archivo Edición Buscar Ayuda
/* Copyright (C) 1996, MPEG Software Simulation Group. All Rights Reserved. */
/*
 * Disclaimer of Warranty
 *
 * These software programs are available to the user without any license fee or
 * royalty on an "as is" basis. The MPEG Software Simulation Group disclaims
 * any and all warranties, whether express, implied, or statutory, including any
 * implied warranties or merchantability or of fitness for a particular
 * purpose. In no event shall the copyright-holder be liable for any
 * incidental, punitive, or consequential damages of any kind whatsoever
 * arising from the use of these programs.
 *
 * This disclaimer of warranty extends to the user of these programs and user's
 * customers, employees, agents, transferees, successors, and assigns.
 *
 * The MPEG Software Simulation Group does not represent or warrant that the
 * programs furnished hereunder are free of infringement of any third-party
 * patents.
 *
 * Commercial implementations of MPEG-1 and MPEG-2 video, including shareware,
 * are subject to royalty fees to patent holders. Many of these patents are
 * general enough such that they are unavoidable regardless of implementation
 * design.
 */
```



Técnicas steganográficas

- Adición
 - se oculta el mensaje secreto en las secciones del medio portador que pueden ser ignoradas por la aplicación que lo procesa
- Generación
 - se crea el esteganograma a partir de la información secreta, sin contar con un medio portador previamente
- Sustitución
 - se modifican ciertos datos del medio portador por los datos del mensaje secreto

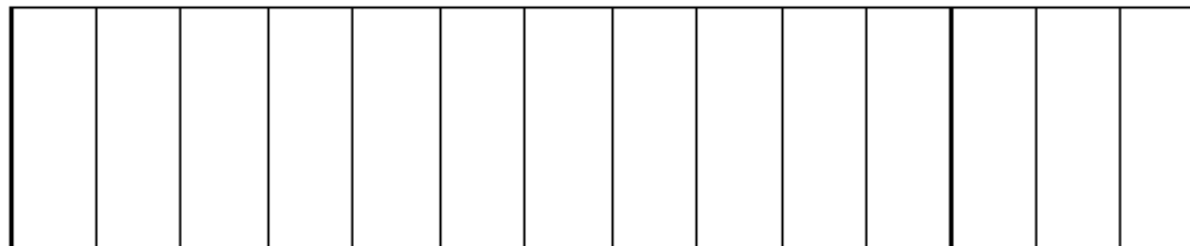
<http://www.wayner.org/books/discrypt2/bitlevel.php>

Ejemplo adición

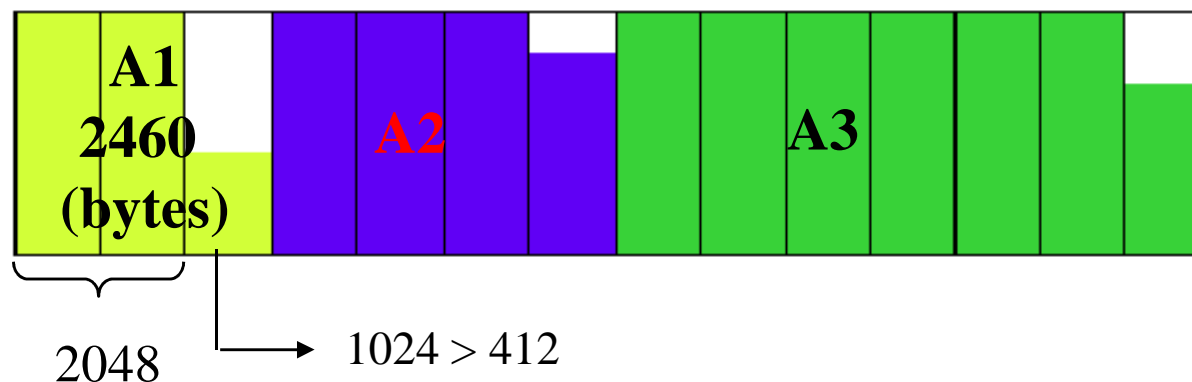
slack space

El slack space

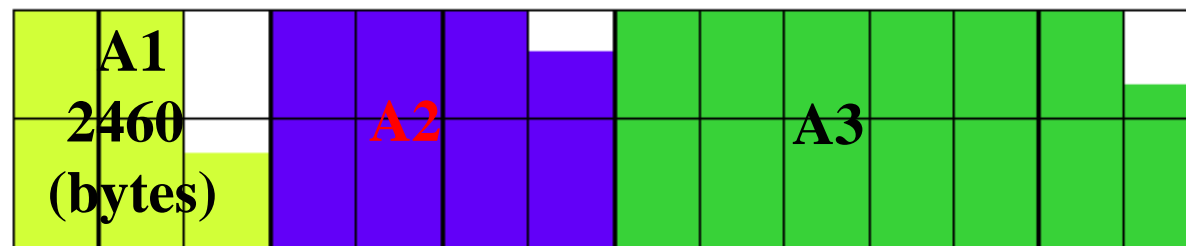
14 clusters libres
c/cluster = 1024 bytes



Tres archivos:
A1, A2 y A3



Cluster = 512bytes



Ejemplos generación

funciones “mimic”

Ejemplos generación

- Mensaje a ocultar es la entrada de un generador de texto
- El generador produce un mensaje que incluye las palabras de la información a ocultar.
- Dos ejemplos
 - Narrador de baseball
 - <http://www.wayner.org/texts/mimic/>
 - Spam Mimic
 - <http://www.spammimic.com/>

Table Loaded. Ready to go.

esto es una prueba

Push for Mimicry

It's time for another game between the Whappers and the Blogs in scenic downtown Blovonía . I've just got to say that the Blog fans have come to support their team and rant and rave . It's a fine day for a game . Top of the inning. No outs yet . Now, Sal Sauvignon swings the bat to get ready and enters the batter's box . He's trying the curveball . He pops it up to Robert Liddlekopf . Wow. Only one out. The crowd is nervous. Mark Cloud comes to the plate . The pitchers is winding up to throw. No wood on that one . Here

Remove Mimicry

ESTO ES UNA PRUEBA

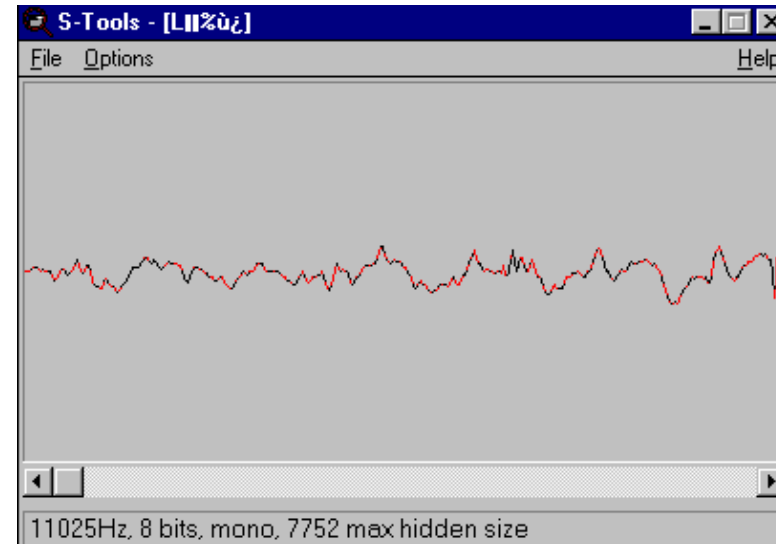
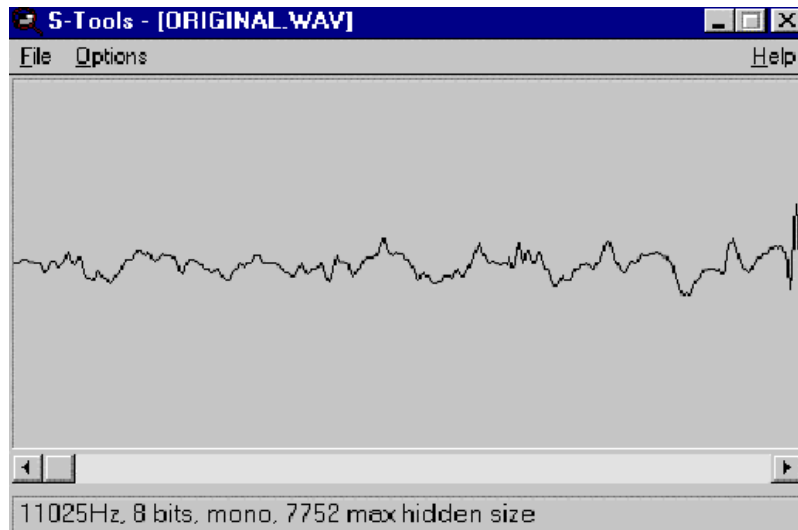
Ejemplos substitución

archivos digitales y Stools

Ejemplos Susbtitución

- Principales métodos
 - LSB: Least-Significant Bit
 - La transformación matemática de la información
 - Transformación discreta del coseno (DCT)
 - Transformación discreta de Fourier
 - Transformación de Wavelet
- Posibles medios medios portadores (archivos digitales)
 - archivos de música
 - archivos de imagenes

Esteganografía en música



Información: 132 134 137 141 121 101 74 38

**Binario: 10000100 10000110 10001001 10001101 01111001 01100101 01001010
00100110**

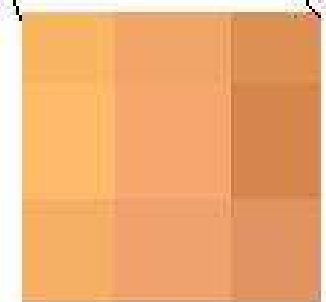
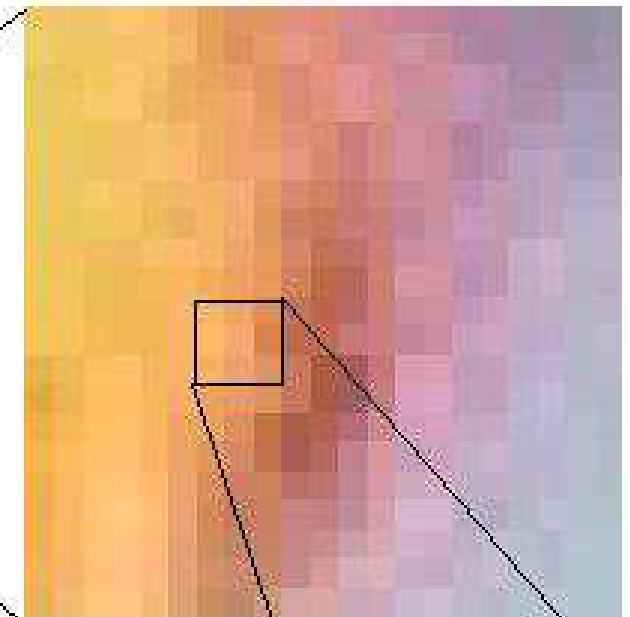
Información a esconder: 11010101 (213)

Resultado: 133 135 136 141 120 101 74 39

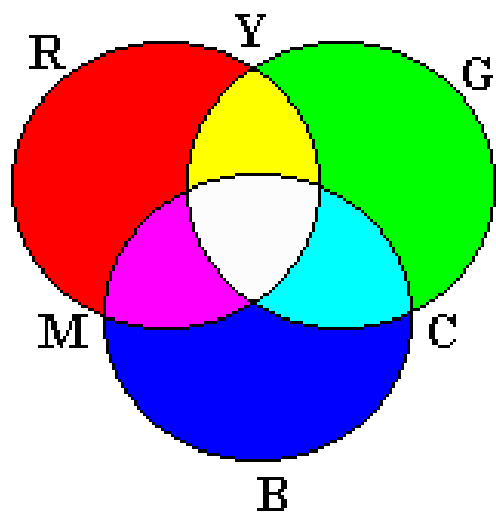
**Binario: 10000101 10000111 10001000 10001101 01111000 01100101
01001010 00100111**

Imágenes

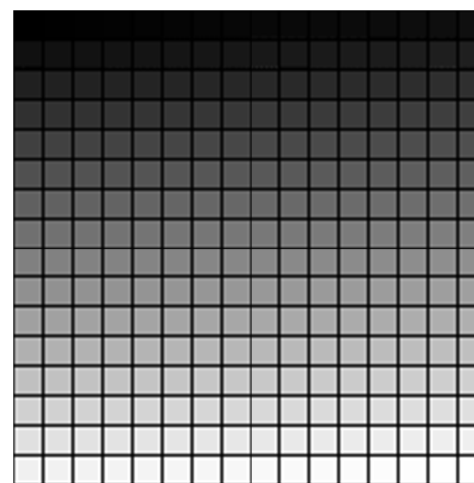
- Una imagen es una matriz de $M \times N$ Píxeles.
- Un Pixel es la unidad mínima de dibujo



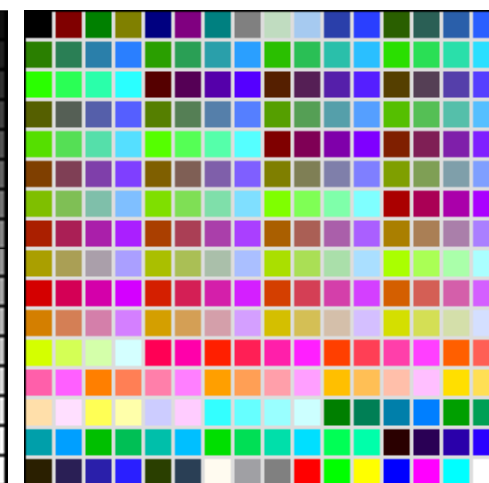
Los colores en las imágenes digitales



RGB



Paleta escala
de grises



Paleta escala
de colores



Modelo de Color RGB

- Emplea síntesis aditiva, es decir, suma colores para obtener nuevos colores.
 - el color de inicio es el negro y la suma de todos los colores da blanco.
- Los colores se representan con 24 bits
 - 8 para cada componente RGB.
- Cada componente 8 bits: 256 posibles niveles color
- Tres canales de color: Rojo (R), Verde (G), Azul (B)

1 0 0 0 1 1 0 0

Azul

1 0 0 0 1 1 0 0

Verde

1 0 0 0 1 1 0 0

Rojo

Maecanismos Susbtitución

- Principales métodos
 - LSB: Least-Significant Bit
 - La transformación matemática de la información
 - Transformación discreta del coseno (DCT)
 - Transformación discreta de Fourier
 - Transformación de Wavelet
- Posibles medios medios portadores (archivos digitales)
 - archivos de música
 - archivos de imagenes

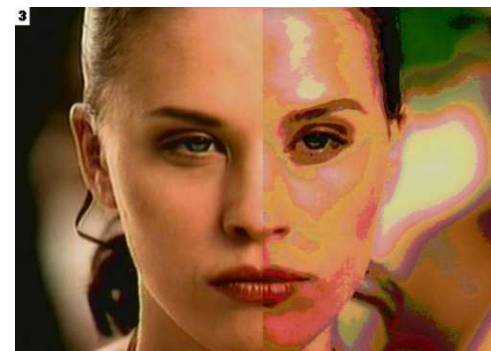
¿Qué pixels se pueden usar?



Bit más significativo



Segundo bit más significativo



Tercer bit más significativo



Cuarto bit más significativo



Quinto bit más significativo

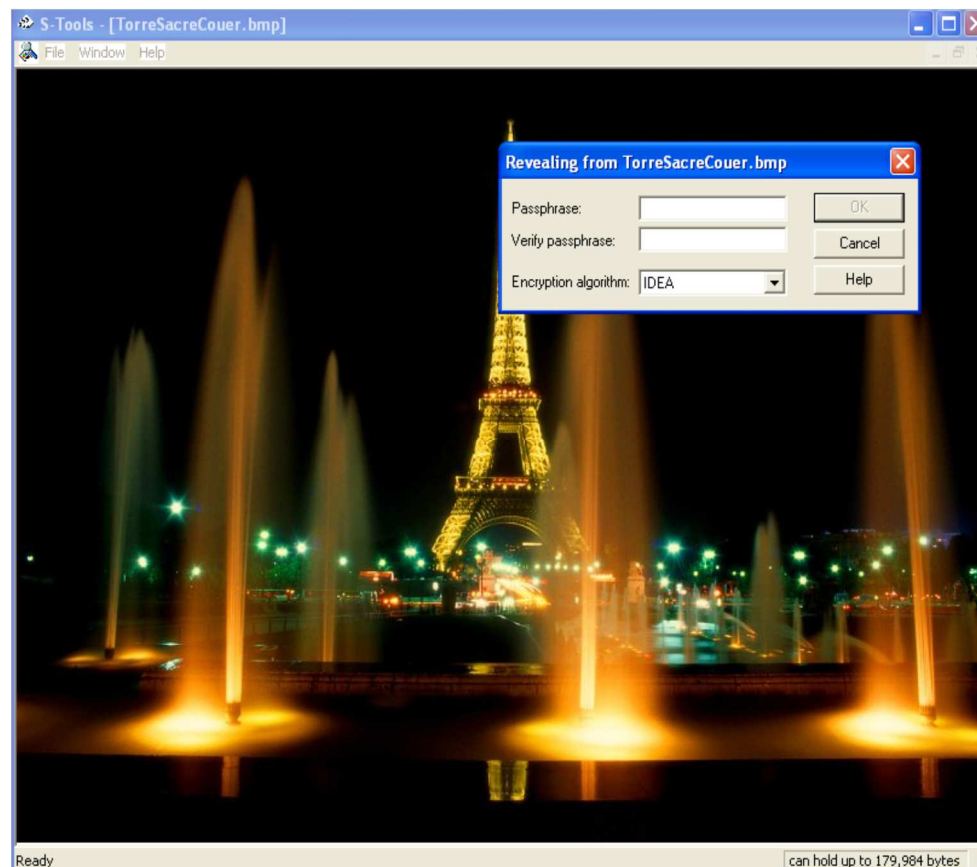


Sexto bit más significativo

<http://www.wayner.org/books/discrypt2/bitlevel.php>

¿Qué información podemos ocultar en una imagen?

- Dentro de una imagen podemos utilizar 1 ó 2 bits por cada canal de cada pixel.
 - dichos bits pueden formar bytes
- Con bytes podemos almacenar cualquier tipo de información: texto, archivos de sonido, programas e incluso otras imágenes.
- Ejemplo herramienta:
 - stools



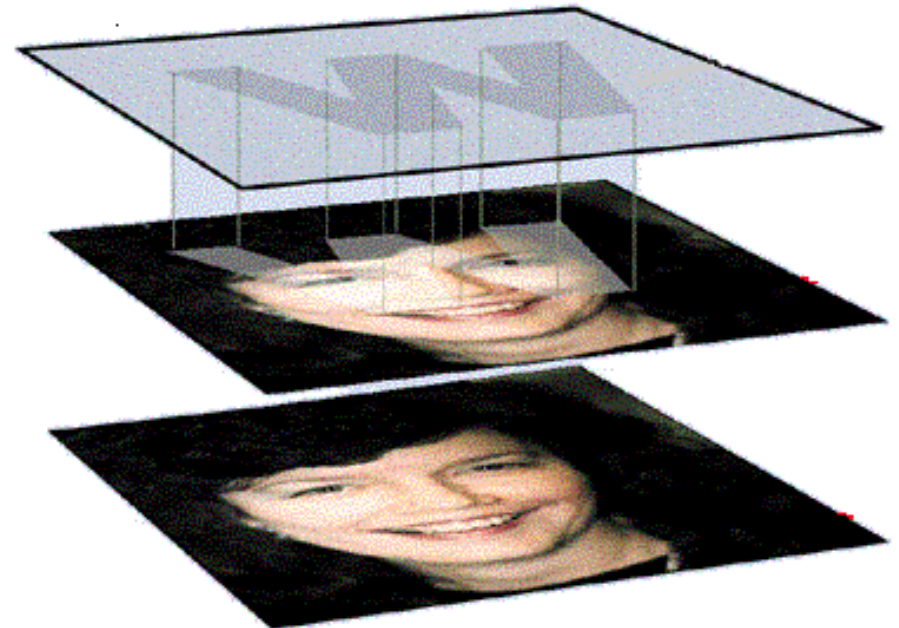
Otras herramientas esteganográficas

- Covert.tcp
- dc-Steganograph
- EzStego
- FFEncode
- Gif-it-Up V1.0
- Gifshuffle
- Gzsteg
- Hide4 PGP
- Hide and Seek
- jpeg-jsteg
- MandelSteg
 - and GIF Extract
- MP3 Stego
- MP3Stegz
- OpenPuff
- Outguess
- Paranoid
- PGE
 - Pretty Good Envelope
- PGPn123
- Publimark
- Stools
- Scytale
- Snow
- Stealth
- Steganos
- Steghide
- Stego
 - John Walker
- Stego
 - Romana Machado
- Stegonosaurus
- StegonoWav
- Stegodos
- Stegtunnel
- Texto
- wbStego
 - Werner Bailer
- Wnstorm
 - WhiteNoise Storm

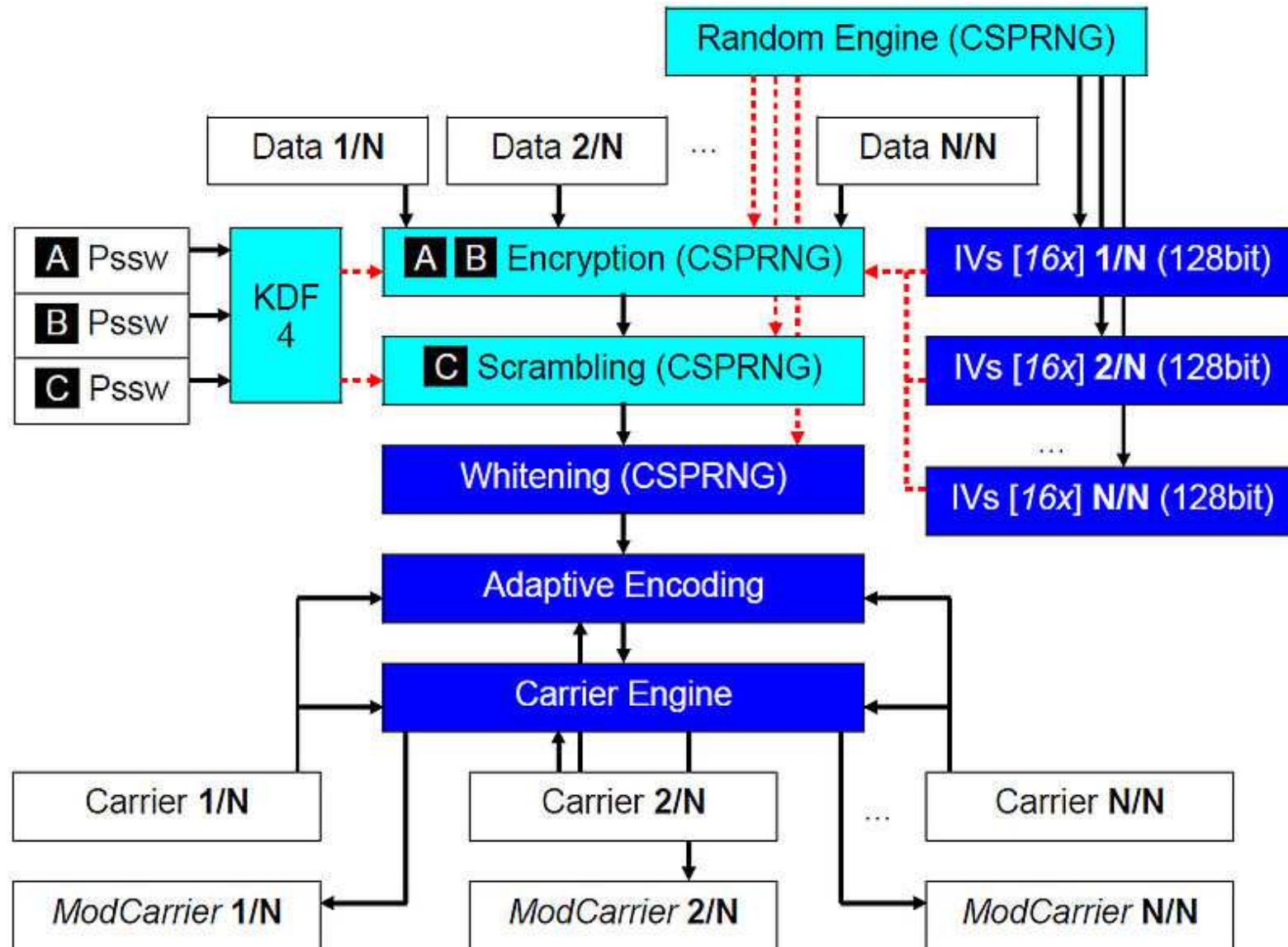
Fuentes: <http://www.jjtc.com/Security/stegtools.htm>
<http://www.jjtc.com/Steganography/toolmatrix.htm>
<http://stegano.net/tools>

Esteganografía vs Watermarking

- Misma características esteganografía
- Robustez en contra de posibles ataques
 - esteganografía esta relacionada con la detección de un mensaje oculto, mientras que watermarking involucra el borrado/duplicación de un pirata
- Watermarking no siempre necesita estar oculto
- Tipos
 - invisible
 - visible



Carrier chain (OpenPuff)



Marcas de agua visible e invisible



Imagen sin marca

+



Marca de agua

=



Imagen con marca



Imagen sin marca

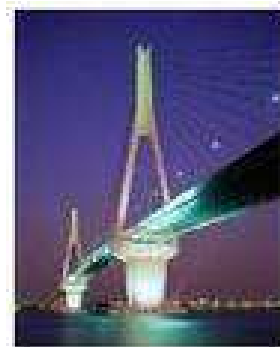


Imagen con marca



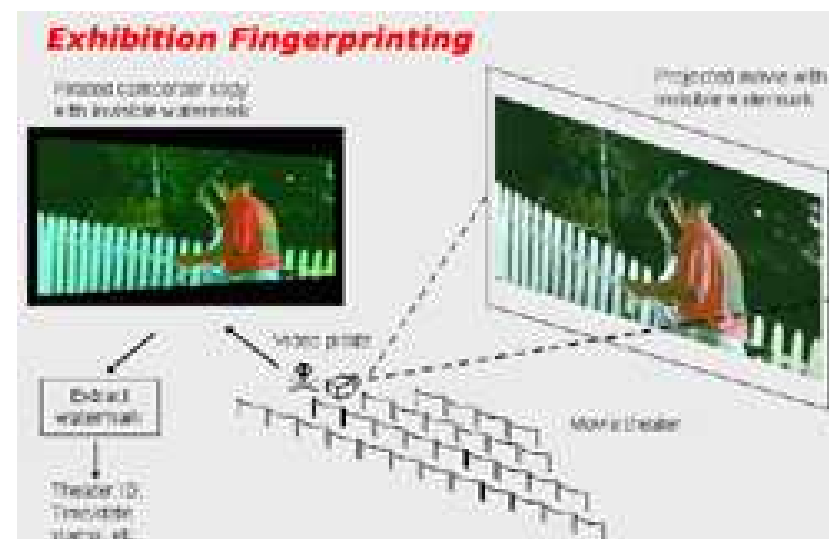
Marca de agua

Robustas vs frágiles

- Marcas de agua robustas
 - soportan un cierto grado de modificación, dependiendo de las necesidades de la aplicación.
 - tienen que considerar los ataques a los que pueden ser sometidas las imágenes marcadas
- Marcas de agua frágiles
 - son diseñadas para destruirse o modificarse ante cualquier distorsión sobre la imagen que la contiene, verificando así la integridad de la imagen.
 - algunas marcas de agua permiten localizar las áreas en el espacio que han sido afectadas, e incluso caracterizar cierto tipo de distorsión

Esteganografía vs Watermarking

- La información ocultada por un sistema de marca de agua, siempre se asocia al objeto digital a ser protegido.
- Comunicaciones esteganograficas son del tipo punto a punto, mientras que watermarking son del tipo punto-multipunto.
- Software
 - AiS Watermark Pictures Protector
 - Easy Watermark Creator
 - Alphatec Watermarking Suite 1.0
- Software de prueba
 - StirMark Benchmark 4 I
 - AudioStirMark
- Referencias:
 - <http://www.elis.ugent.be/~banckaer/watermarking.html>



Stegoanálisis

- Arte de descubrir y convertir los mensajes en no útiles.
- Ataques y análisis de información oculta pueden tomar diferentes formas:
 - detección: solo detectar contenido esteganográfico
 - extracción: quitar la información
 - confusión: alteración, introducción, dejar inservible la información almacenada
 - deshabilitación de la información oculta
- Muchos casos requieren contar con porciones del objeto encubierto (stego-object) y posibles porciones del mensaje.
 - resultado: el stego-object

Métodos de detección de Steganografía

- Detección Visual
 - JPEG, BMP, GIF, etc.
- Detección Auditiva
 - WAV, MPEG, etc.
- Detección estadística o análisis de histogramas
 - cambios en los patrones de los píxeles o LSB
 - histograma: resumen gráfico de la variación de un conjunto de datos
- Detección estructural: verificar propiedades/contenidos de archivos
 - diferencia en el tamaño del archivo
 - diferencias en tiempo y fecha
 - modificaciones del contenido
 - checksum

Detección estructural

- Comparar las propiedades de los archivos
- Propiedades:
 - 04/04/2003 05:25p 240,759 helmetprototype.jpg
 - 04/04/2003 05:26p 235,750 helmetprototype.jpg
- Checksum
 - C:\GNUTools>cksum a:\before\helmetprototype.jpg
3241690497 240759 a:\before\helmetprototype.jpg
 - C:\GNUTools>cksum a:\after\helmetprototype.jpg
3749290633 235750 a:\after\helmetprototype.jpg

Detección visual



Imagen original



LSB resaltados
imagen pura



LSB resaltados
con 1KB de datos
aleatorios



LSB resaltados
con 5KB de datos
aleatorios



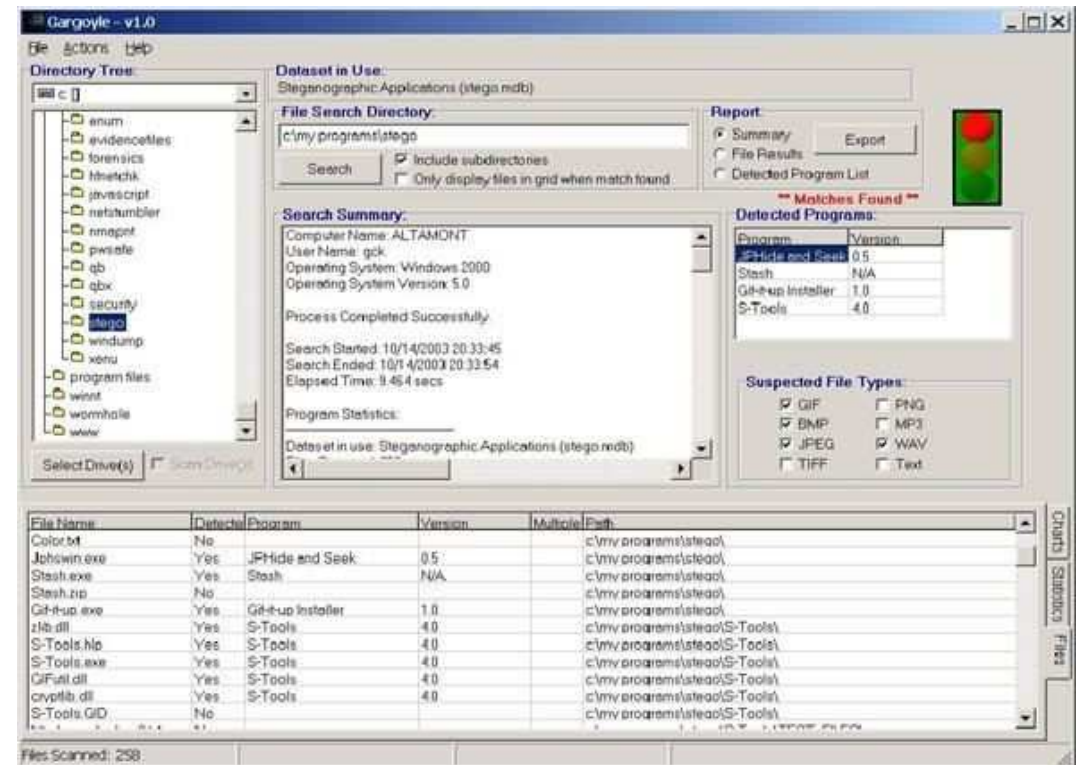
LSB resaltados
con poema "if"
(1.5 Kb)

Fuente; <http://www.guillermi2.net>

- Necesario saber si en la computadora existe software esteganográfico y cual es este.
- Una vez detectado se puede proceder a un análisis más dirigido de los archivos sospechosos.
- A tomar en cuenta
 - Software esteganográfico en un medio de almacenamiento portable.

Gargoyle (StegoDetect)

- Detección de software esteganográfico en base a un conjunto de datos (hash set) propietario de los archivos de software esteganográfico.
- También puede ser usado para detectar la presencia de otro tipo de software
 - Criptografía, SMS, cracks

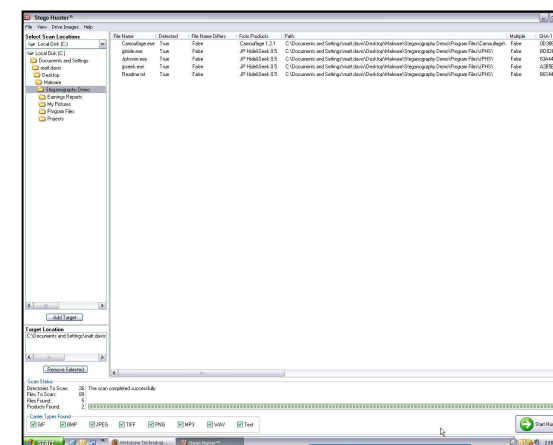
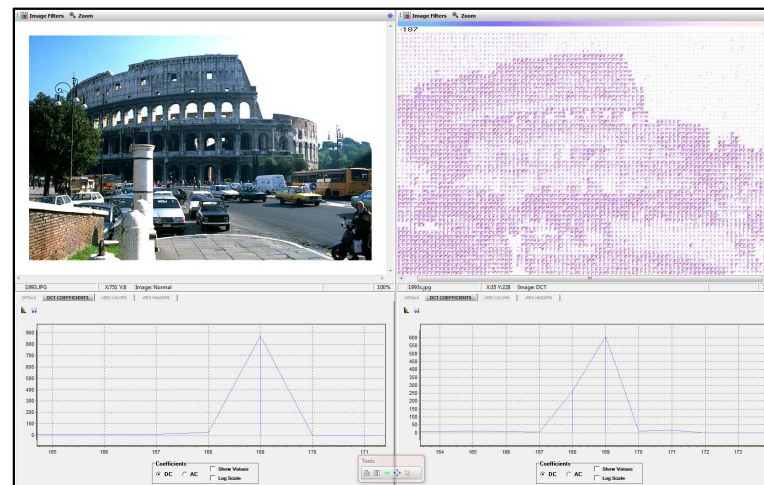


Forensic Toolkit y EnCase

- Detección de software esteganográfico
 - Pueden usar el HashKeeper, Maresware, y National Software Reference Library.
- A tomar en cuenta
 - Tamaño software esteganográfico en comparación con capacidad medios de almacenamiento temporal

Stego Suite = Stego Hunter

- Conjunto de herramientas para investigación forense
- Herramientas que se incluyen
 - Stego Hunter
 - Stego Analyst
 - Stego Break
- Producido por WetStone Technologies
 - <https://www.wetstonetech.com/>



Introducción a la criptología

Roberto Gómez Cárdenas

ITESM-CEM

rogomez@itesm.mx