TECNOLÓGICO DE MONTERREY®

Introducción a la criptologia

Roberto Gómez Cárdenas

rogomez@itesm.mx

http://cryptomex.org

TECNOLÓGICO DE MONTERREY®

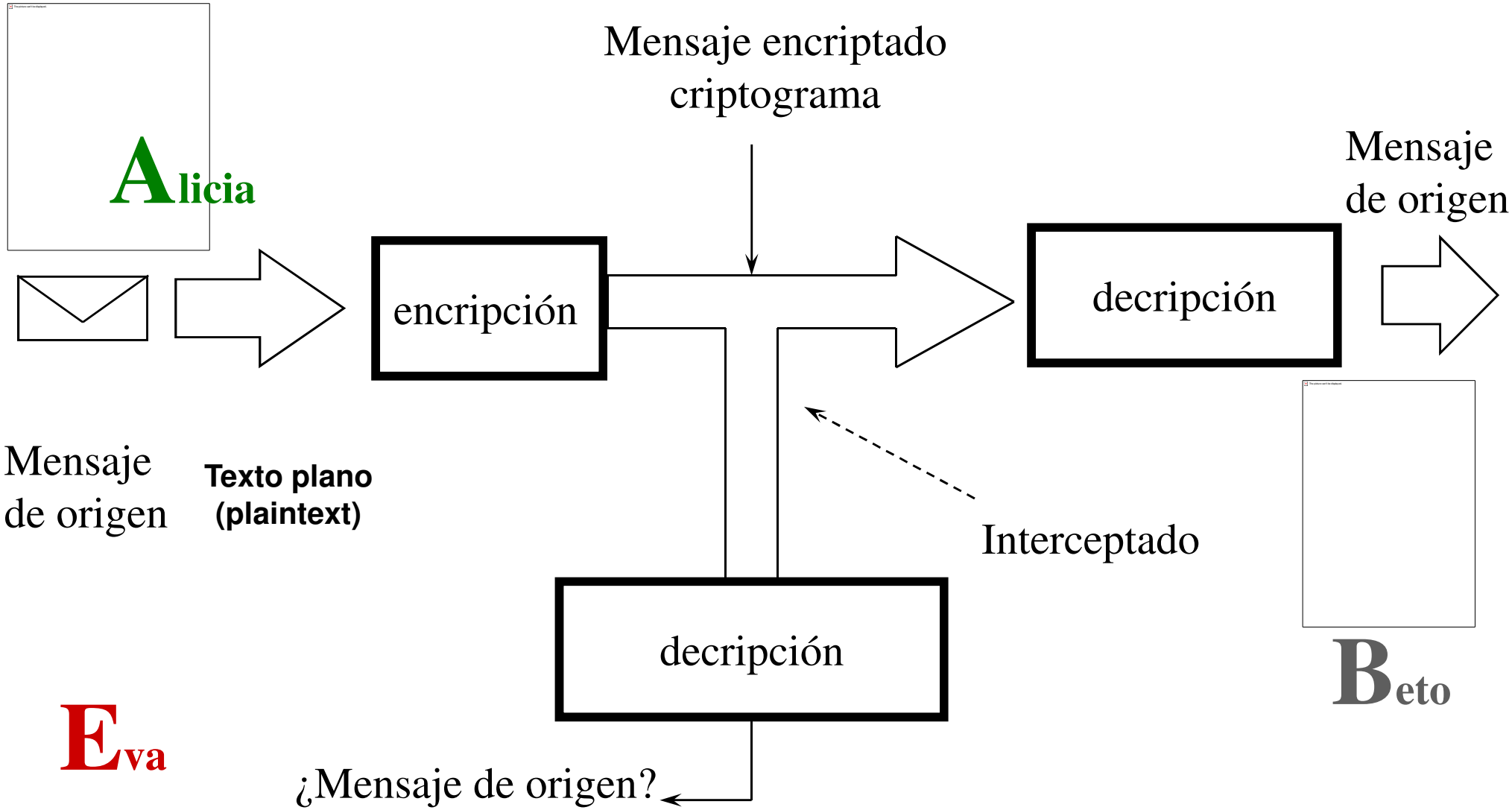
El Triángulo de la Seguridad

TECNOLÓGICO DE MONTERREY®

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 encripción/decripción



TECNOLÓGICO DE MONTERREY®

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

Clasificación seguridad criptográfica

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

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

TECNOLÓGICO DE MONTERREY®

Criptografía y seguridad

- En la práctica la seguridad que ofrece un criptosistema consiste en mostrar que *"cualquier ataque que tiene una probabilidad de romper la llave requiere de una cantidad infinita de computación"*.
- Un sistema criptográfico se dice *inseguro* cuando los contenidos de encripción pueden ser descifrados en un tiempo NO muy grande.

TECNOLÓGICO DE MONTERREY®

Obscuridad vs Seguridad

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

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

Principio de Kerchkhoffs

TECNOLÓGICO DE MONTERREY®

Entropía

- Teoría Información
  - Medida de la incertidumbre asociada con una variable aleatoria
- Criptografia
  - Entropía debe ser proporcionado por el criptosistema para su inserción en el texto plano de un mensaje de tal forma que neutralice la estructura que esta presente en el texto plano de un mensaje inseguro
- Características
  - Aumento de la entropía = aumento del desorden.
  - Mucha entropía cuando hay mucha imprevisibilidad.
- ¿Cómo se logra?
  - Confusión: Intenta ocultar la relación directa entre el texto plano y el cifrado.
  - Difusión: Diluir la redundancia del texto por todo el texto cifrado

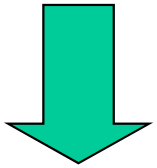
TECNOLÓGICO DE MONTERREY®

Procedimientos clásicos de encripción

- Primeros métodos criptográficos
  - Epoca romana hasta siglo XX
- Basados en dos técnicas
  - Transposición
  - Substitución

Transposición

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



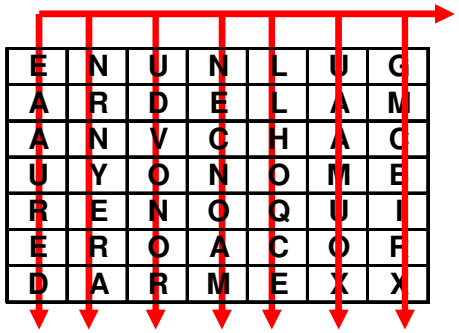
S I N O I O N A C T R P S

- 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

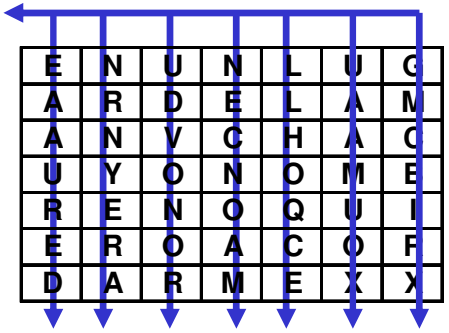
EN UN LUGAR DE LA MANCHA
DE CUYO NOMBRE NO
QUIERO ACORDARME

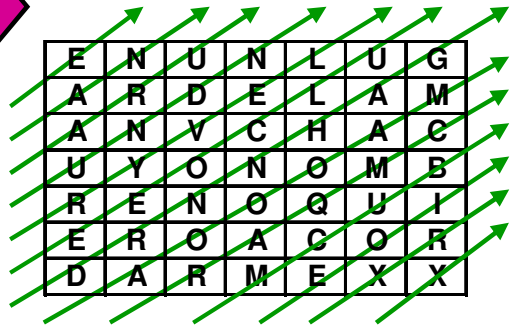
E	N	U	N	L	U	G
A	R	D	E	L	A	M
A	N	V	C	H	A	C
U	Y	O	N	O	M	B
R	E	N	O	Q	U	I
E	R	O	A	C	O	R
D	A	R	M	E	X	X



EAAURED NRNYERA UDVONOR NECNOAM LLHOCQE UAAMUOX GMCBIRX

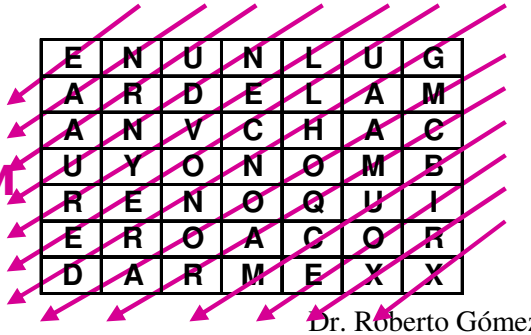
GMCBIRX UAAMUOX LLHOCQE NECNOAM UDVONOR NRNYERA EAAURED





EANARUU NDNRYVE LEEOCLU DRNNHAG AOOOAMR AQMCMCU BEOIXRX

ENAURAN DNULEVY RULCOEE GAHNNRD MAOOOAC MQARBUCM IOERXX

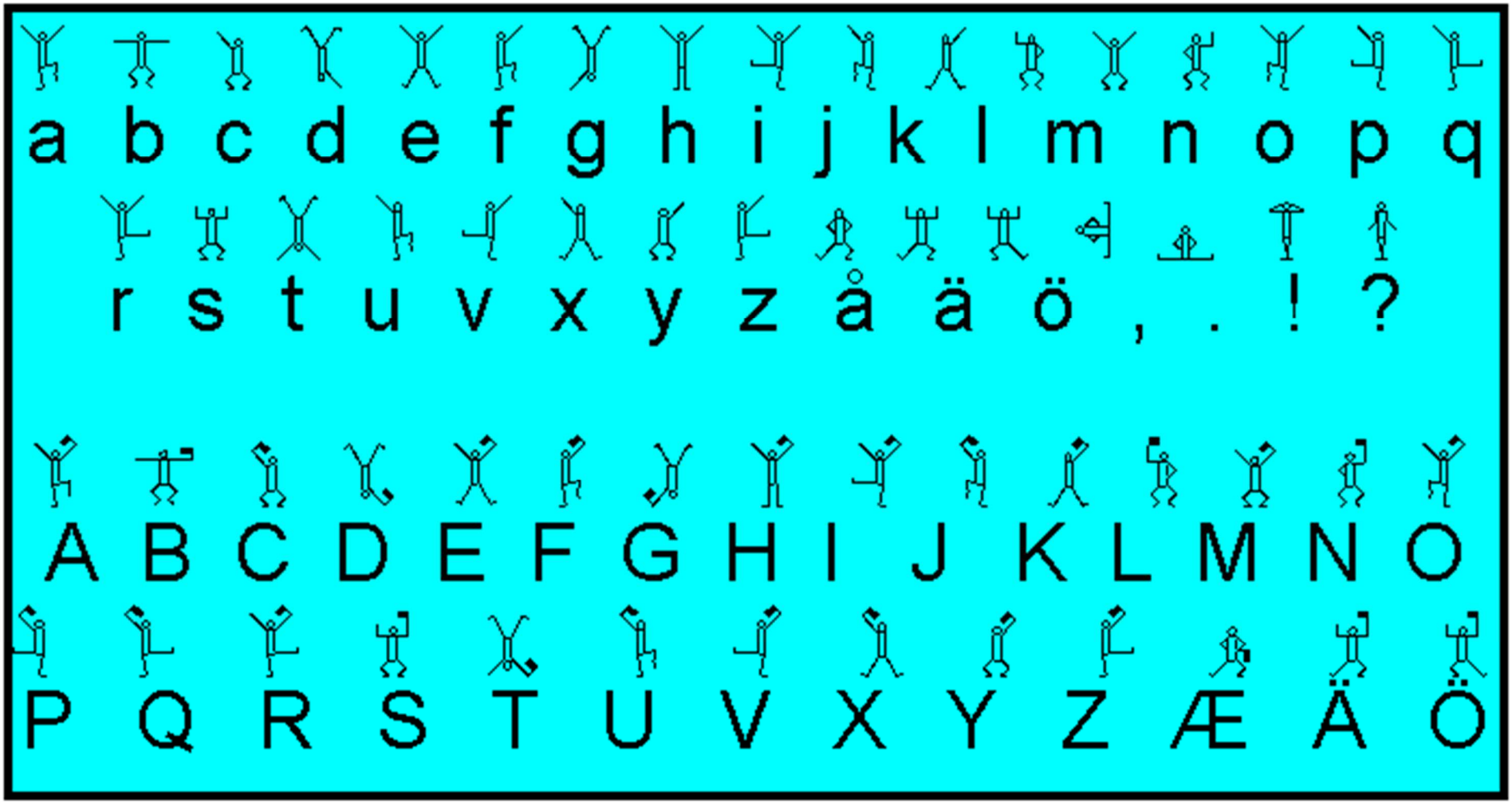


TECNOLÓGICO DE MONTERREY®

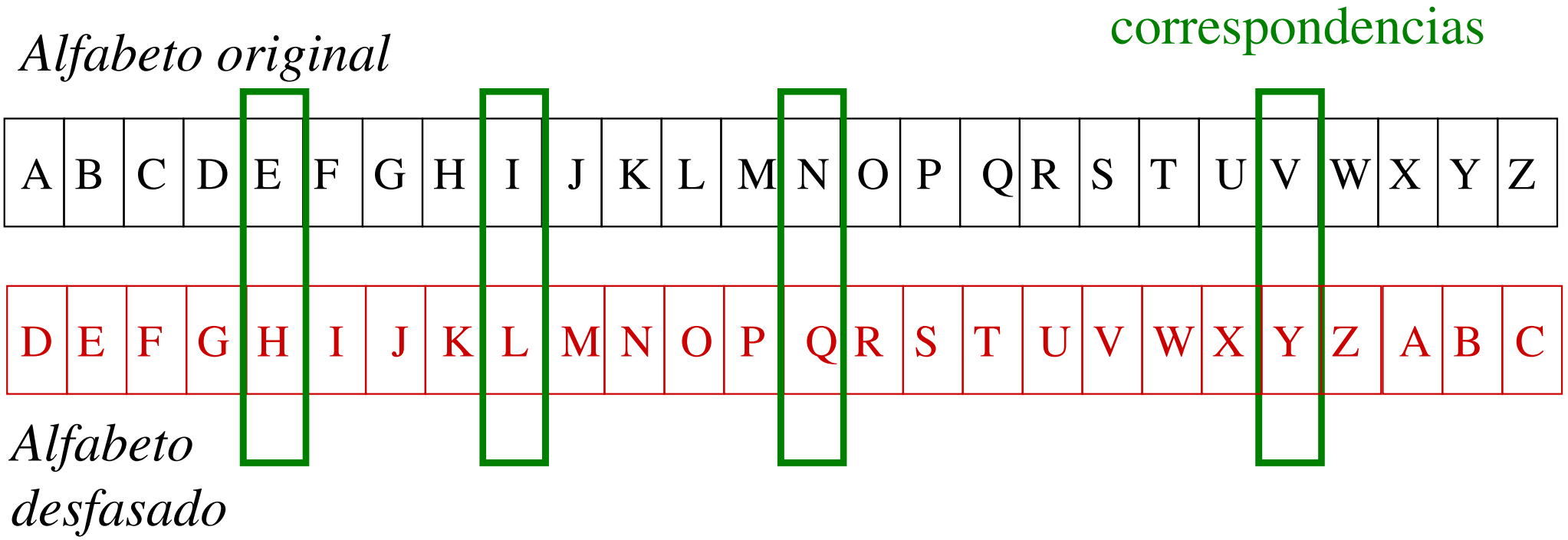
La substitución

- 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

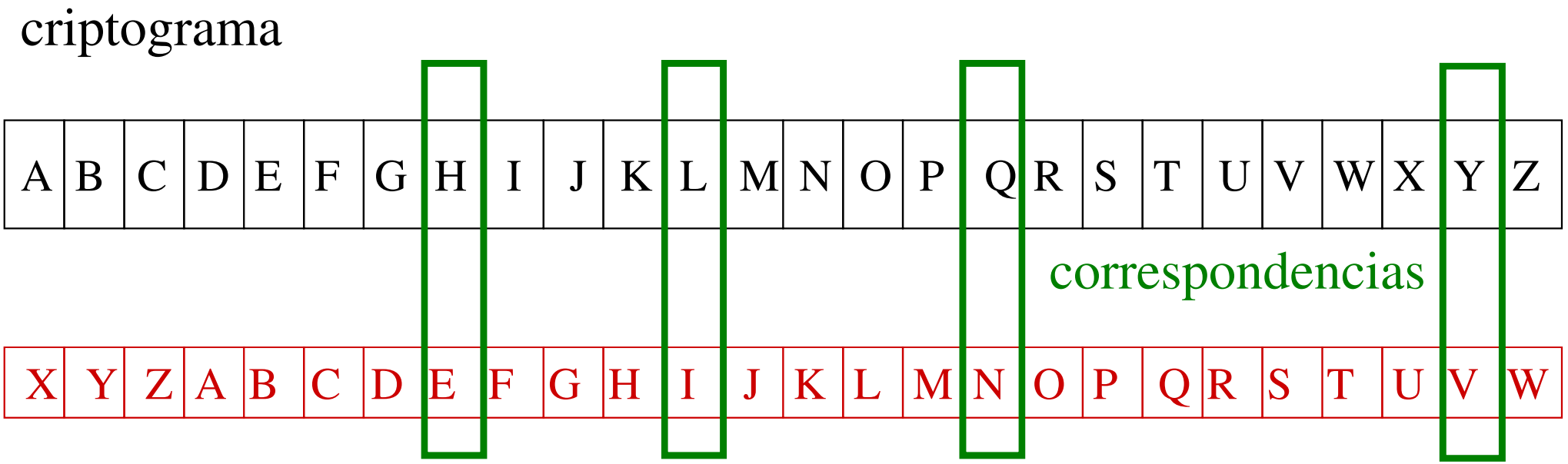


Cifrado de Cesar



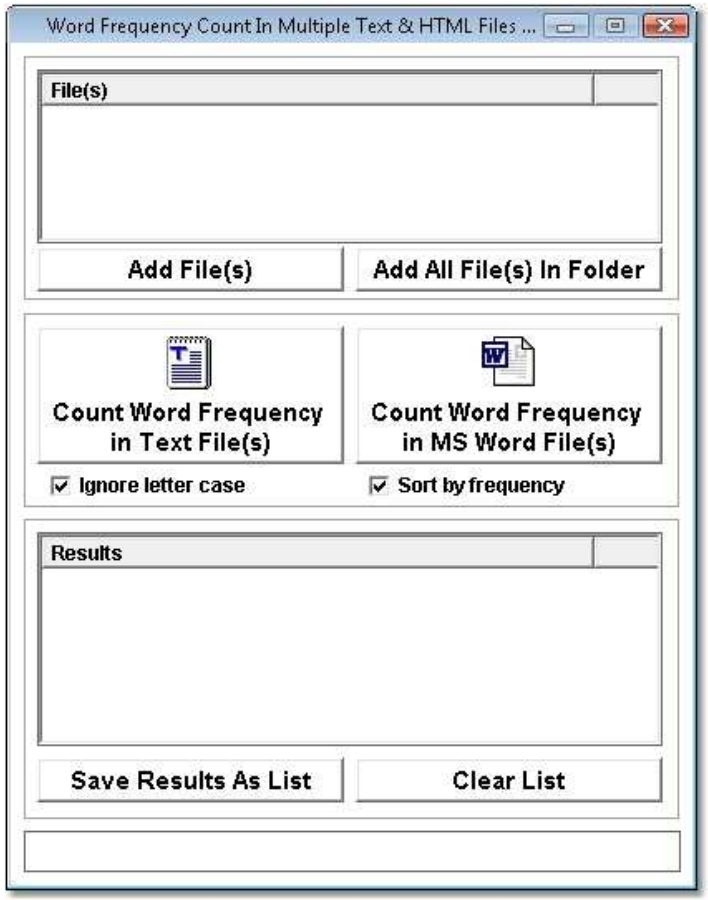
Mensaje:	VENI	VIDI	VICI
Llave:	DDDD	DDDD	DDDD
Criptograma:	YHQL	YLGL	YLFL

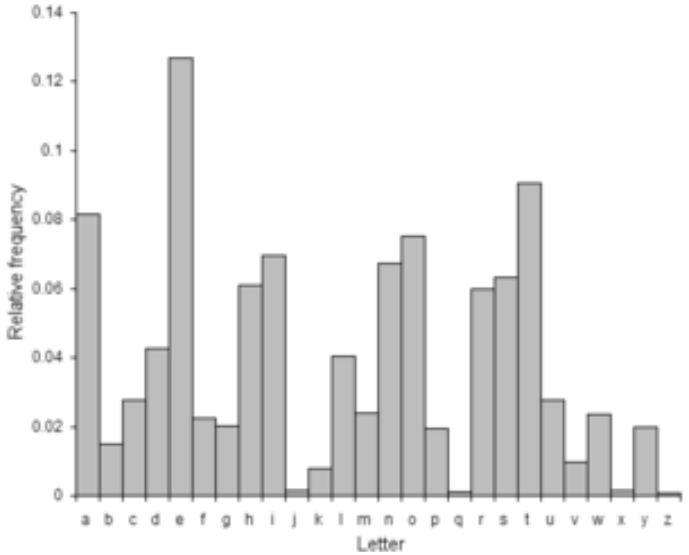
Descifrando en Cesar



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

Análisis por frecuencia





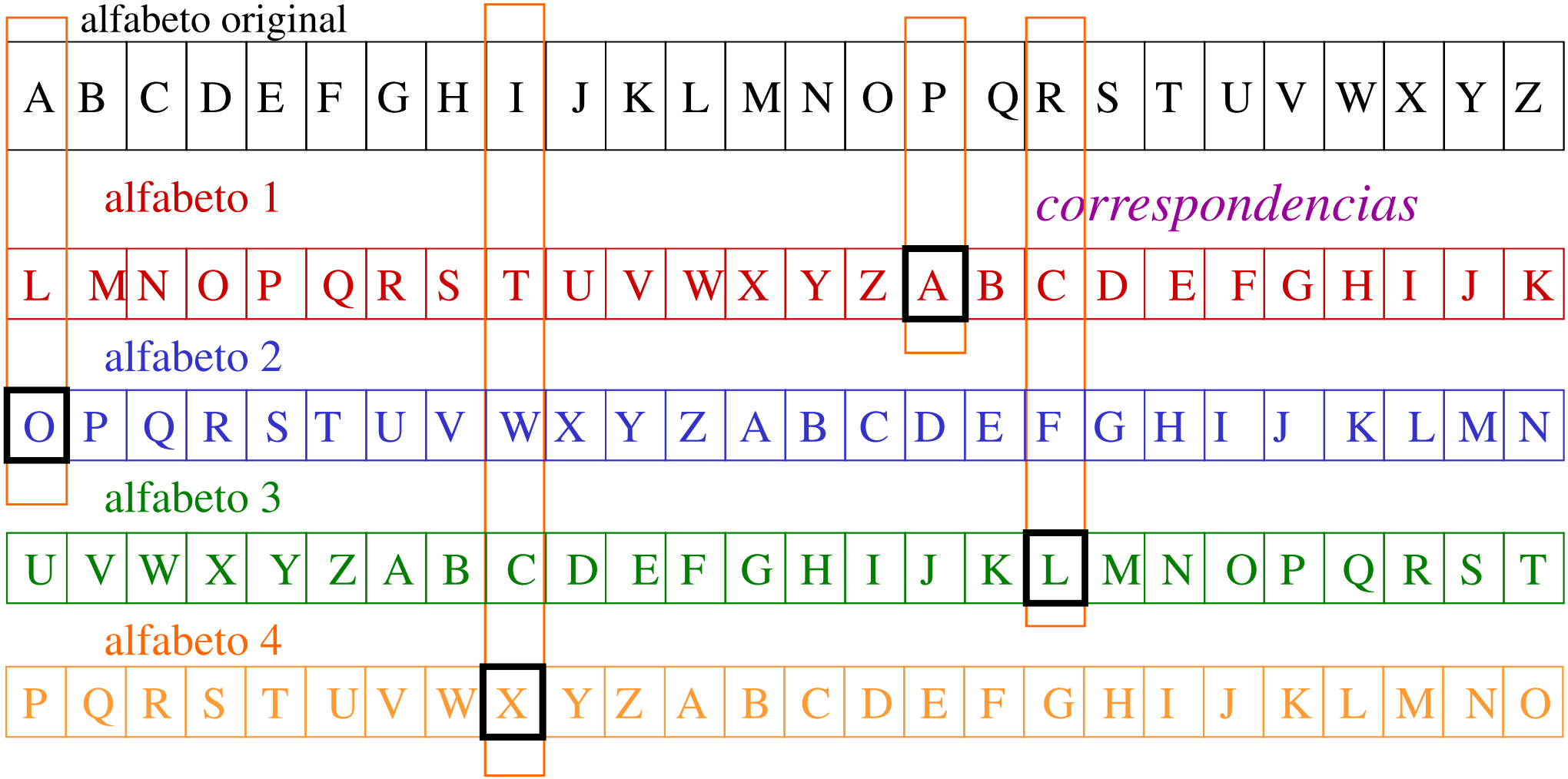
Letter	French	German	Spanish	Portuguese	Esperanto	Italian	Turkish	Swedish	Polish	Toki Pona	Dutch
a	7.636%	6.51%	12.53%	14.63%	12.12%	11.74%	11.68%	9.3%	8.0%	17.2%	7.49%
b	0.901%	1.89%	1.42%	1.04%	0.98%	0.92%	2.95%	1.3%	1.3%	0.0%	1.58%
c	3.260%	3.06%	4.68%	3.88%	0.78%	4.5%	0.97%	1.3%	3.8%	0.0%	1.24%
d	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%

TECNOLÓGICO DE MONTERREY®

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

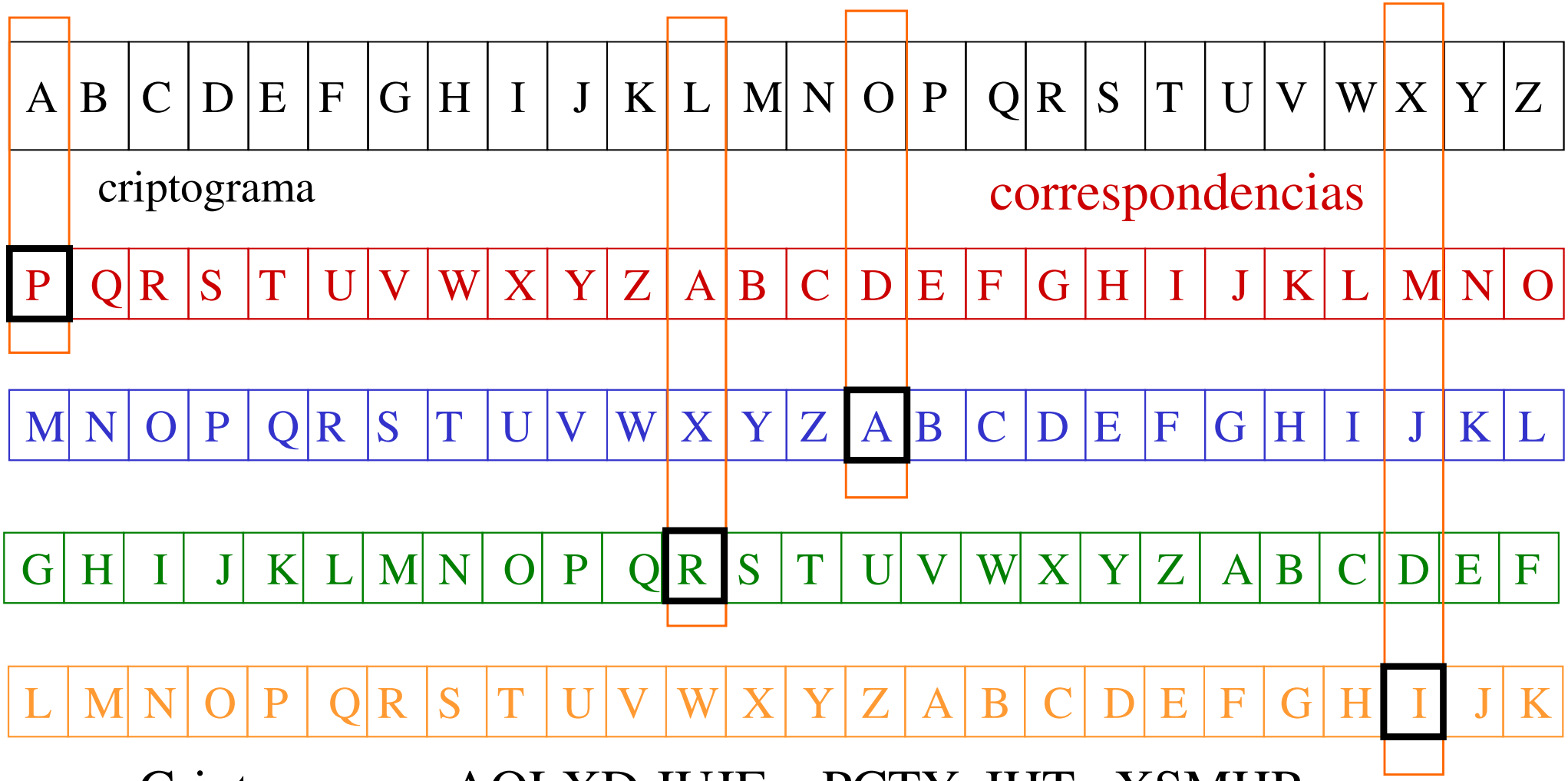


Mensaje: PARIS VAUT BIEN UNE MESSE

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

TECNOLÓGICO DE MONTERREY®

Un criptograma resultado de Vigenere

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

TECNOLÓGICO DE MONTERREY®

Encontrando patrones

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 "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

TECNOLÓGICO DE MONTERREY®

One time pad

- No consiste de una serie de palabras sino una gran serie de letras elegidas al azar
- Propone utilizar este conjunto de letras como parte de un criptosistema de Vigenere
- Principio funcionamiento:
  - Primer paso: conseguir un bloque (pad) de hojas
  - Cada hoja contiene una llave única en forma de lineas de secuencias aleatorias de letras.
  - Dos copias bloque: una para emisor y otra para receptor.
  - Emisor y receptor usan las hojas del bloque para encriptar y decriptar la información.
  - Cada llave es usada una sola vez, el sistema se conoce como *onetime pad*

TECNOLÓGICO DE MONTERREY®

Ejemplo one time pad

Hoja 1
P L M O E
Z Q K J Z
L R T E A
V C R C B
Y N N R B

Hoja 2
O I W V H
P I Q Z E
T S E B L
C Y R U P
D U V N M

Hoja 3
J A B P R
M F E C F
L G U X D
D A G M R
Z K W Y I

Llave: **P L M O E Z Q K J Z L R T E A V C R C B Y**

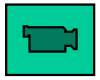
Texto claro: **a t t a c k t h e v a l l e y a t d a w n**

Criptograma: **P E F O G J J R N UL C E I Y V V U C X L**

TECNOLÓGICO DE MONTERREY®

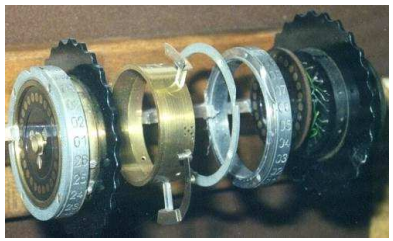
Otros criptosistemas clásicos

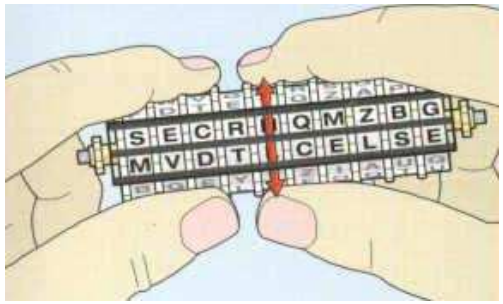
- Pigpen
- Redefence
- Nihilist
- Grilla
- El criptosistema de Bacon
- El Polybius square
- Checker board
- Atbash
- Los nomenclators
- Porta
- Playfair
- Grandpre
- Beale
- Criptosistema ADFVX

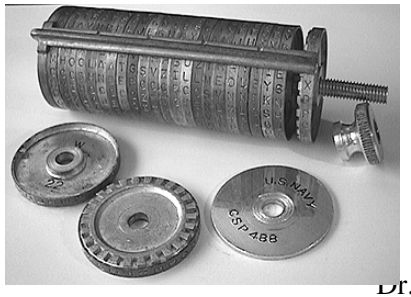


Máquinas criptograficas

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

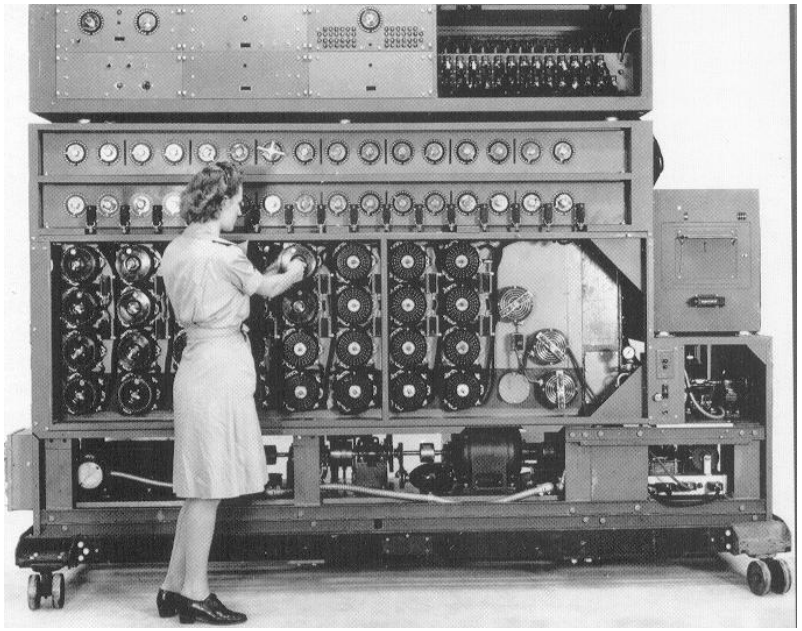


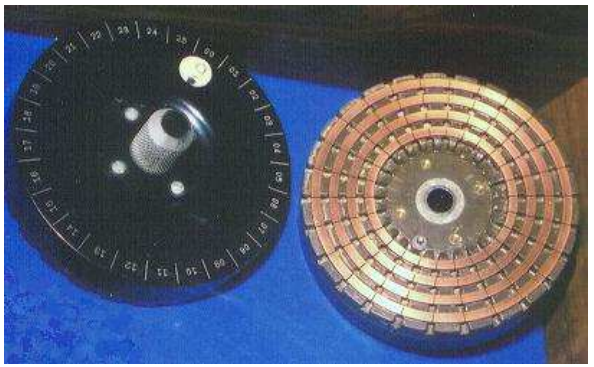




TECNOLÓGICO DE MONTERREY®

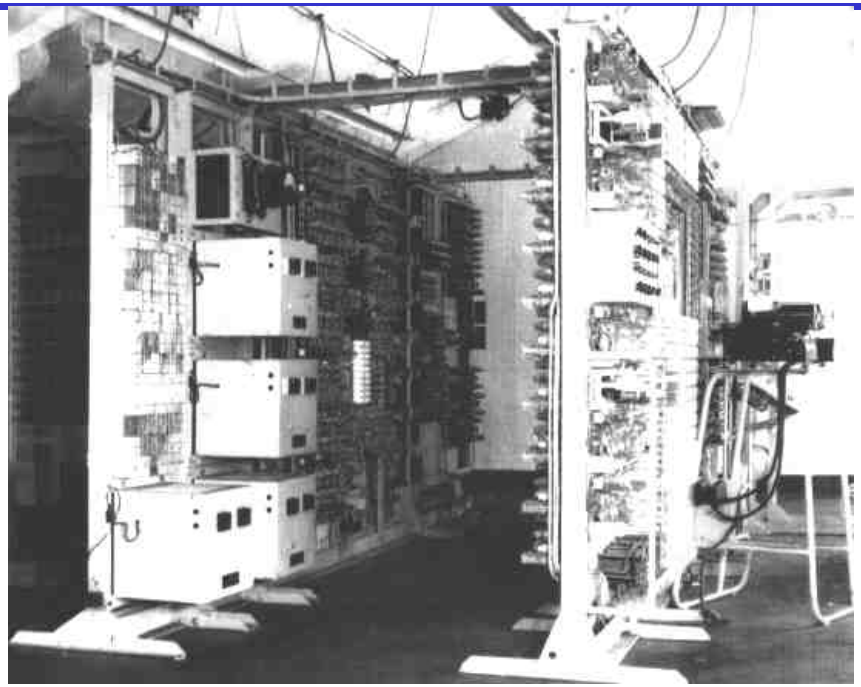
Lorenz y la Bomba

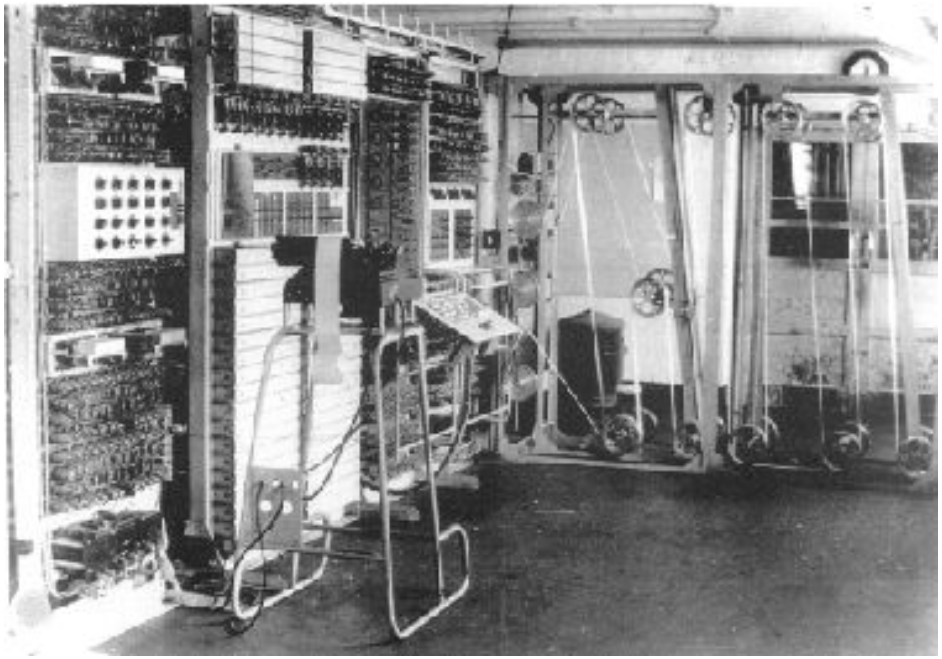




La primera computadora: Colossus

Bletchley Park





TECNOLÓGICO DE MONTERREY®

Encriptando con una computadora

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

a = 1100001
! = 0100001
& = 0100110

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

TECNOLÓGICO DE MONTERREY®

Transposición en la computadora

- Convertir mensaje a ASCII

Texto claro:
HELLO = 1001000 1000101 1001100 1001100 1001111

- Transposición: intercambiar las letras en un orden predeterminado

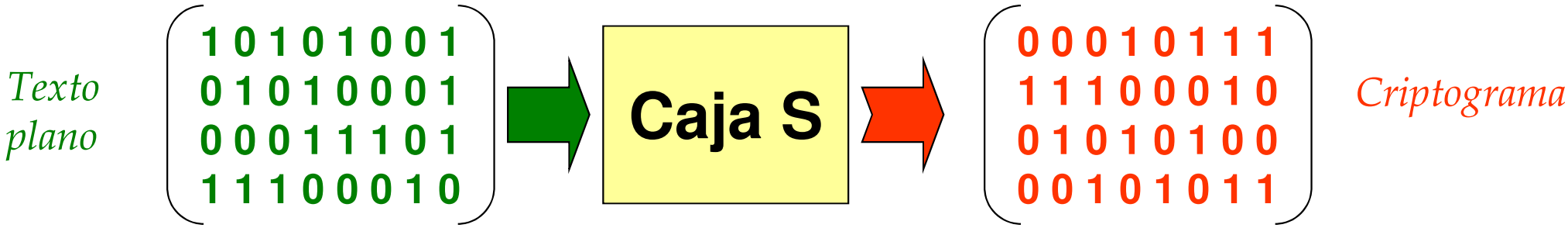
Texto claro:
HELLO = 1001000100010110011001001100 1001111
Criptograma:
LHOEL = 1001100100100010011111000101 1001100

- 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)



TECNOLÓGICO DE MONTERREY®

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)

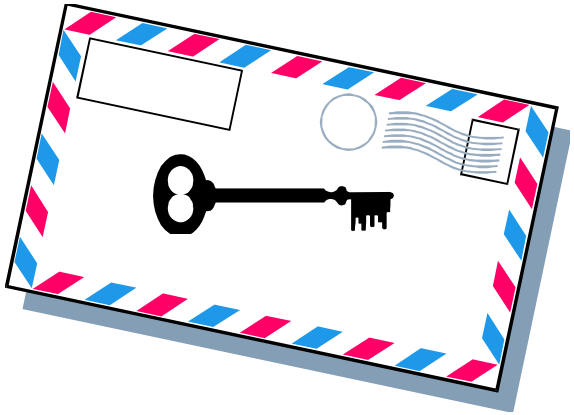
Texto claro: **HELLO**
Texto ASCII: **1001000100010110011001001100100111**
Llave: **1000100100000110101101001001100010 0**
Criptograma: **0001100000010000110100000101000101 1**

TECNOLÓGICO DE MONTERREY®

Métodos Criptográficos

- Métodos simétricos
  - llave encriptado coincide con la de descifrado
  - la llave tiene que permanecer secreta
  - emisor y receptor se han puesto de acuerdo previamente o existe un centro de distribución de llaves
  - 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

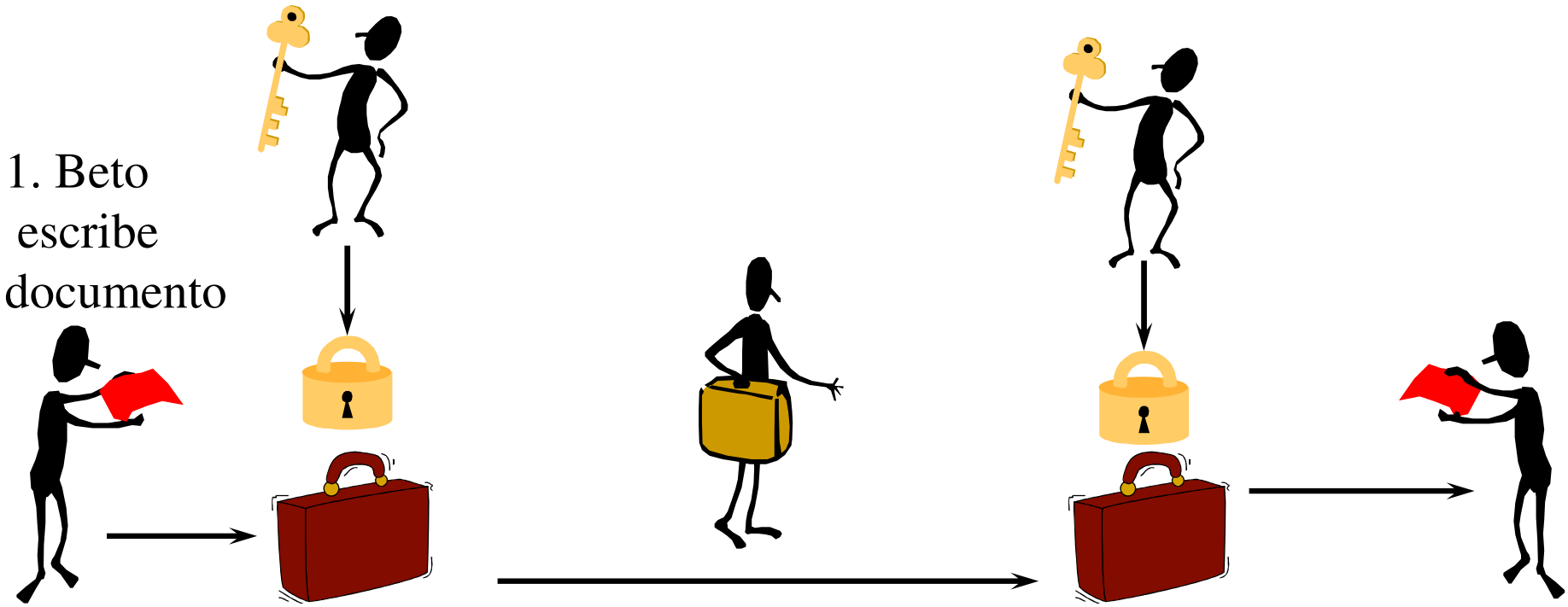
Algoritmos encripción simétricos



Encripción 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.



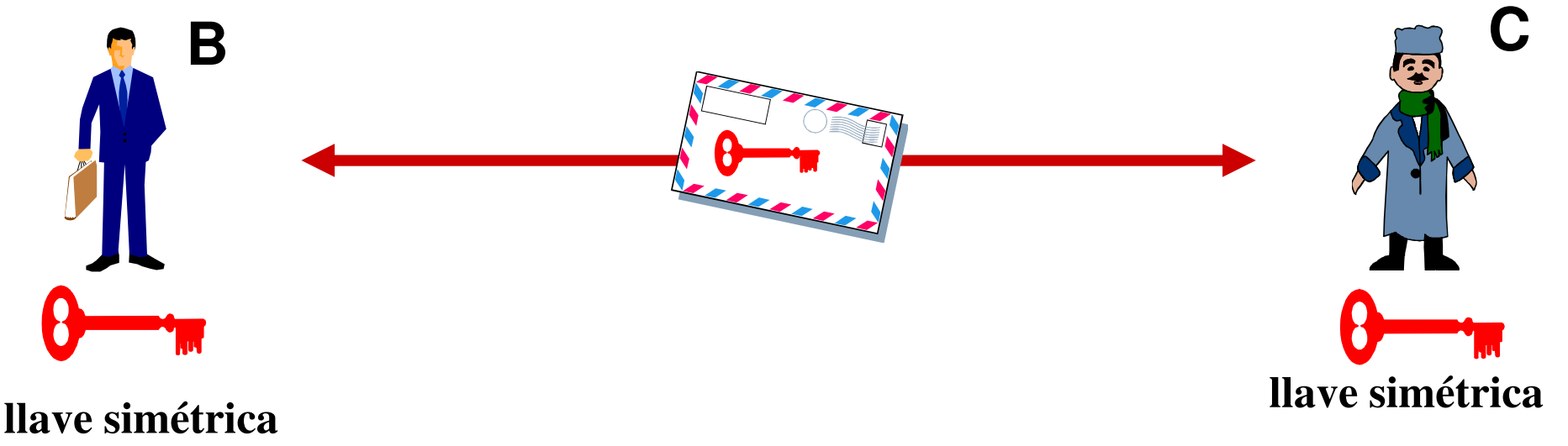
1. Beto escribe documento

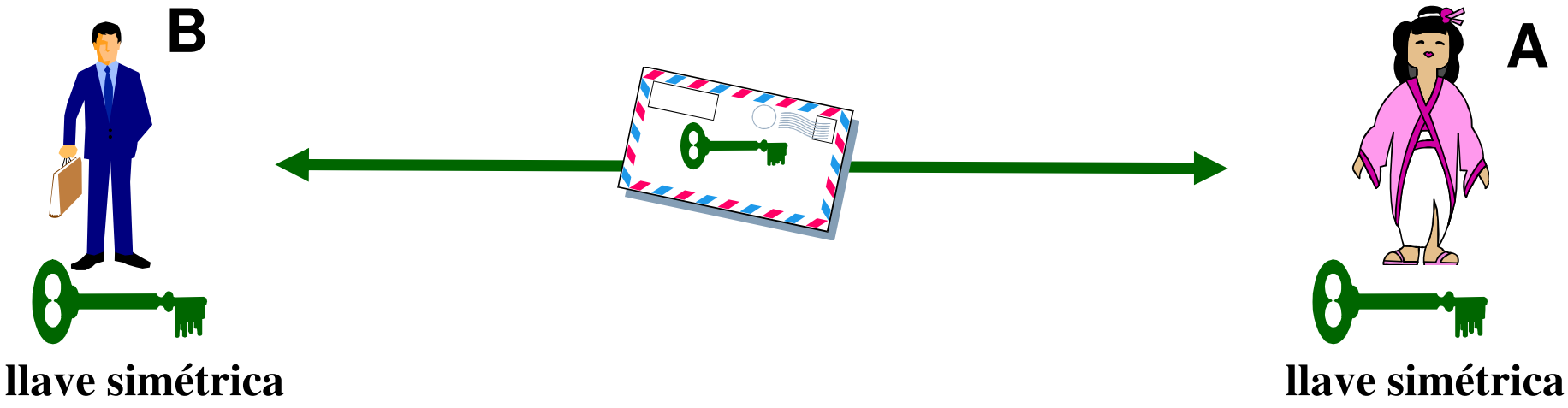
2. Beto coloca el documento en la caja fuerte

4. La caja se trans-porta hacia Alicia

6. Alicia obtiene el documento.

Esquema general encripción llave secreta

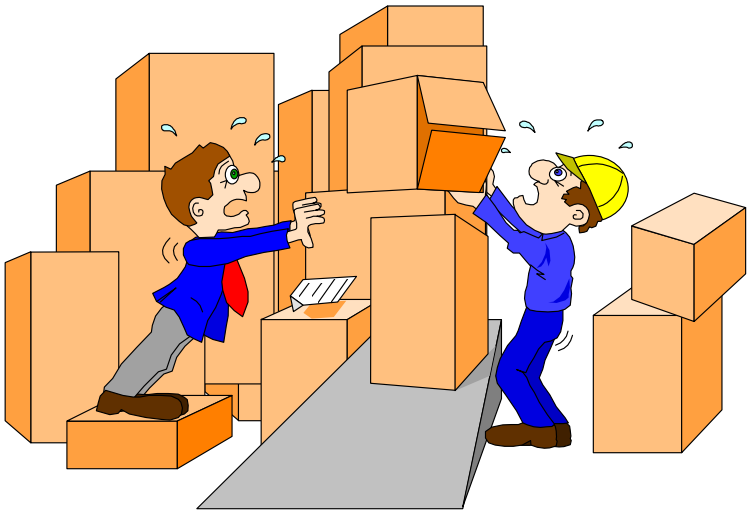




Clasificación métodos encripción simetricos

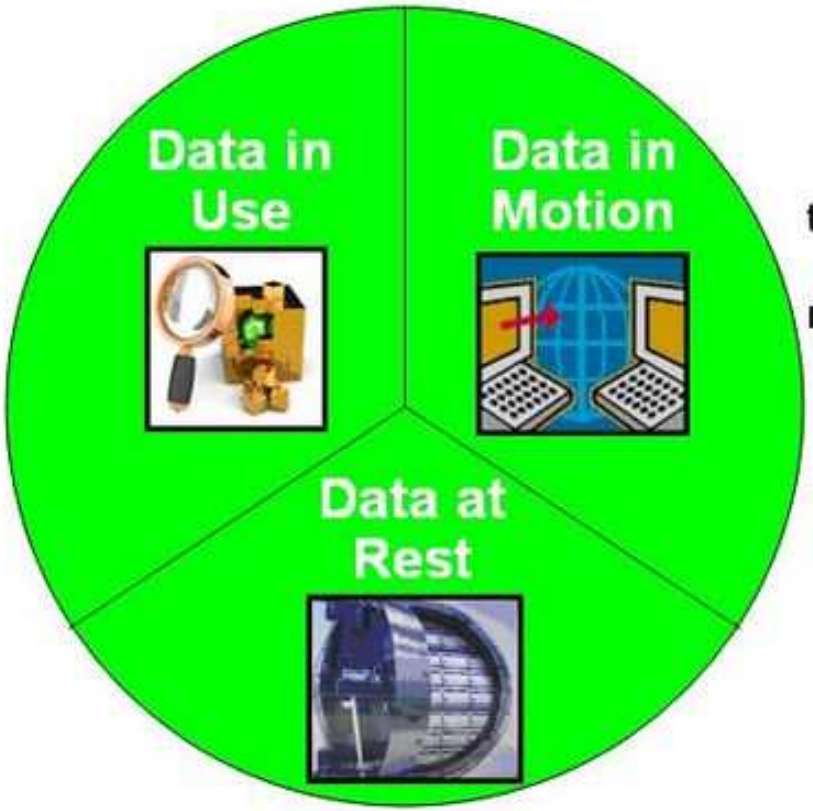
- Encripción en flujo

- Encripción en bloques



Datos en reposo y movimiento

Data in Use:
Active data under constant change stored physically in databases, data warehouses, spreadsheets etc.



Data in Motion:
Data that is traversing a network or temporarily residing in computer memory to be read or updated.

Data at Rest:
Inactive data stored physically in databases, data warehouses, spreadsheets, archives, tapes, off-site backups etc.

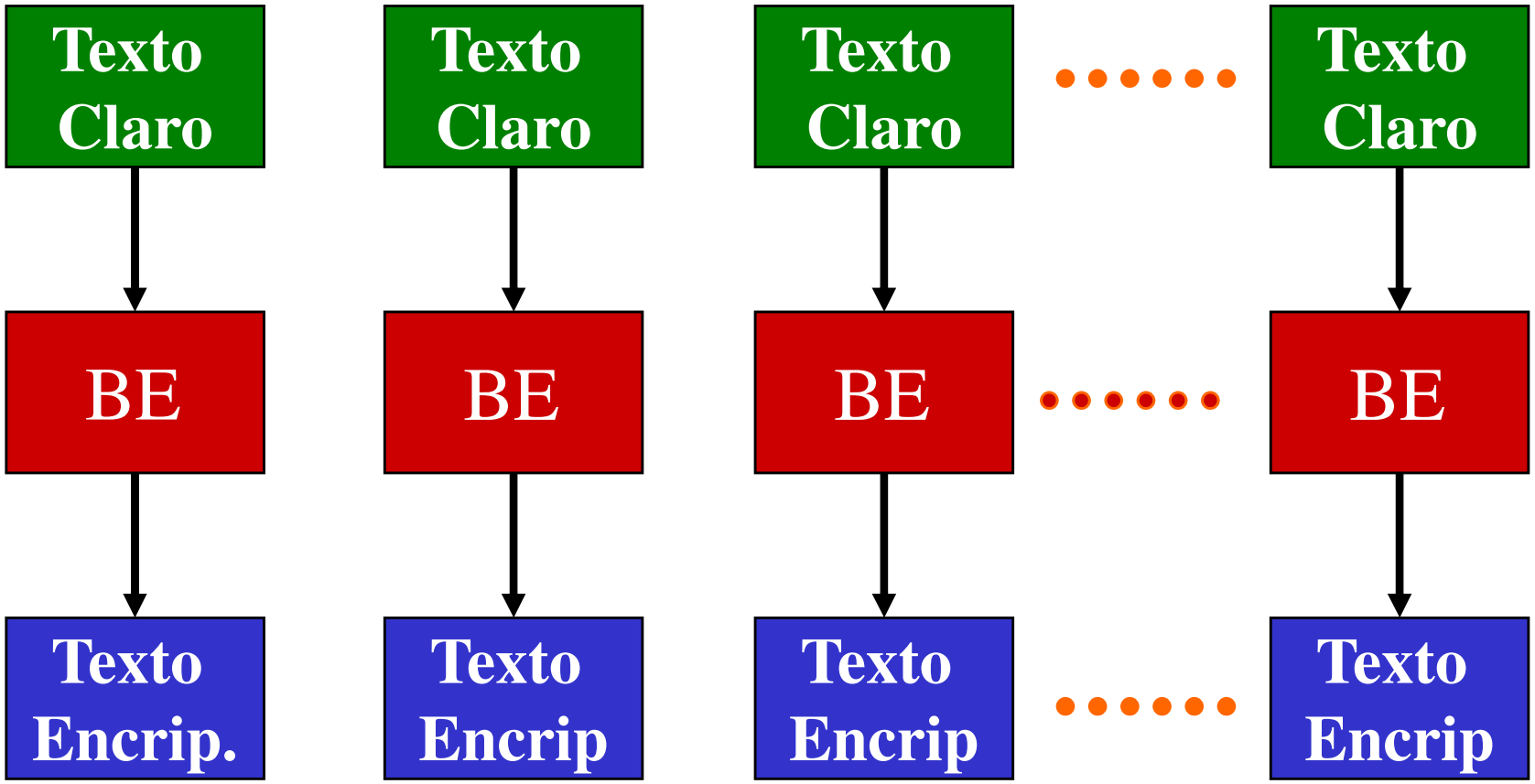
Algoritmos de Encripcion Simétrica en Bloque

TECNOLÓGICO DE MONTERREY®

Métodos de encripción en bloque

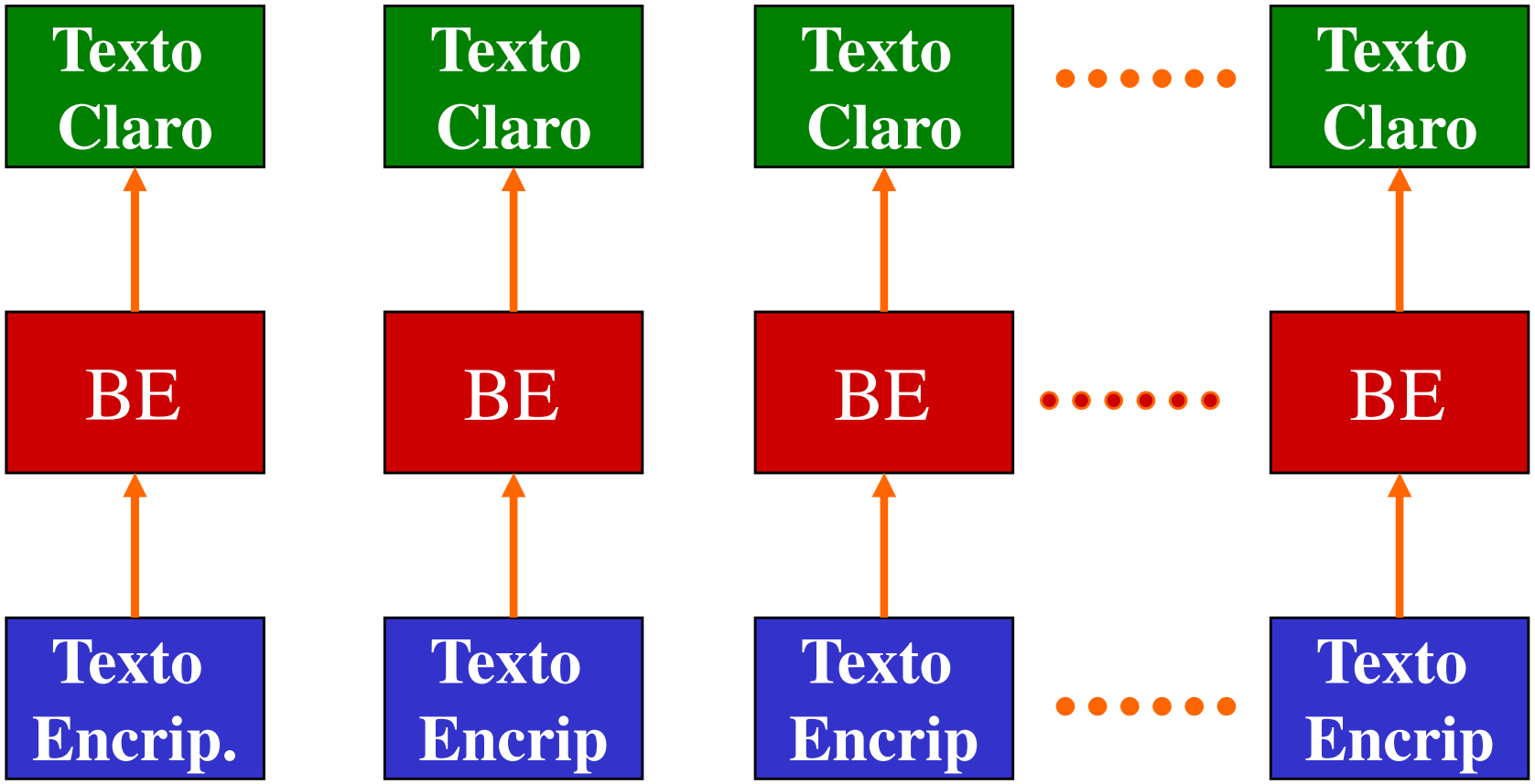
- Se encripta el mensaje original agrupando los símbolos en grupos (bloques) de dos o más elementos
- Modos operación de encripción en bloque:
  - ECB: Electronic Code Book
  - CBC: Cipher Block Chaining

Esquema ECB de encripción en bloque



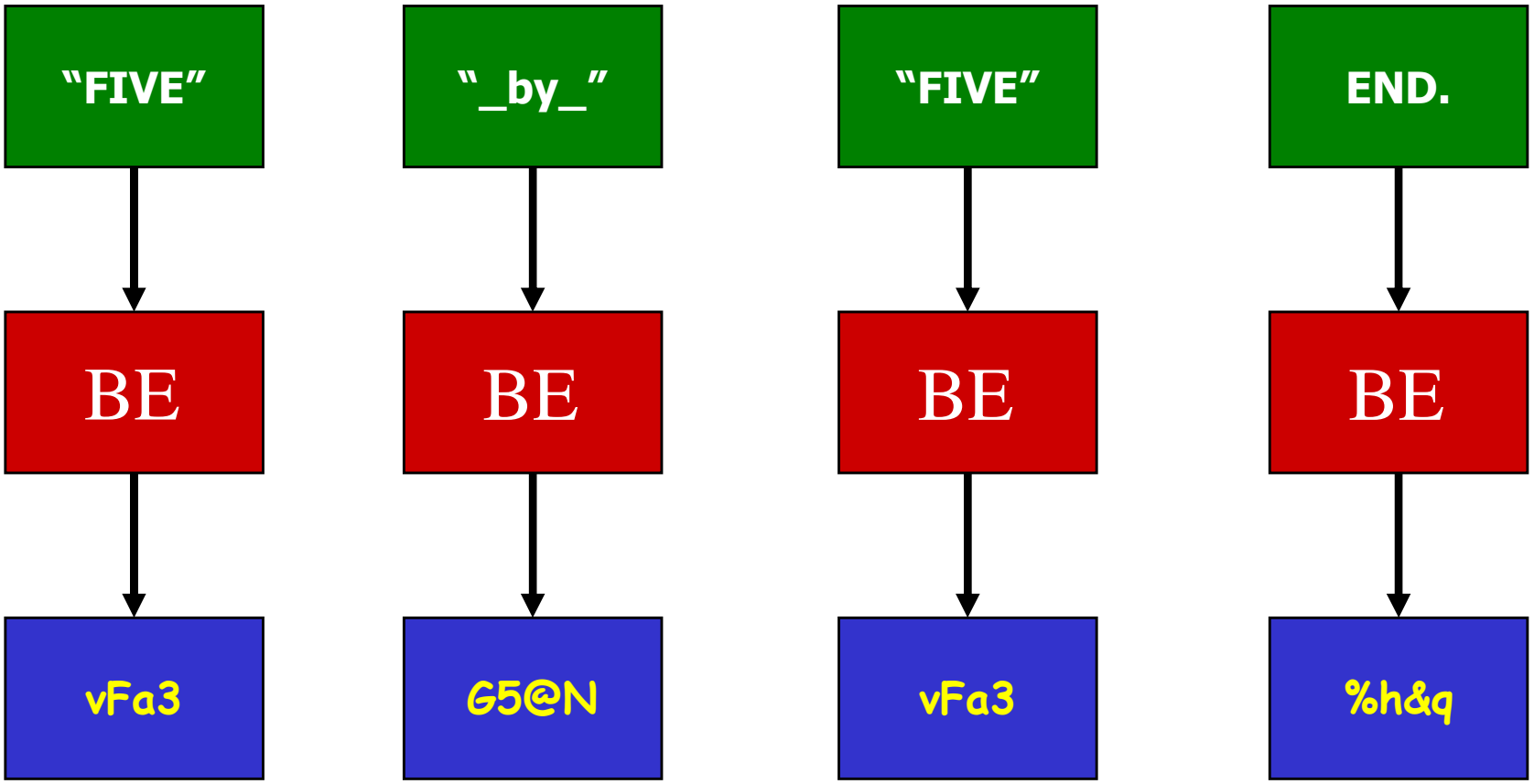
ECB: Electronic Code Book

Esquema ECB decripción en bloque

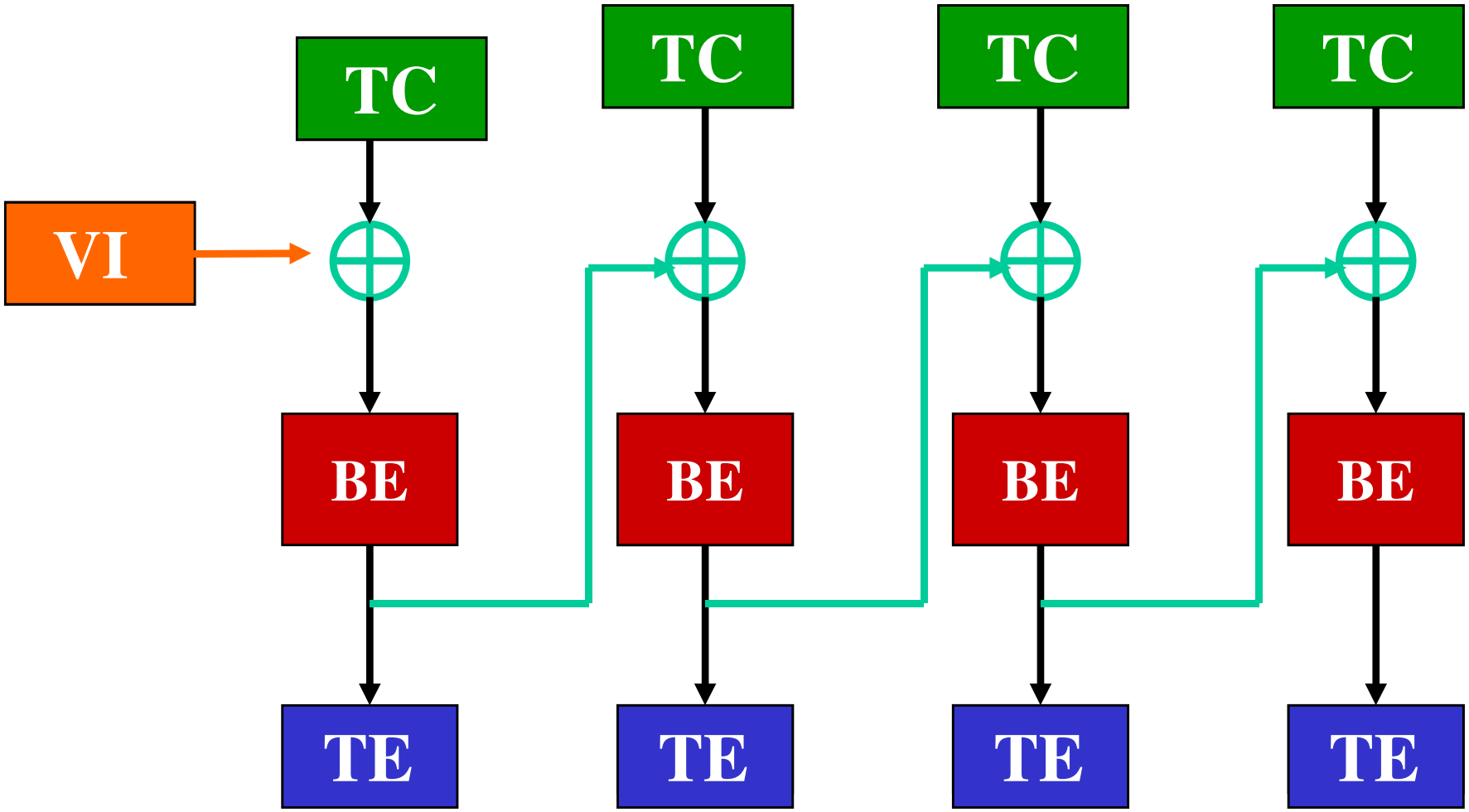


ECB: Electronic Code Book

Ejemplo problema esquema ECB



Cipher Block Chaining (CBC) Encripción

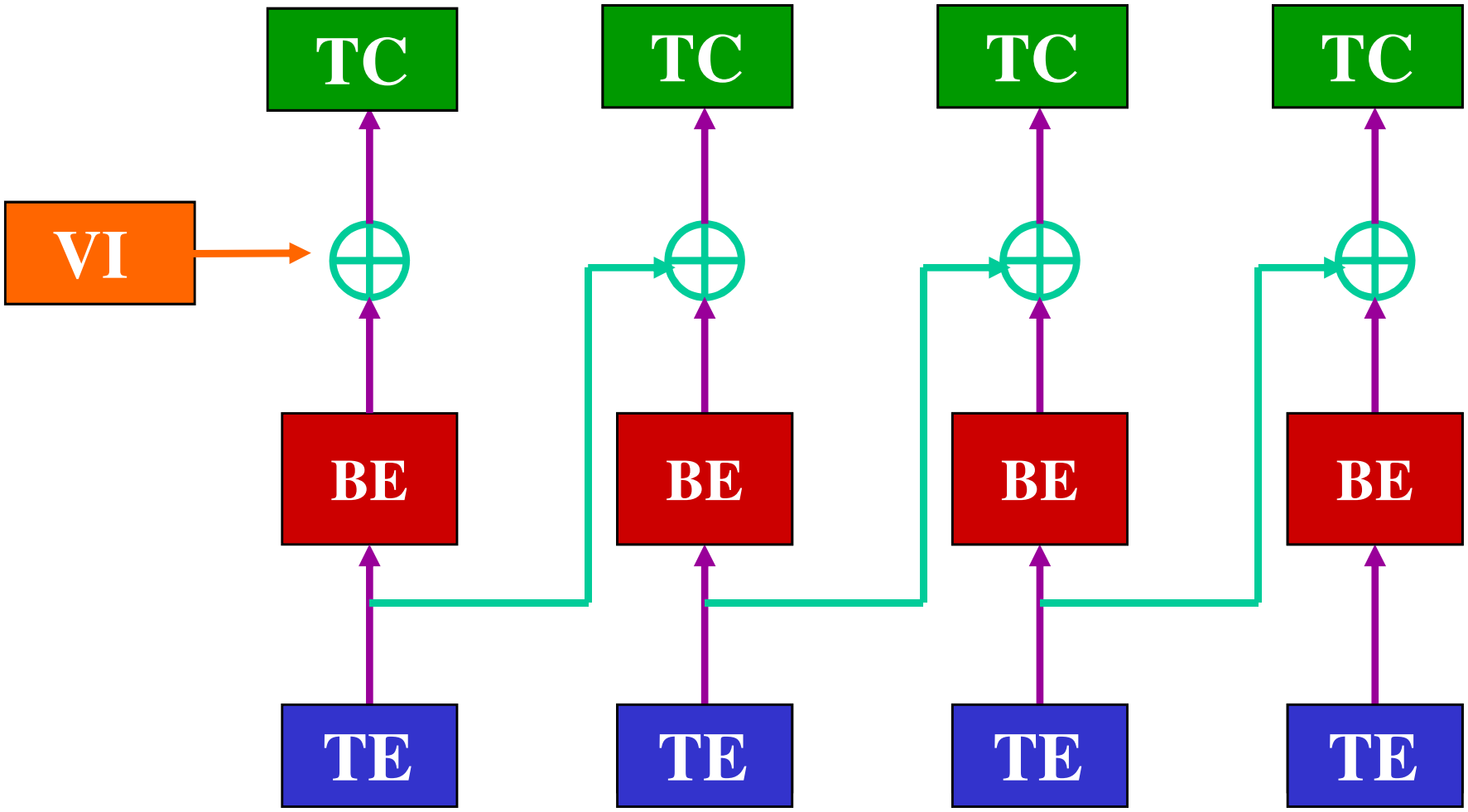


VI: Vector Inicialización aleatorio

TC: Texto Claro

TE: Texto Encriptado

Cipher Block Chaining (CBC) Encripción

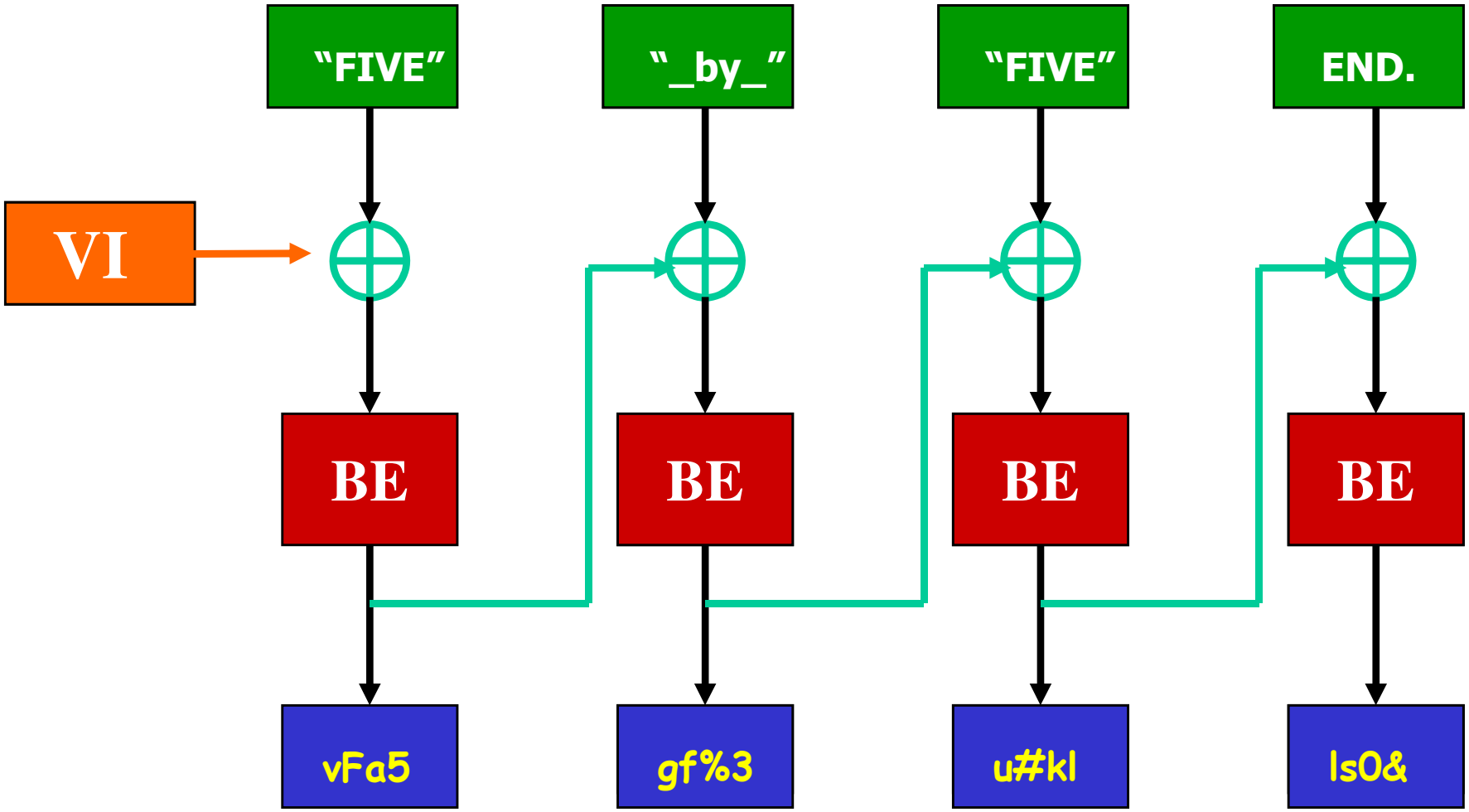


VI: Vector Inicialización aleatorio

TC: Texto Claro

TE: Texto Encriptado

Cipher Block Chaining (CBC) Decripción



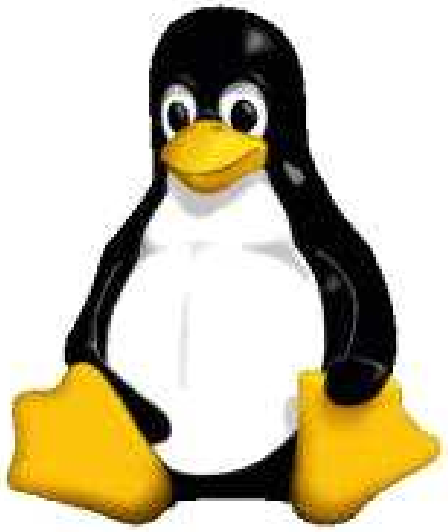
VI: Vector Inicialización aleatorio

TC: Texto Claro

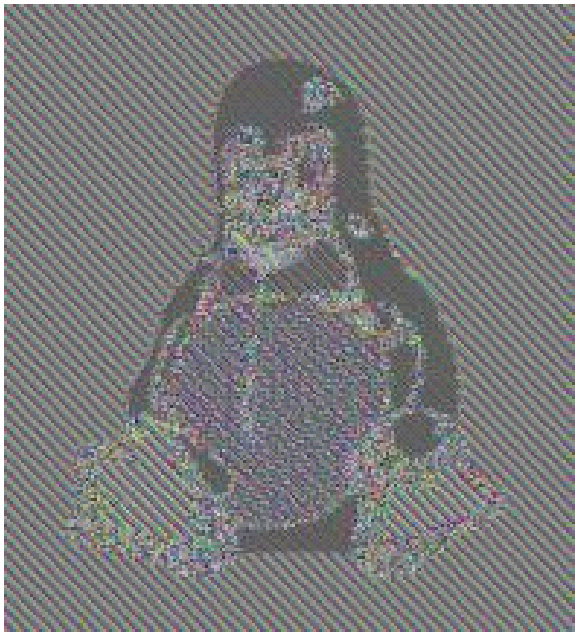
TE: Texto Encriptado

TECNOLÓGICO DE MONTERREY®

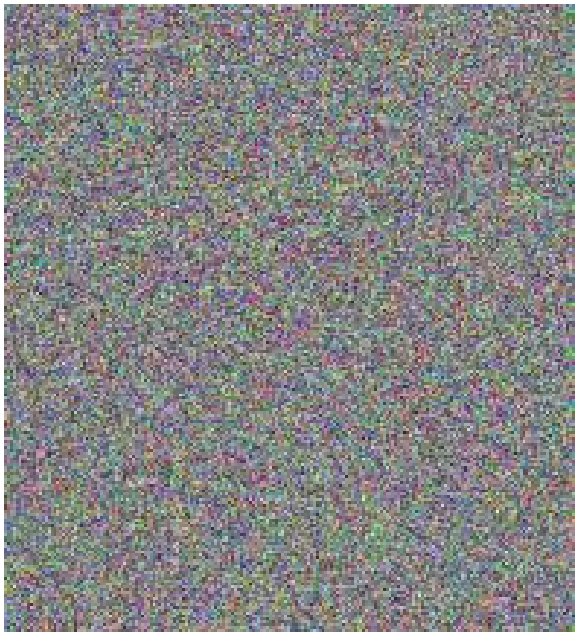
Comparando modos operación



Información original

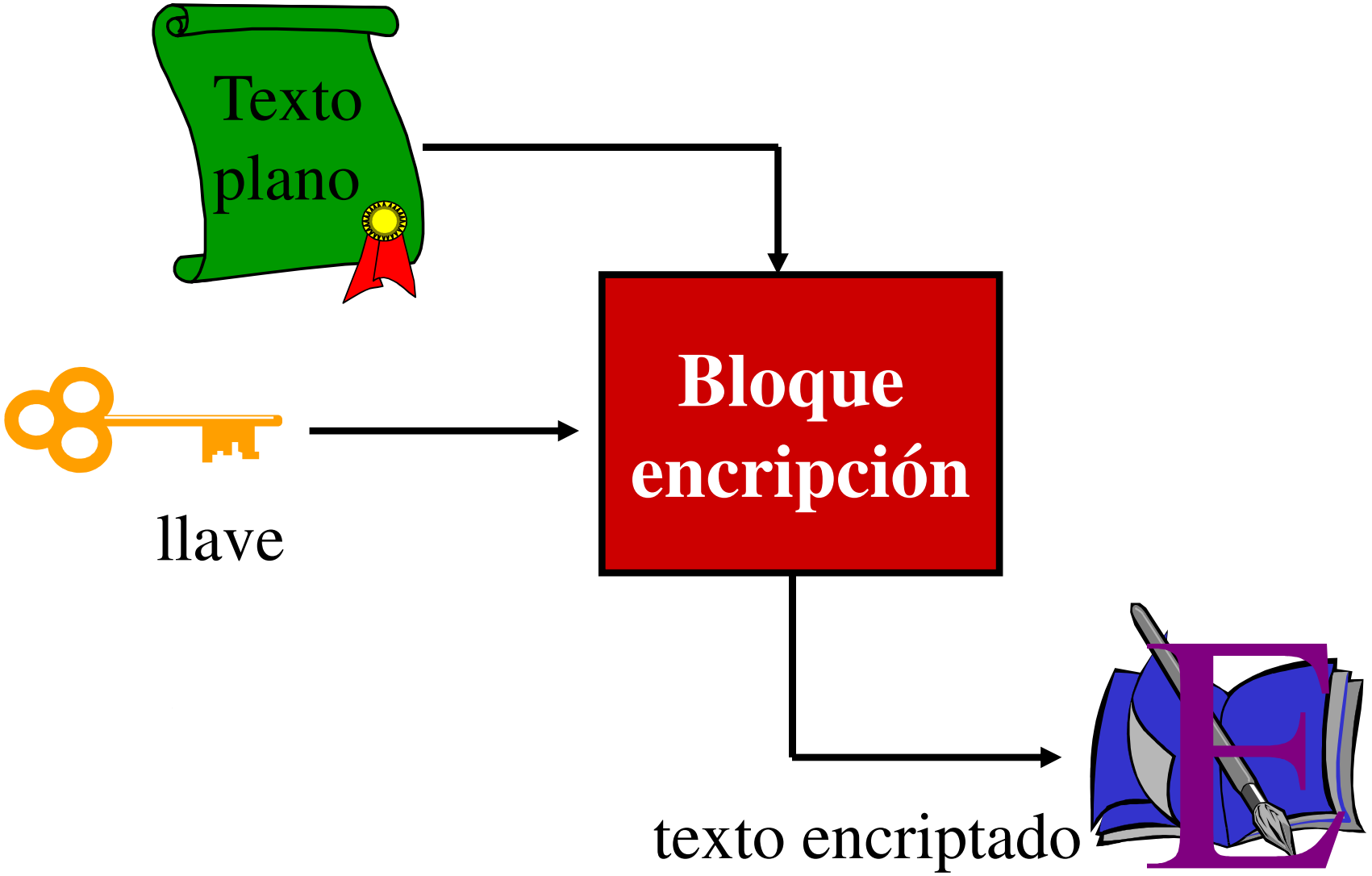


Información encriptada en modo ECB



Información encriptada en modo CBC

¿Cómo construir un block cipher?

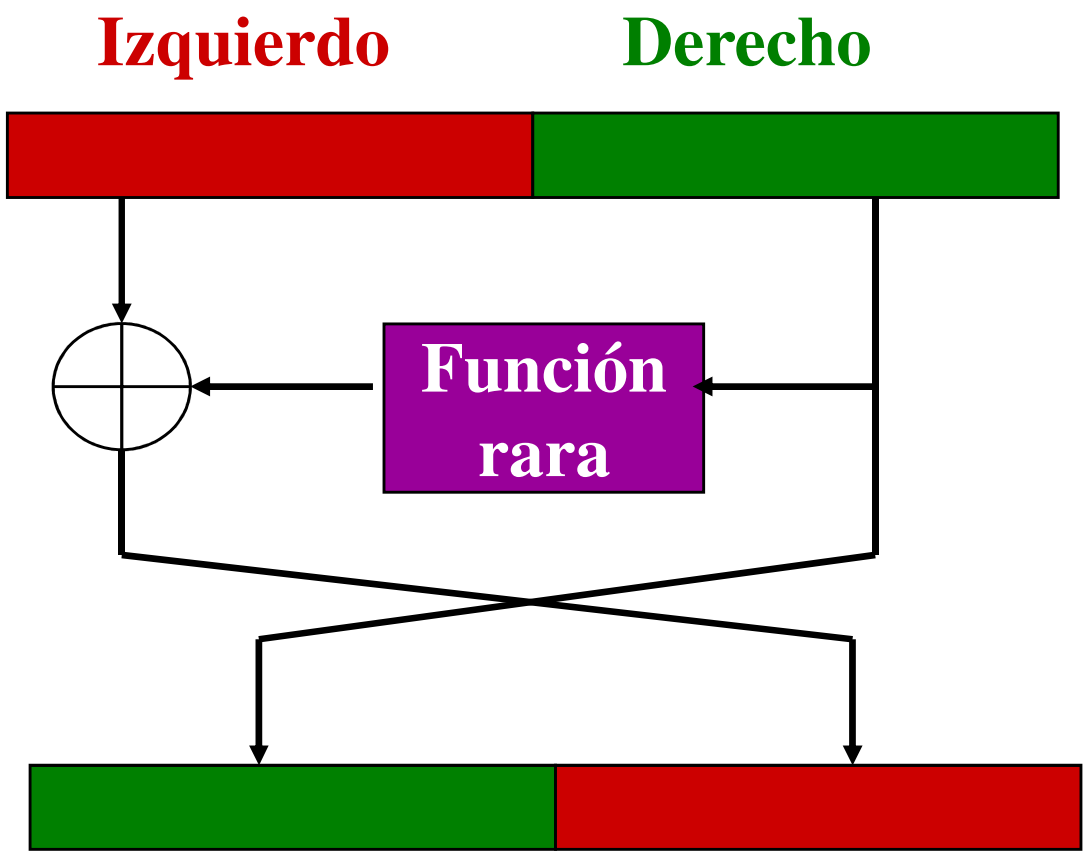


TECNOLÓGICO DE MONTERREY®

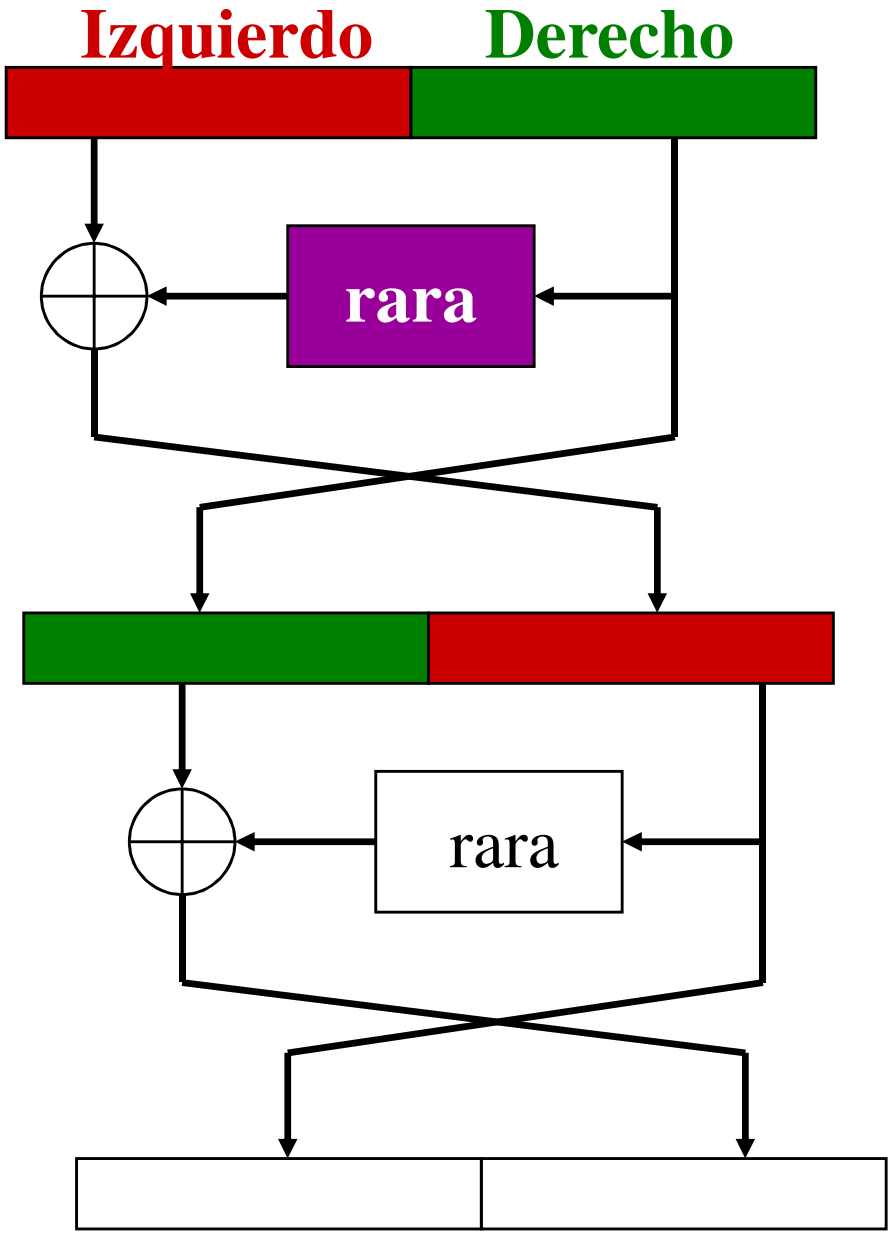
Los criptosistemas de Feistel

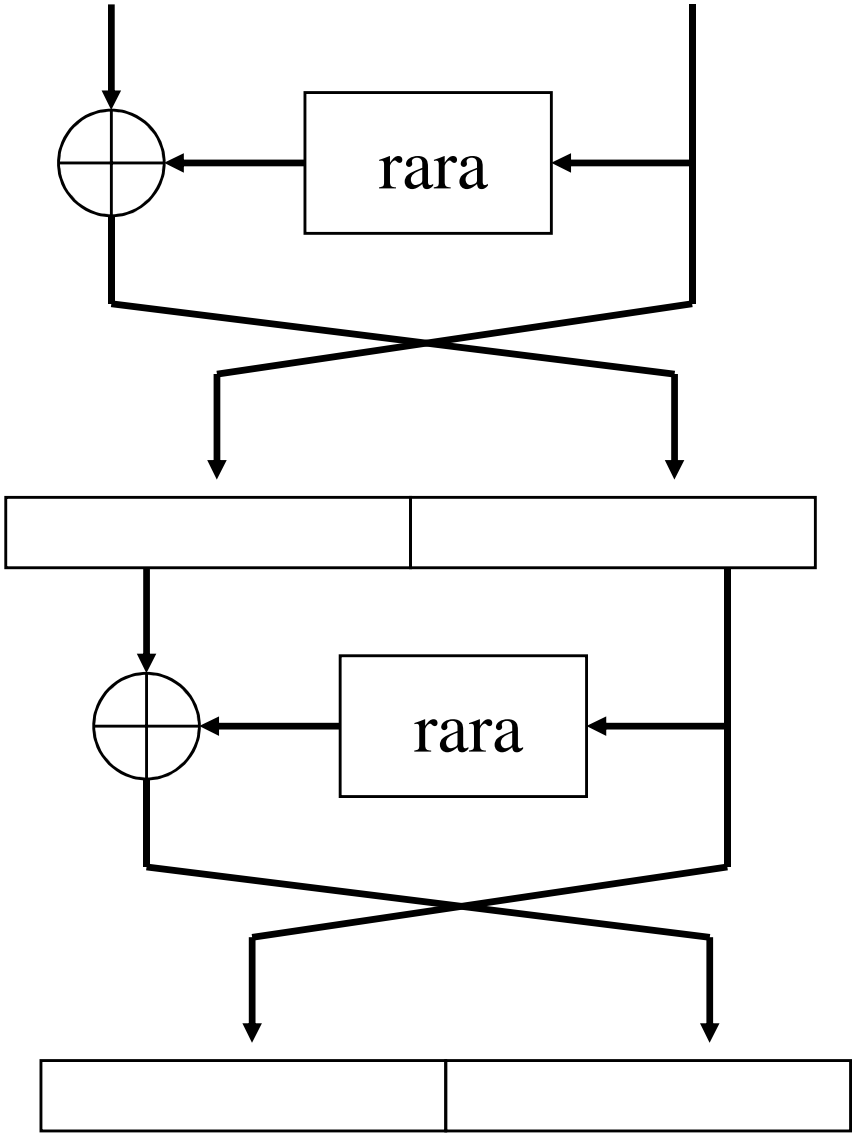
- Criptosistemas en los que el bloque de datos se divide en dos mitades y en cada vuelta de encriptación se trabaja alternadamente, con una de las mitades
- Ejemplos:
  - LUCIFER
  - DES
  - LOKI
  - FEAL

Barajeando los datos de entrada



Repitiendo





TECNOLÓGICO DE MONTERREY®

Comentarios

- 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 Fiestel más fuerte

Primer estándar de cifrado simétrico: DES

- Data Encryption Standard
- 15 mayo 1973: NBS (National Bureau of Standards) publica convocatoria para algoritmos criptográficos
- No recibe nada hasta 6 agosto 1974
  - IBM somete algoritmo de desarrollo interno: LUCIFER
- NBA evalua algoritmo junto con la NSA (National Security Agency, USA)
- 15 julio 1977 NBS adopta una modificación de LUCIFER
  - FIPS PUB 46
  - La llave de 128 bits de LUCIFER se modifico a 56 en DES
  - Diseño de las cajas S

TECNOLÓGICO DE MONTERREY®

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
- Basado en el método de Feistel
- En 1981 ANSI adopto el DES con el nombre de Data Encryption Algorithm
  - No exige chip y puede ser programado

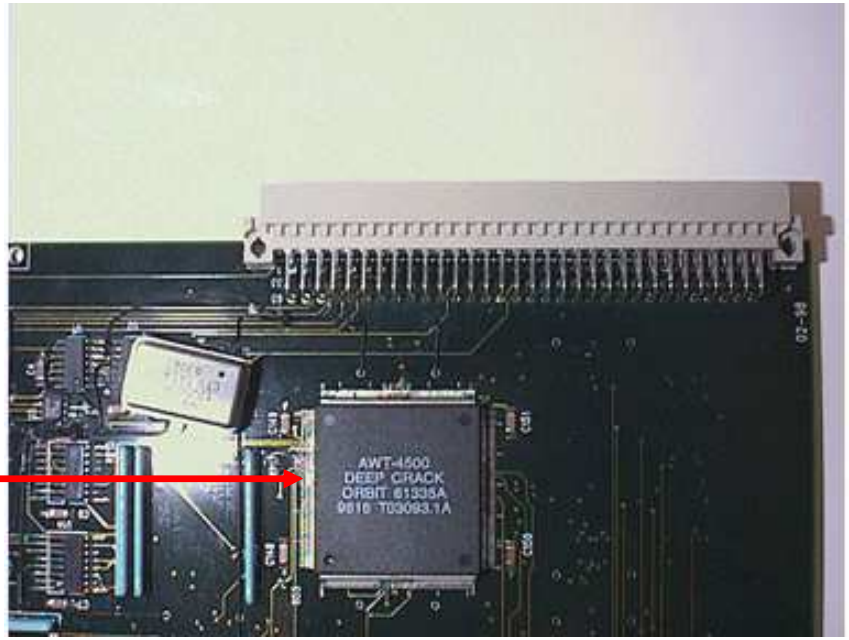
TECNOLÓGICO DE MONTERREY®

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

Imagenes de la máquina

27 tarjetas



1800 chips con 24 unidades de busqueda

TECNOLÓGICO DE MONTERREY®

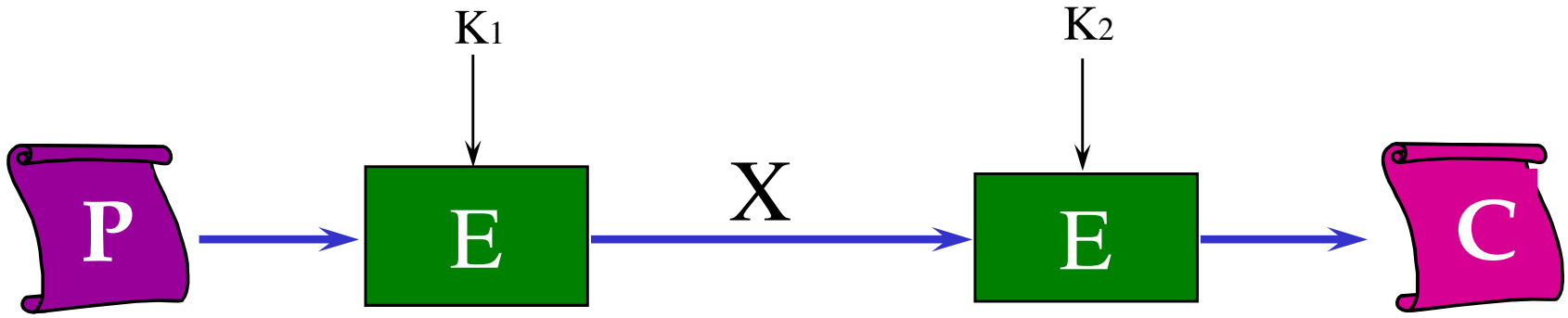
Mejoras a DES

- Debido a las vulnerabilidades que presenta DES contra ataques de fuerza bruta, se han buscado alternativas.

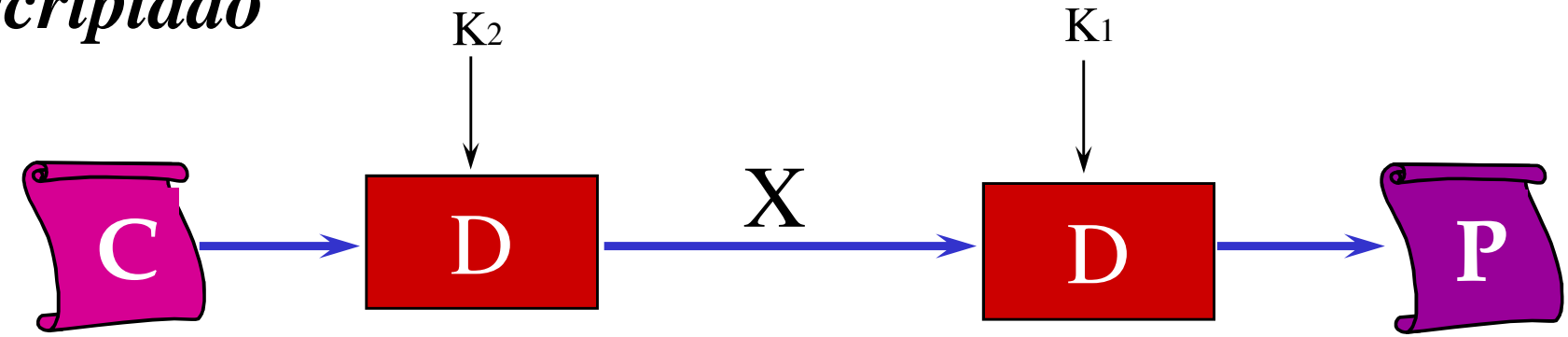
- Una de esta es realizar un múltiple encriptado con DES usando más de una llave.

Doble DES

Encriptado



Decriptado



TECNOLÓGICO DE MONTERREY®

¿Es suficiente?

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

```
C = E(k2,E(k1,P))
P = D(k1,D(k2,C))
```

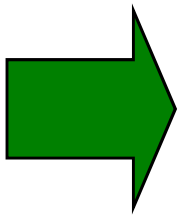
- Si se conoce P y C es posible un ataque de fuerza bruta con todos los pares de llaves k1 y k2
  - cada llave es de 56 bits, entonces se tiene que intentar 2^{112} pares de llaves, lo cual hace el ataque muy ineficiente

TECNOLÓGICO DE MONTERREY®

Atacando doble DES

- Re-escribiendo la ecuación

```
C = E(k2,E(k1,P))
P = D(k1,D(k2,C))
```

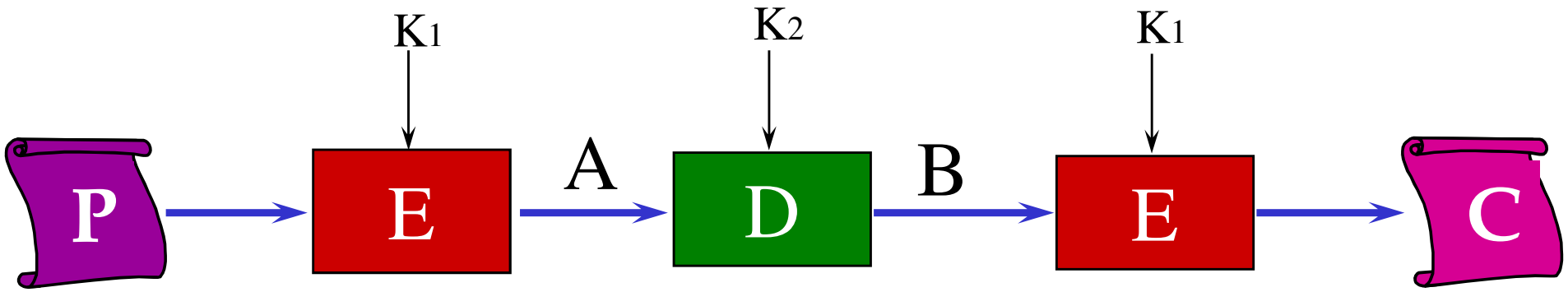


```
M = E(k1,P)
M = D(k2,C)
```

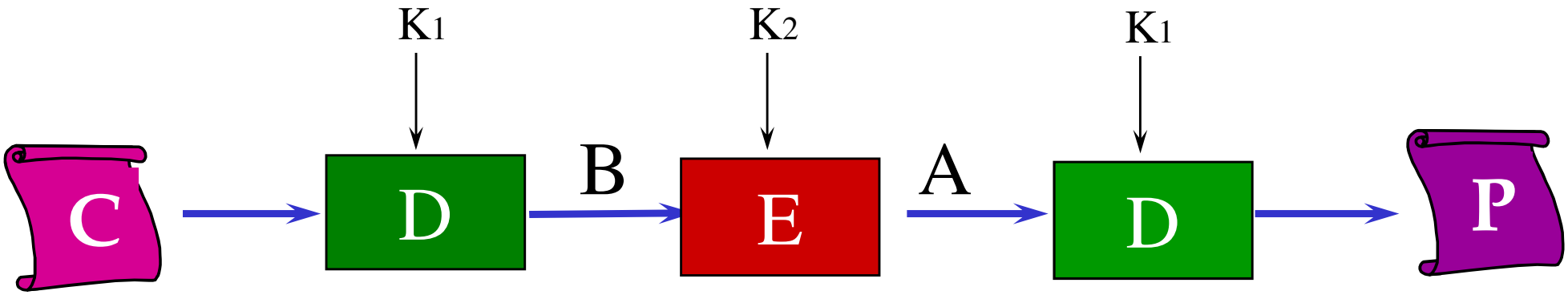
- Se intenta un número grande de decripciones con varios valores de k2 y se almacenan los resultados en una tabla
- Después se empieza con E(k1,P) encripciones, checando cada resultado con lo almacenado en la tabla.
- Con suficiente espacio: rompe DES con trabajo de 2^{57}
- Requerimientos memoria prohibitivos
  - trabajo investigación para disminuir estos requerimientos

Triple DES

Encriptado



Decriptado



TECNOLÓGICO DE MONTERREY®

Hacia un nuevo estándar: AES

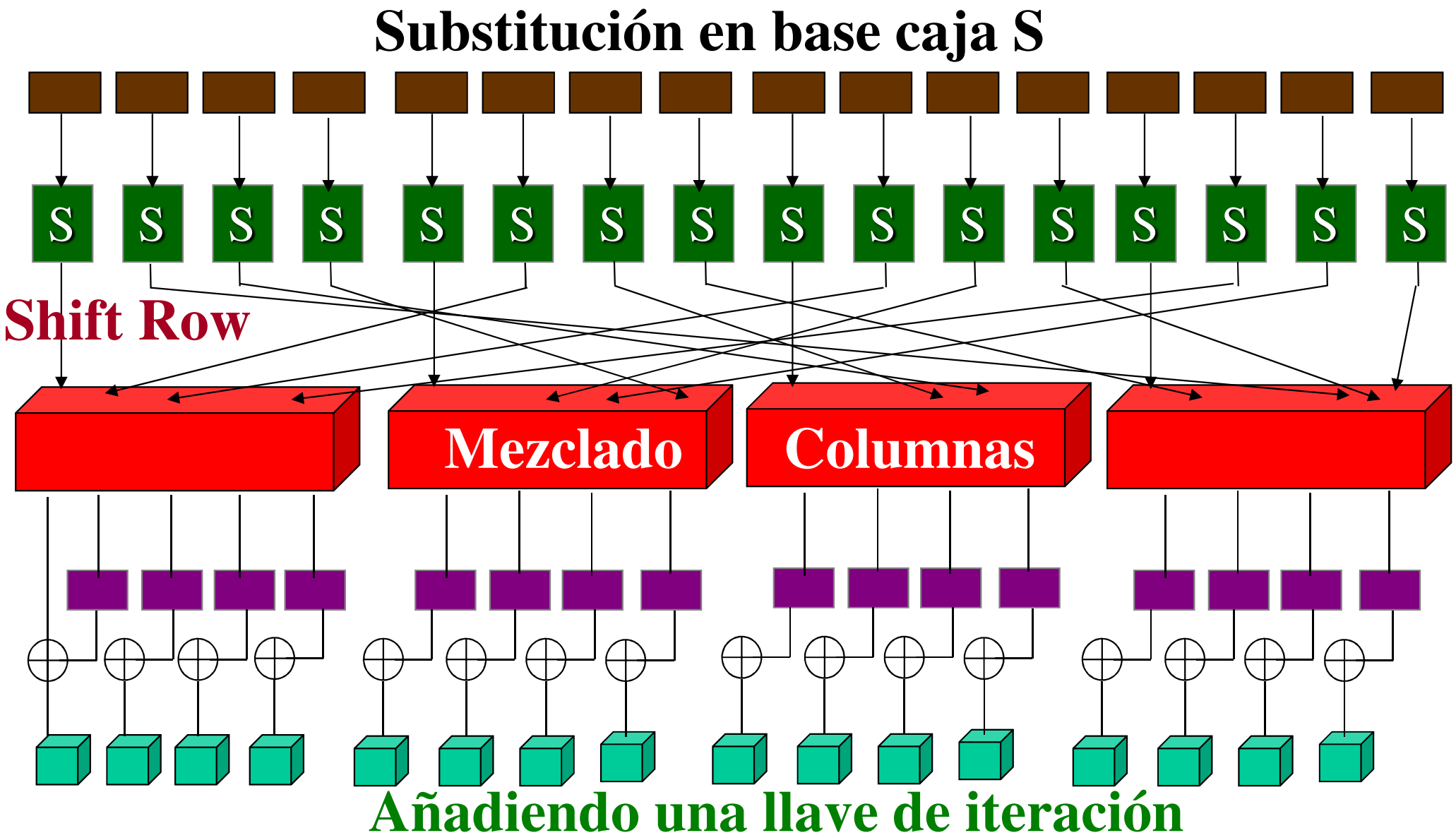
- En 1997 la NIST anuncia el substituto de DES: AES (Advanced Encryption Standard)
- Referencia: http://csrc.nist.gov/encryption/aes/
- Candidatos (al 20-abril- 2000):
  - MARS (IBM)
  - RC6 (Laboratorios RSA)
  - **Rijndael (J. Daemen y V. Rijmen) !!!! (2.10.2000)**
  - Serpent (R. Anderson, E.Biham,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

TECNOLÓGICO DE MONTERREY®

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 192 y 256 bits
  - bloque 128 bits no es consideredo suficientemente fuerte.
- No usa otros componentes criptograficos.
- No tiene partes obscuras y cosas dificiles de entender entre operaciones aritméticas.
- No deja espacio suficiente para esconder un trapdoor.
- Modo encripción en bloque ECB.

Funcionamiento Rijndael



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

TECNOLÓGICO DE MONTERREY®

Características algoritmos encripción 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

TECNOLÓGICO DE MONTERREY®

Características algoritmos encripción 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

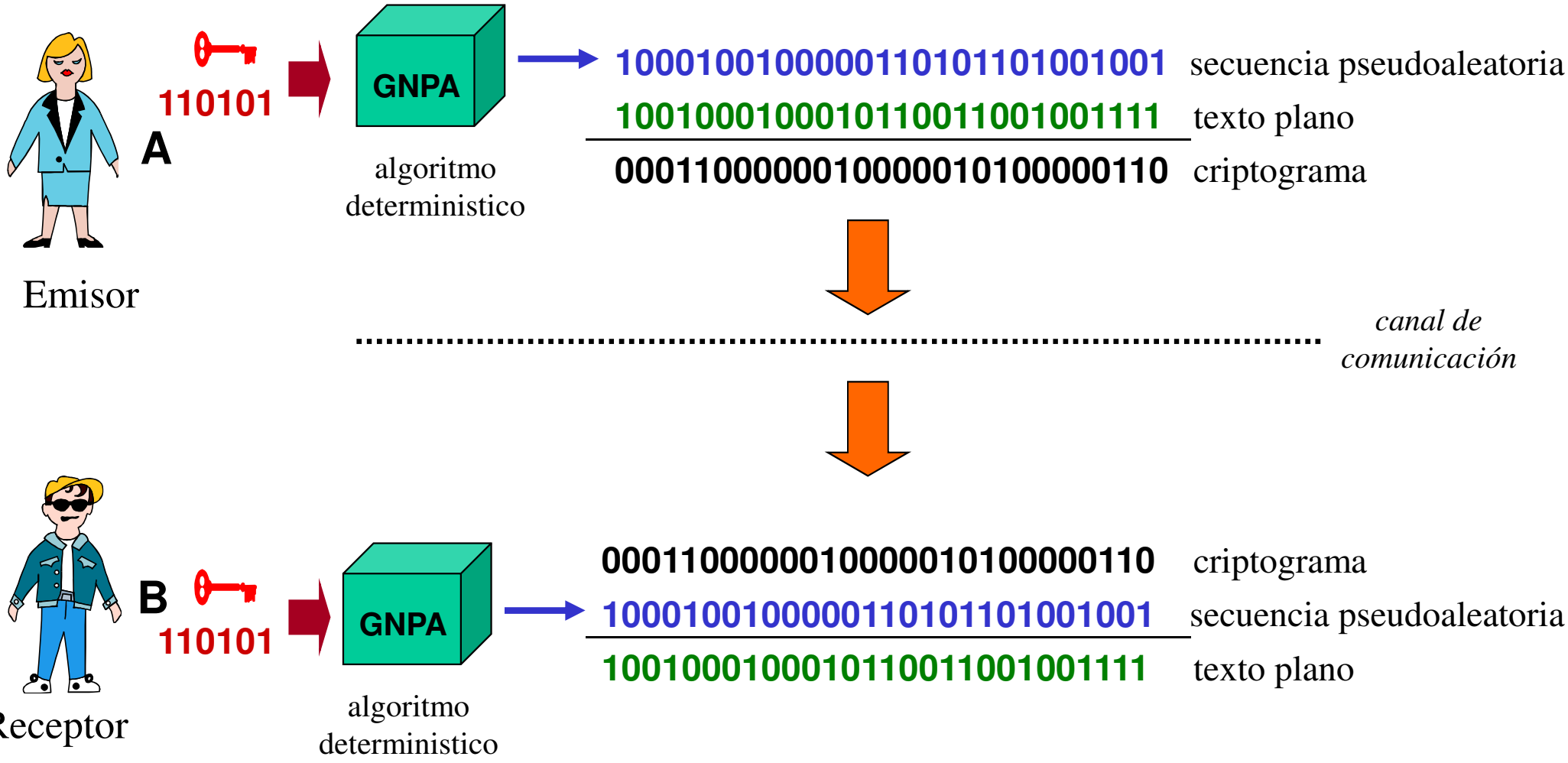
TECNOLÓGICO DE MONTERREY®

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 simetrico
- La secuencia se suma módulo 2 con el texto claro (emisión) o con el criptograma (recepción)
- Es rápido y simple

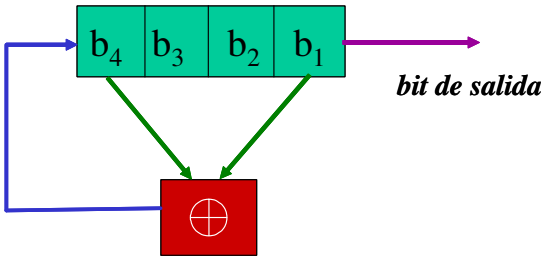
Ejemplo envío/recepción

Mensaje a enviar: HOLA
HOLA = 1001000100010110011001001111



Implementación

- A nivel hardware
  - Feedback Shift Registers
  - Proyecto eSTREAM
- A nivel software
  - Modos cifrado en flujo
  - Proyecto eSTREAM



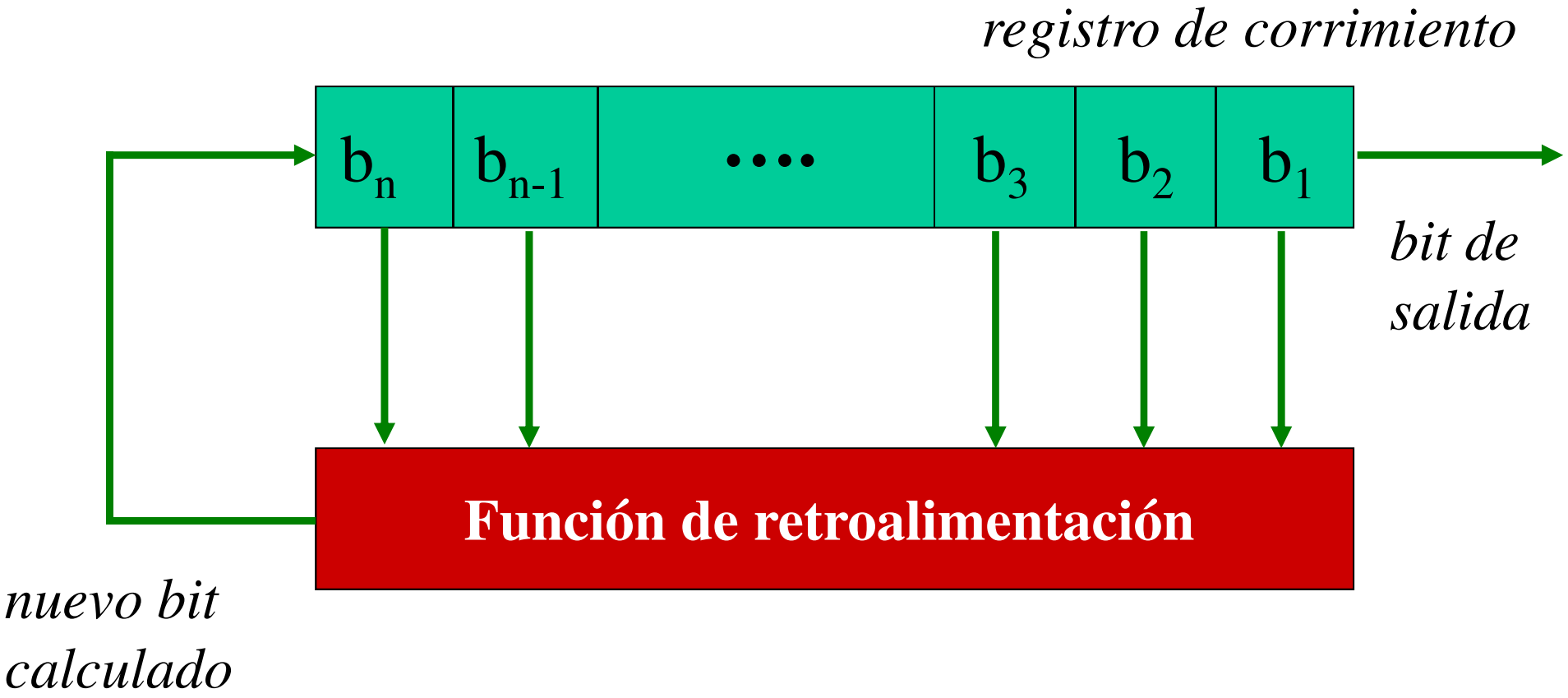
1111	1001
0111	1001
1011	0100
0101	0010
1010	0001
1101	1000
0110	1100
0011	1110

TECNOLÓGICO DE MONTERREY®

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



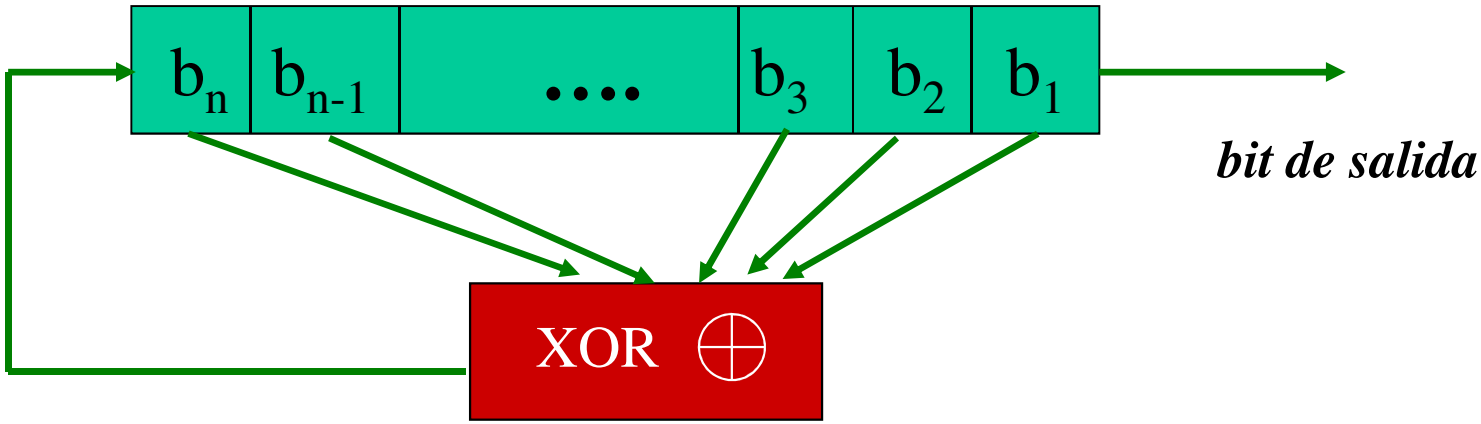
TECNOLÓGICO DE MONTERREY®

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

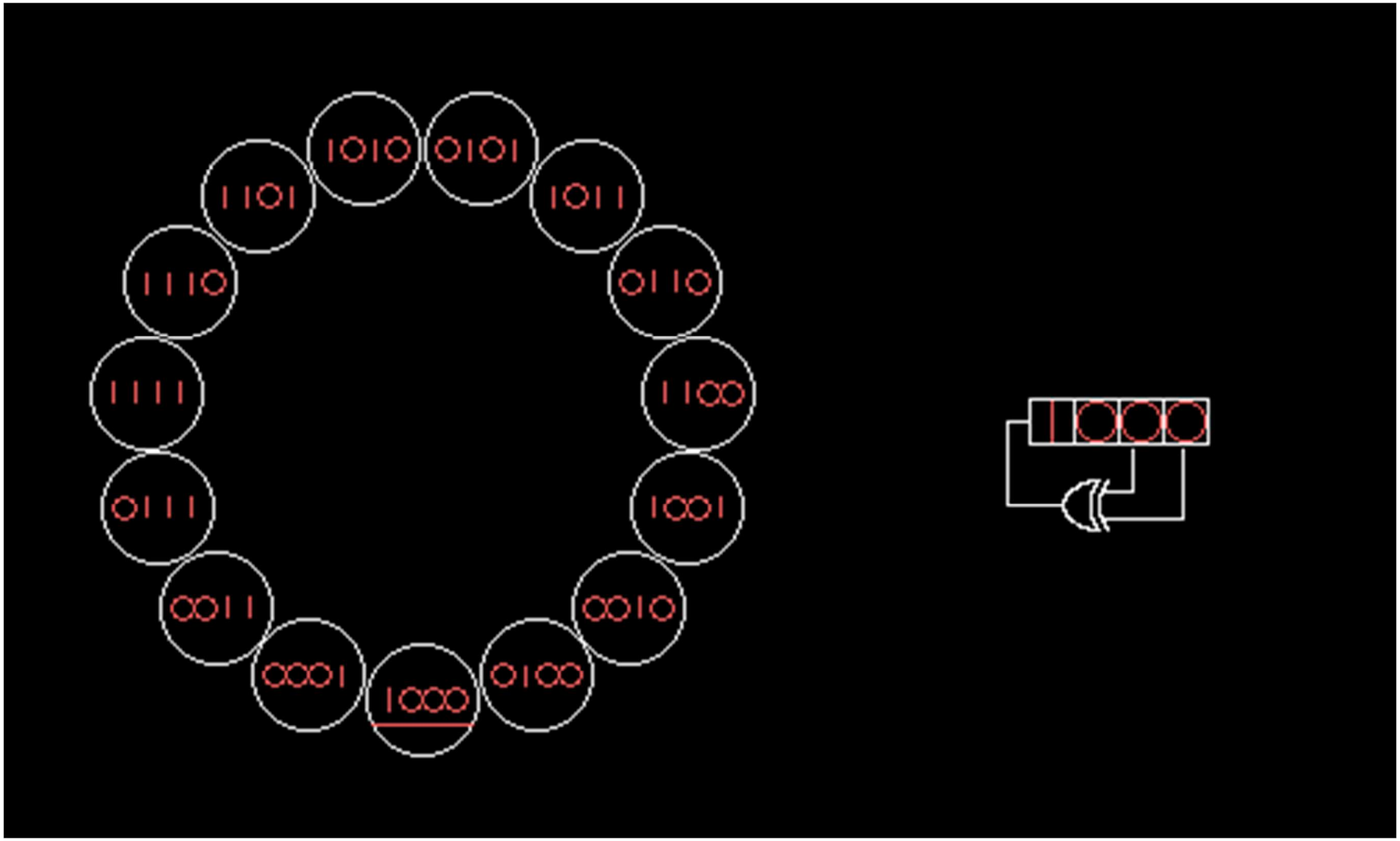
Registros de desplazamientos realimentados linealmente

- 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 denomida tap register (secuencia de entrada)



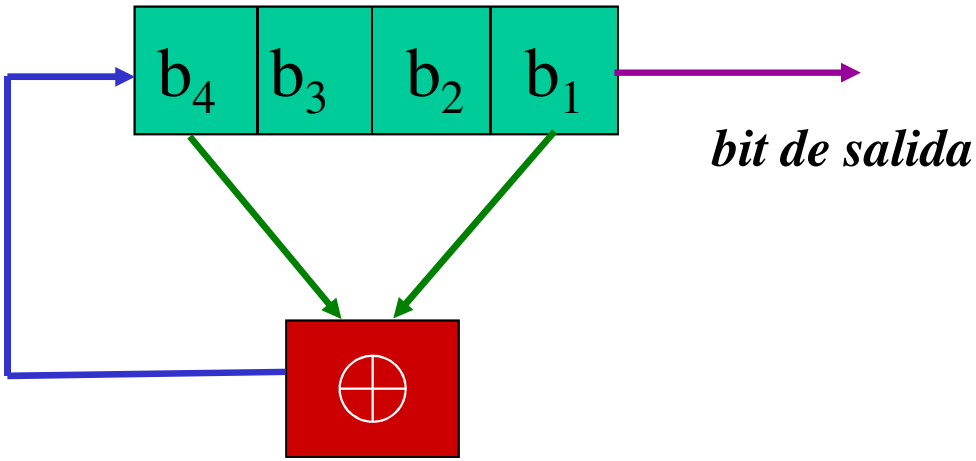
TECNOLÓGICO DE MONTERREY®

Un primer ejemplo



Ejemplo LSFR

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



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

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

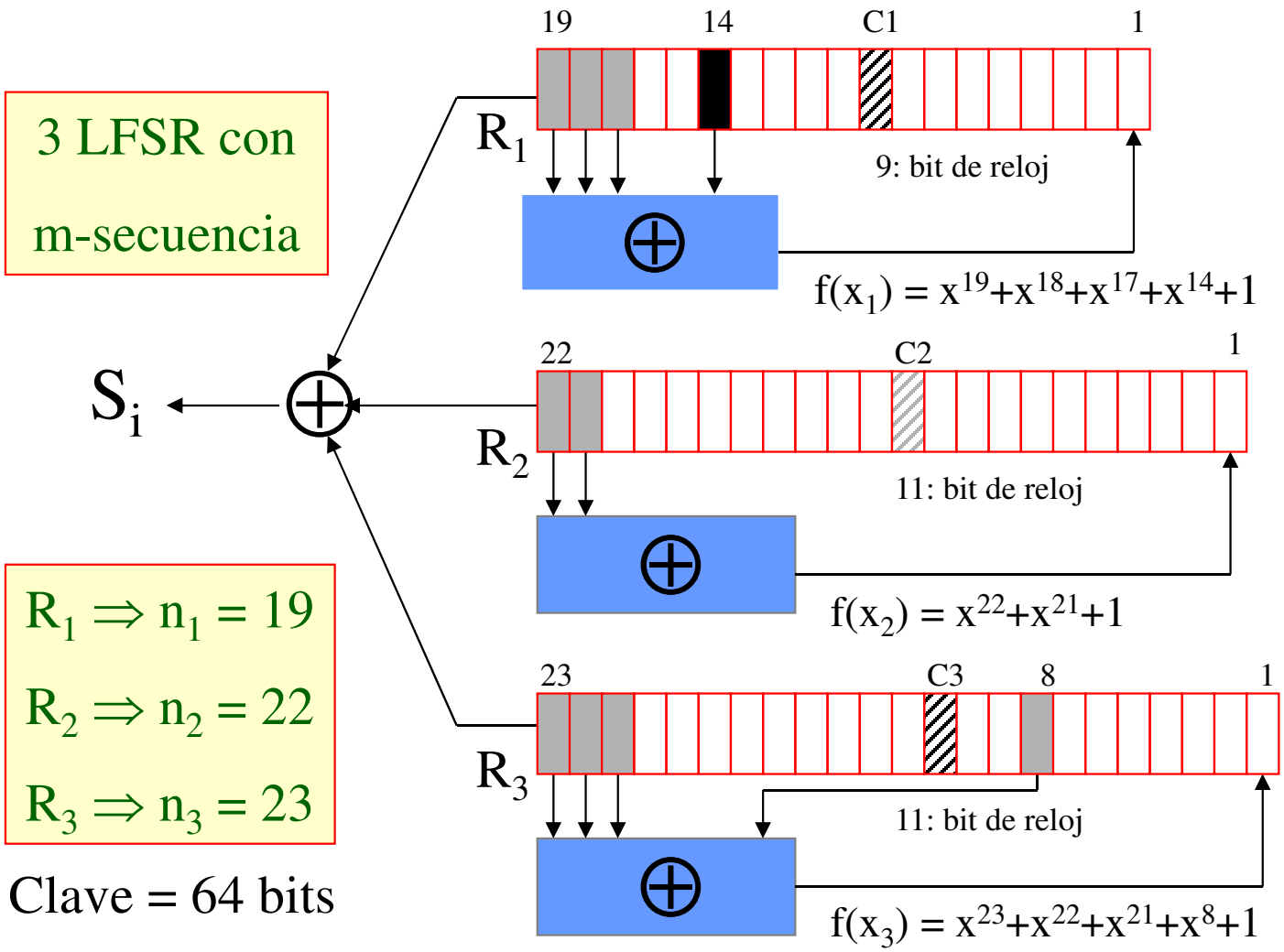
TECNOLÓGICO DE MONTERREY®

Polinomios primitivos

- Ejemplo polinomio primitivo para cada valor de m en rango de m (2,3…,128)
- Existen 68,273,666 diferentes polinomios primitivos de grado 31 (m=31)

(0,1,2)	(0,1,3,4,24)	(0,1,46)	(0,1,5,7,68)	(0,2,3,5,90)	(0,3,4,5,112)
(0,1,3)	(0,3,25)	(0,5,47)	(0,2,5,6,69)	(0,1,5,8,91)	(0,2,3,5,113)
(0,1,4)	(0,1,3,4,26)	(0,2,3,5,48)	(0,1,3,5,70)	(0,2,5,6,92)	(0,2,3,5,114)
(0,2,5)	(0,1,2,5,27)	(0,4,5,6,49)	(0,1,3,5,71)	(0,2,93)	(0,5,7,8,115)
(0,1,6)	(0,1,28)	(0,2,3,4,50)	(0,3,9,10,72)	(0,1,5,6,94)	(0,1,2,4,116)
(0,1,7)	(0,2,29)	(0,1,3,6,51)	(0,2,3,4,73)	(0,11,95)	(0,1,2,5,117)
(0,1,3,4,8)	(0,1,30)	(0,3,52)	(0,1,2,6,74)	(0,6,9,10,96)	(0,2,5,6,118)
(0,1,9)	(0,3,31)	(0,1,2,6,53)	(0,1,3,6,75)	(0,6,97)	(0,8,119)
(0,3,10)	(0,2,3,7,32)	(0,3,6,8,54)	(0,2,4,5,76)	(0,3,4,7,98)	(0,1,3,4,120)
(0,2,11)	(0,1,3,6,33)	(0,1,2,6,55)	(0,2,5,6,77)	(0,1,3,6,99)	(0,1,5,8,121)
(0,3,12)	(0,1,3,4,34)	(0,2,4,7,56)	(0,1,2,7,78)	(0,2,5,6,100)	(0,1,2,6,122)
(0,1,3,4,13)	(0,2,35)	(0,4,57)	(0,2,3,4,79)	(0,1,6,7,101)	(0,2,123)
(0,5,14)	(0,2,4,5,36)	(0,1,5,6,58)	(0,2,4,9,80)	(0,3,5,6,102)	(0,37,124)
(0,1,15)	(0,1,4,6,37)	(0,2,4,7,59)	(0,4,81)	(0,9,103)	(0,5,6,7,125)
(0,1,3,5,16)	(0,1,5,6,38)	(0,1,60)	(0,4,6,9,82)	(0,1,3,4,104)	(0,2,4,7,126)
(0,3,17)	(0,4,39)	(0,1,2,5,61)	(0,2,4,7,83)	(0,4,105)	(0,1,127)
(0,3,18)	(0,3,4,5,40)	(0,3,5,6,62)	(0,5,84)	(0,1,5,6,106)	(0,1,2,7,128)
(0,1,2,5,19)	(0,3,41)	(0,1,63)	(0,1,2,8,85)	(0,4,7,9,107)	
(0,3,20)	(0,1,2,5,42)	(0,1,3,4,64)	(0,2,5,6,86)	(0,1,4,6,108)	
(0,2,21)	(0,3,4,6,43)	(0,1,3,4,65)	(0,1,5,7,87)	(0,2,4,5,109)	
(0,1,22)	(0,5,44)	(0,3,66)	(0,8,9,11,88)	(0,1,4,6,110)	
(0,5,23)	(0,1,3,4,45)	(0,1,2,5,67)	(0,3,5,6,89)	(0,2,4,7,111)	

Ejemplo encripción flujo: A5/1



Una función mayoría entre C1, C2 y C3 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.

Generador de Congruencia Lineal

$x_{i+1} = (a*x_i \pm b)(\text{mod } n)$ secuencia cifrante

Sea:
$a = 5 \quad b = 1$
$n = 16 \quad x_0 = 10$

$x_{i+1} = (a*x_i \pm b)(\text{mod } n)$

Pero...

$S_i = 10, 3, 0, 1, 6, 15, 12, 13, 2, 11, 8, 9, 14, 7, 4, 5$

$x_1 = (5*10+1) \text{ mod } 16 = 3$ $\quad x_2 = (5*3+1) \text{ mod } 16 = 0$
$x_3 = (5*0+1) \text{ mod } 16 = 1$ $\quad x_4 = (5*1+1) \text{ mod } 16 = 6$
$x_5 = (5*6+1) \text{ mod } 16 = 15$ $\quad x_6 = (5*15+1) \text{ mod } 16 = 12$
$x_7 = (5*12+1) \text{ mod } 16 = 13$ $\quad x_8 = (5*13+1) \text{ mod } 16 = 2$
$x_9 = (5*2+1) \text{ mod } 16 = 11$ $\quad x_{10} = (5*11+1) \text{ mod } 16 = 8$
$x_{11} = (5*8+1) \text{ mod } 16 = 9$ $\quad x_{12} = (5*9+1) \text{ mod } 16 = 14$
$x_{13} = (5*14+1) \text{ mod } 16 = 7$ $\quad x_{14} = (5*7+1) \text{ mod } 16 = 4$
$x_{15} = (5*4+1) \text{ mod } 16 = 5$ $\quad x_{16} = (5*5+1) \text{ mod } 16 = 10$

Casos especiales

$$x_{i+1} = (a*x_i \pm b)(\text{mod } n)$$

¿Qué sucede si
a = 11 b = 1
n = 16 x_0 = 7?

¿Qué sucede si
a = 5 b = 2
n = 16 x_0 = 10?

¿Qué sucede si
a = 5 b = 2
n = 16 x_0 = 1?

¿Qué sucede si
a = 4 b = 1
n = 16 x_0 = 10?

TECNOLÓGICO DE MONTERREY®

Erase una vez…. RC4

- Criptosistema de llave de tamaño variable desarrollado en 1987 por Ron Rivest para la RSA.
  - Rivest Cipher 4
  - También conocido como ARCFOUR o ARC4
- Durante siete años su implementación fue privada.
- En septiembre 1994, alguien lo puso en la lista de correo Cypherpunks anónimamente.
- Varios ataque lo hacen no recomendable
  - Adrew Ross en 1995 descubre vulnerabilidad empírica
  - Klein en 2005
  - Ataque PTW en 2007 (base de aircrack)
  - Ataque de RC4 en TLS: 2013

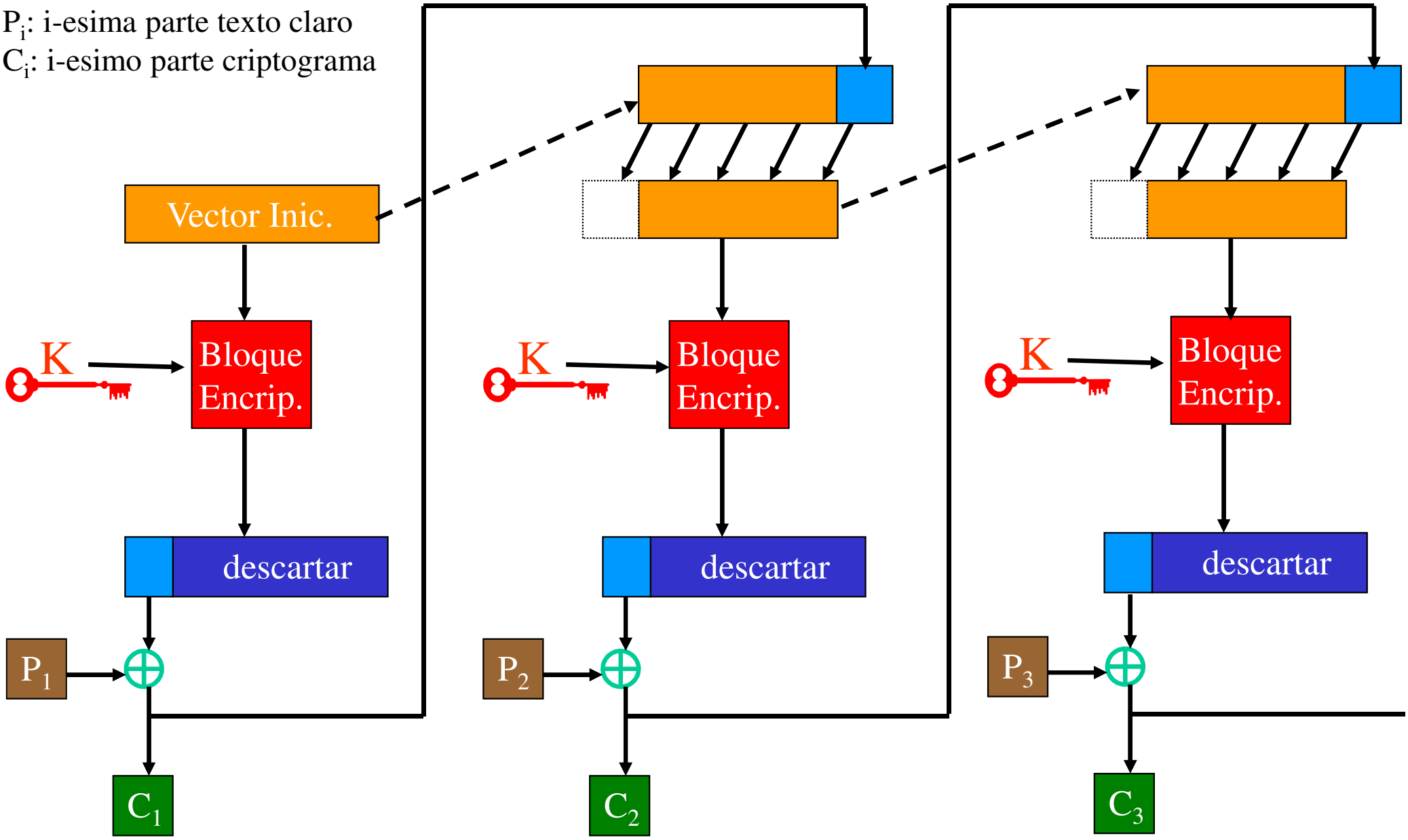
TECNOLÓGICO DE MONTERREY®

Modos de cifrado de flujo

- CFB: Cipher Feedback Block
  - De block cipher a self-synchronizing stream cipher.
- OFB: Output Feedback
  - De block cipher a synchronous stream cipher
- CTR: Counter
  - De block cipher a stream cipher
  - También conocido como:
    - ICM: Integer Counter Mode
    - SIC: Segmented Integer Counter

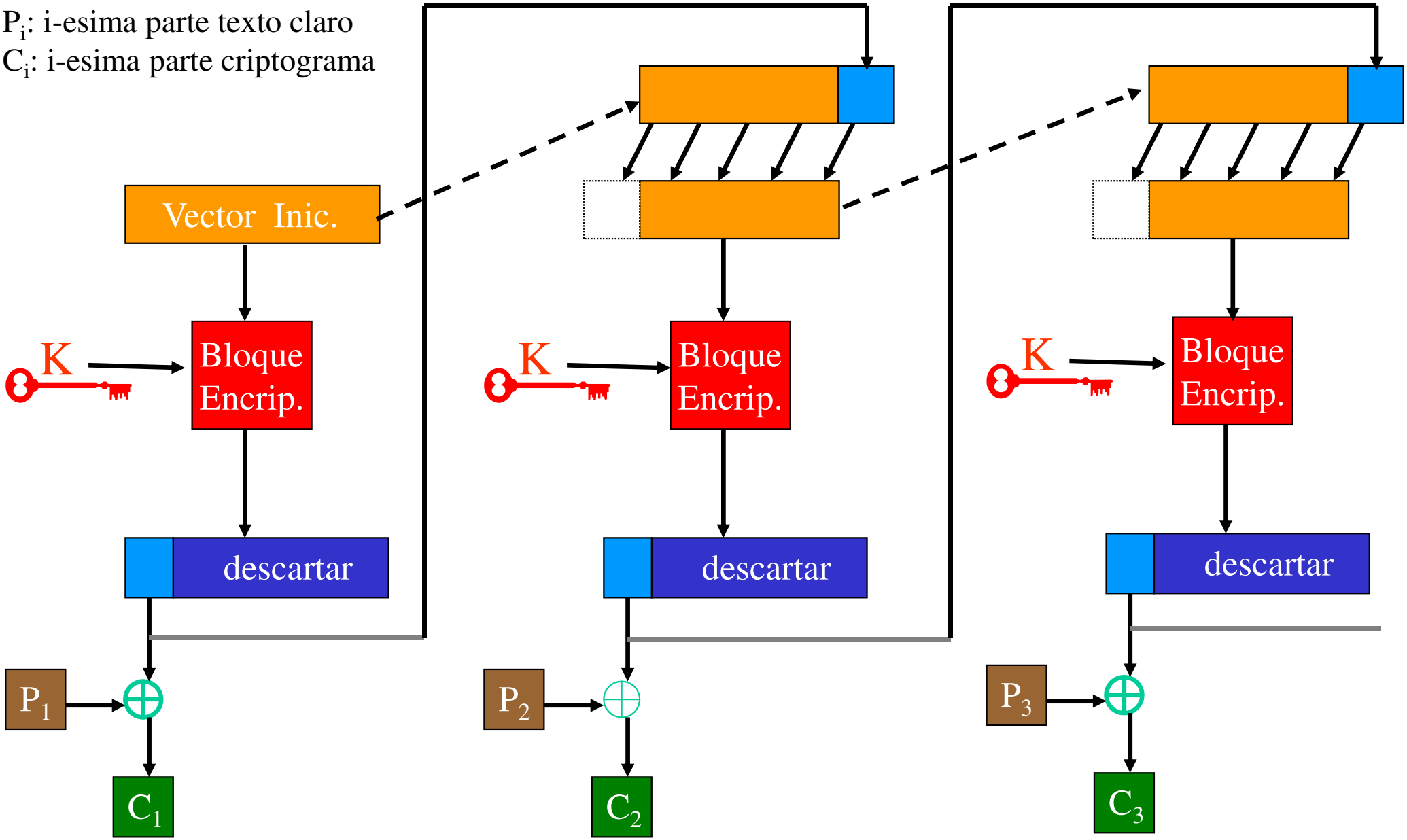
Encripción en modo CFB

P_i: i-esima parte texto claro
C_i: i-esimo parte criptograma

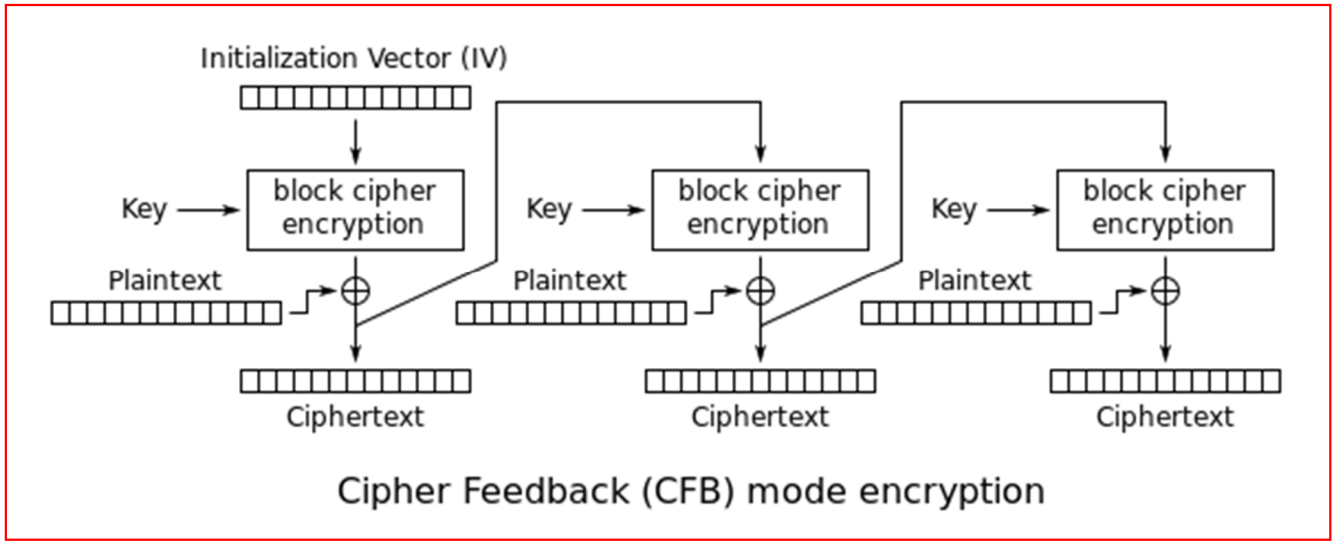


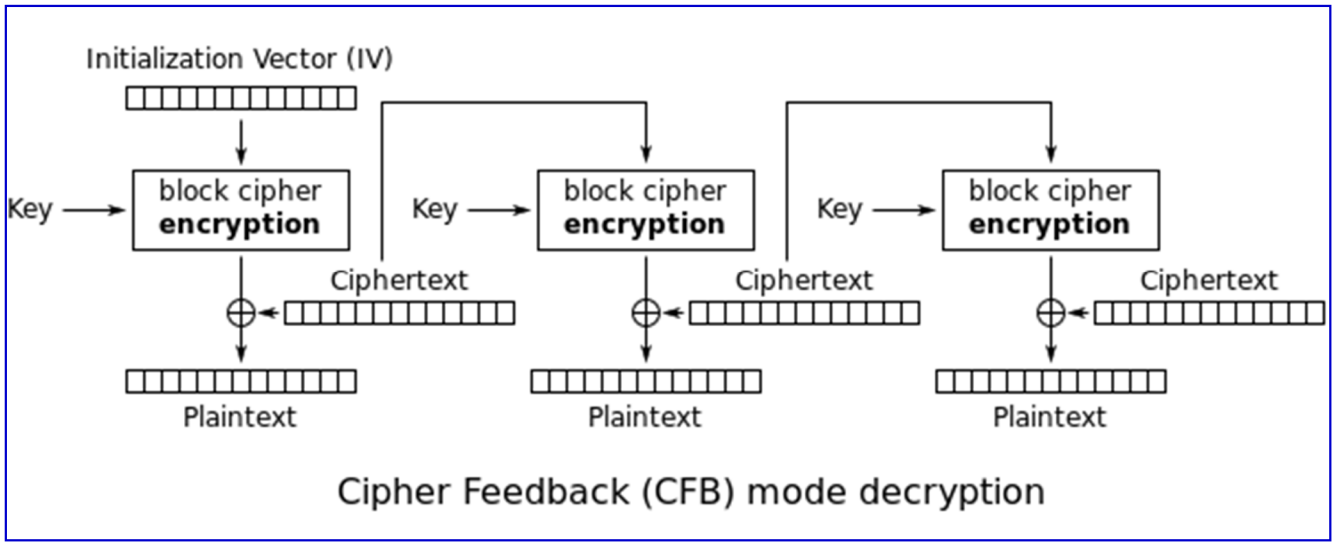
Encripción en modo OFB

P_i: i-esima parte texto claro
C_i: i-esima parte criptograma



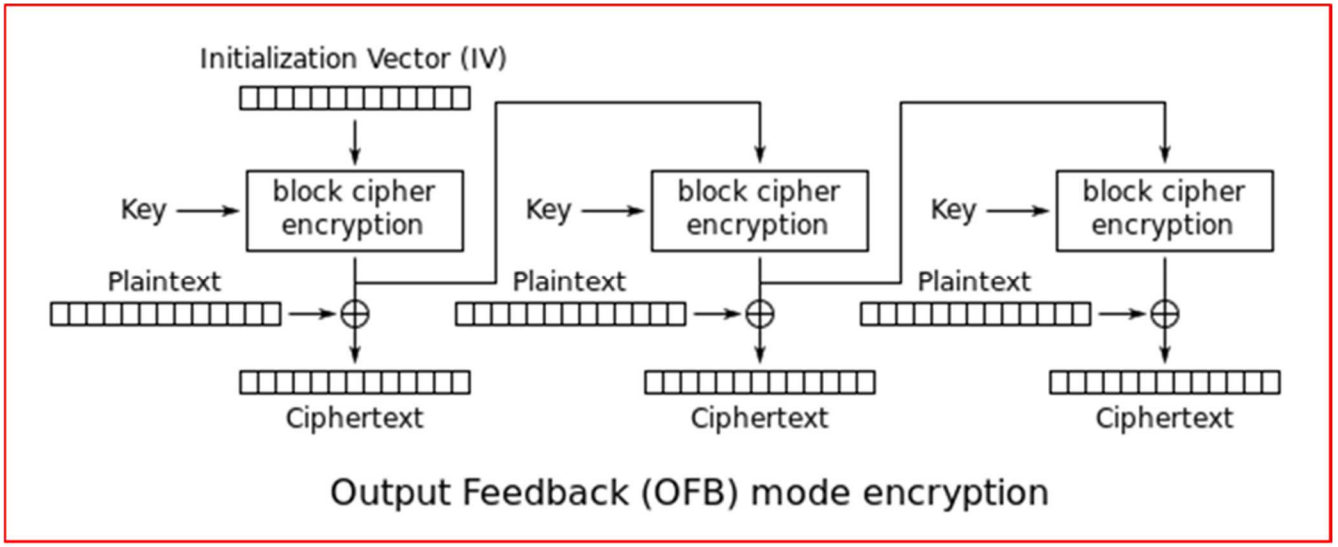
Cipher Feedback Block

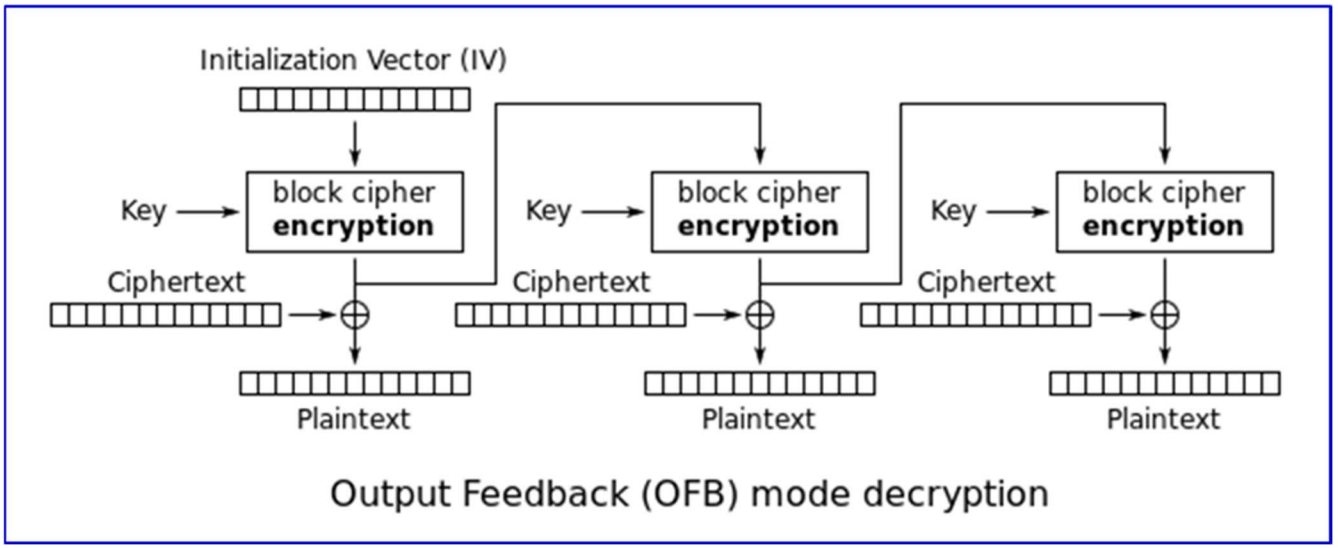




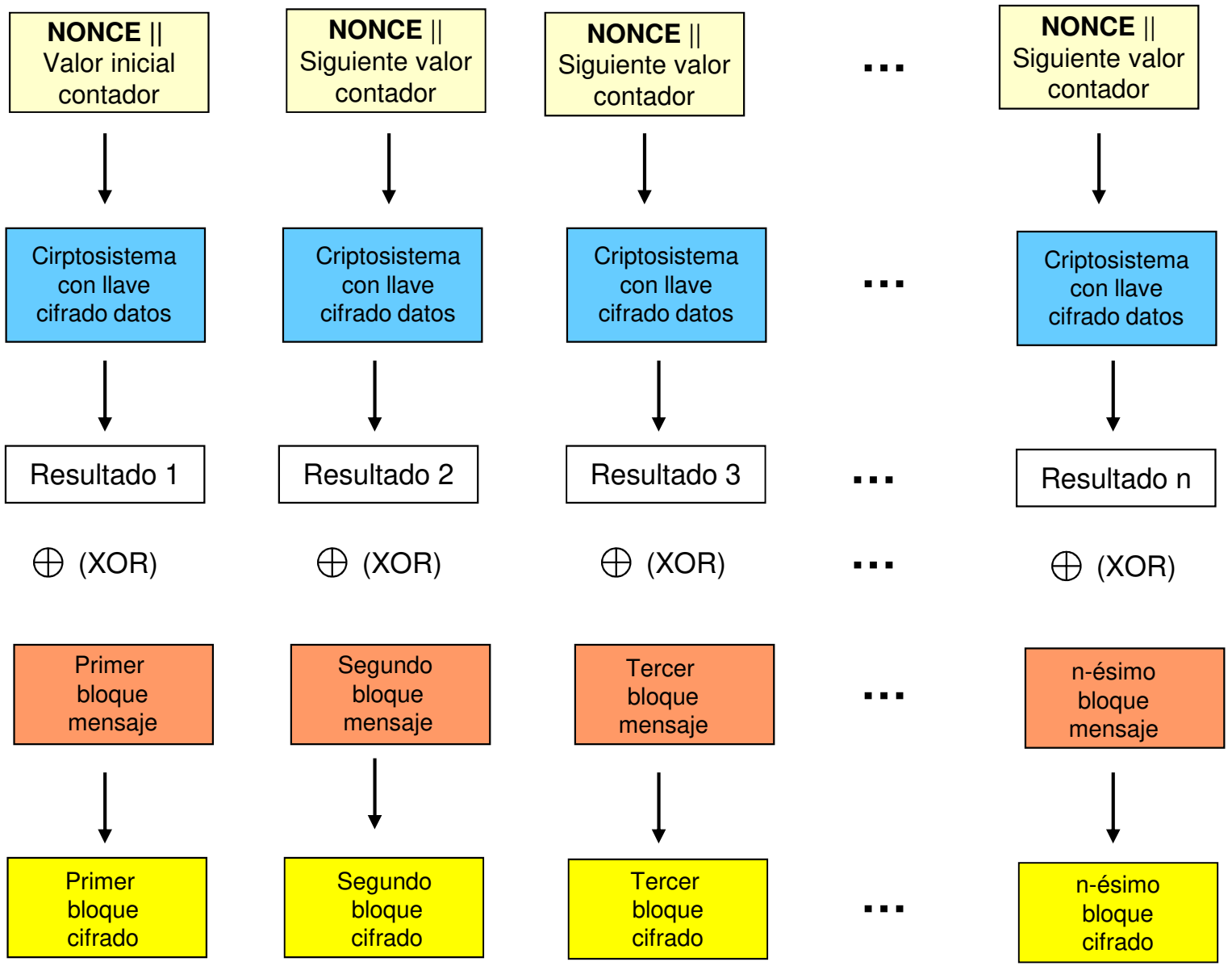
TECNOLÓGICO DE MONTERREY®

Output feedback mode



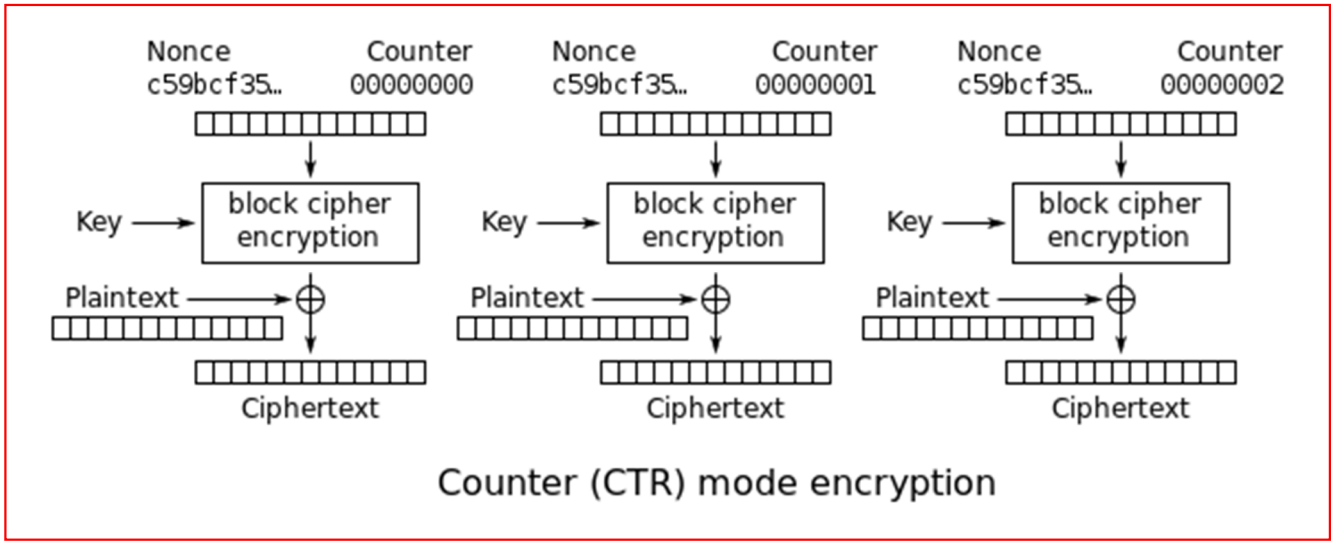


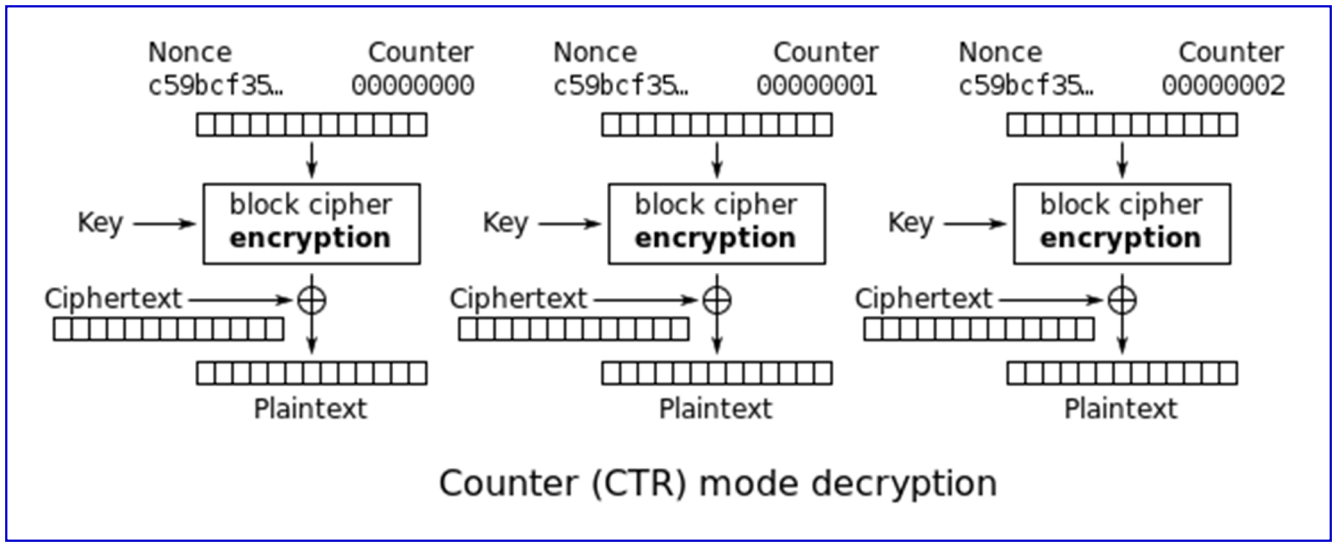
Ejemplo encripción modo CTR



TECNOLÓGICO DE MONTERREY®

Counter mode





TECNOLÓGICO DE MONTERREY®

Proyecto eSTREAM

- Organizado por ECRYPT
  - European Network of Excellence un Cryptology
- Proyecto lanzado en workshop SASC en 2004
  - State of the Art Stream Ciphers
- Proyecto termina 2008, no son un estándar
- Actualización 2009

Perfil 1 – Software	Perfil 2 – Hardware
HC – 128	Grain v1
Rabbit	MICKEY v2
Salsa20/12	Trivium
Sosemanuk	

TECNOLÓGICO DE MONTERREY®

Resumen modos de cifrado

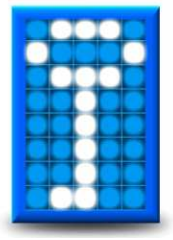
Objetivo cifrado	Modos de cifrado
Cifrado bloque	ECB: Electronic Code Book
	CBC: Cipher Block Chaining
Cifrado flujo	CTR: Counter
	OFB: Output Feedback Block
	CFB: Cipher Feedback Block
Cifrado disco	XEX: Xor-encrypt-xor
	XTS: XEX-based tweaked-codebook mode with ciphertext stealing (soportado por BestCrypt, FreeOTFE, TrueCrypt, VeraCrypt)
	LRW: Liskov, Rivest, and Wagner
Cifrado autenticado	CCM: Counter with CBC-MAC
	OCB: Offset Codebook Mode
	GCM: Galois/Counter Mode

Cifrado de disco y archivos

Métodos, opciones y herramientas

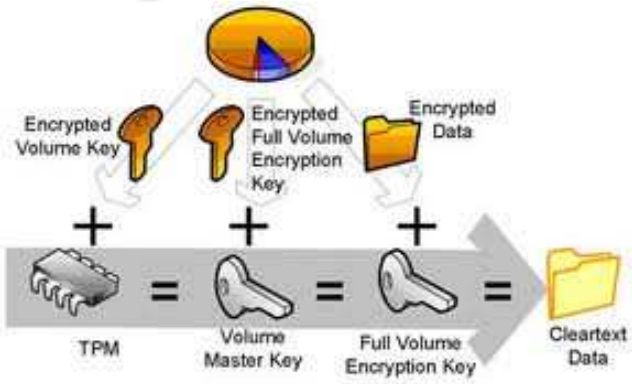
Aplicaciones criptográficas para cifrado en disco

- 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









TECNOLÓGICO DE MONTERREY®

¿Qué deseo proteger?

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

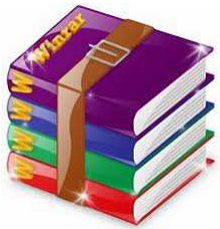
TECNOLÓGICO DE MONTERREY®

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”?

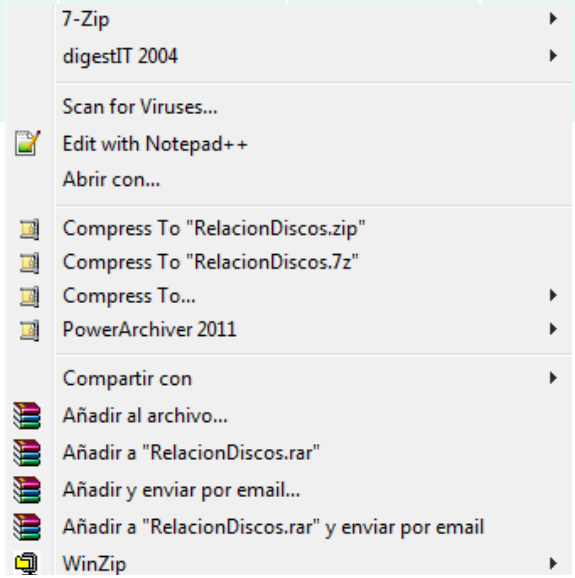
- Problema software cifrado
  - Emisor y receptor deben contar con el mismo software.
  - Posible que emisor genere un archivo autoejecutable
    - No es posible el envío por correo.
- Opción: utilizar la opción de cifrado de los programas de comprensión más utilizados en el mercado.
  - Solución simple 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.



TECNOLÓGICO DE MONTERREY®

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.

TECNOLÓGICO DE MONTERREY®

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.

Protección medios móbiles

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

Herramientas protección USB

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

TECNOLÓGICO DE MONTERREY®

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

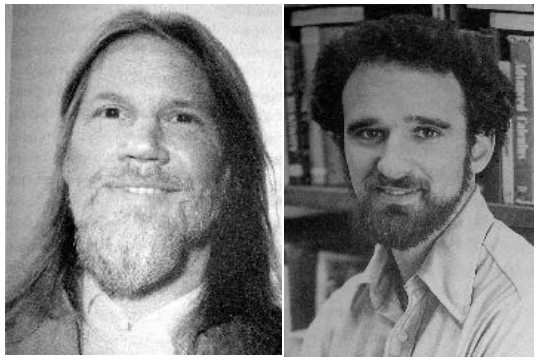
Criptosistema Diffie Hellman

Algoritmo intercambio llaves

TECNOLÓGICO DE MONTERREY®

Diffie-Hellman

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



- Basado dificultad para calcular logaritmos discretos
  - i.e. el problema del logaritmo discreto

1: Communications-Electronic Security Group

El problema del logaritmo discreto

- Dados g, x y p en la formula:

$$y = g^x \bmod p$$

  - 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 $y = 7^8 \bmod 13$ calcular y es fácil,
  - pero $3 = 7^x \bmod 13$ calcular x es muy difícil
- Conclusión:
  - es muy fácil calcular exponentes mod un primo
  - es muy pesado calcular un logaritmo discreto

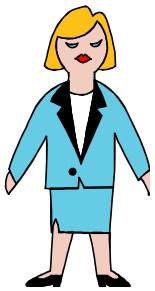
TECNOLÓGICO DE MONTERREY®

Algoritmo de Diffie-Hellman

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

Esquema Diffie Hellman

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



A

La llave de A y B es K

B

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

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

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

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

Y_A →

← Y_B

Generando llave secreta A

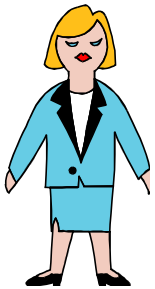
$$K = (Y_B)^{X_A} \bmod q$$

Generando llave secreta B

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

Ejemplo Diffie Hellman

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



A

La llave de A y B es 21

B

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

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

$= 45 \mod 53$

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

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

$= 12 \bmod 53$

$Y_A \; (45)$ →

← $Y_B \; (12)$

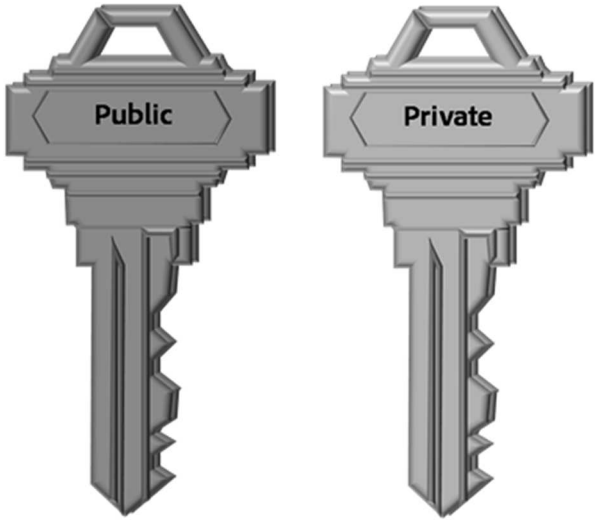
Generando llave secreta A

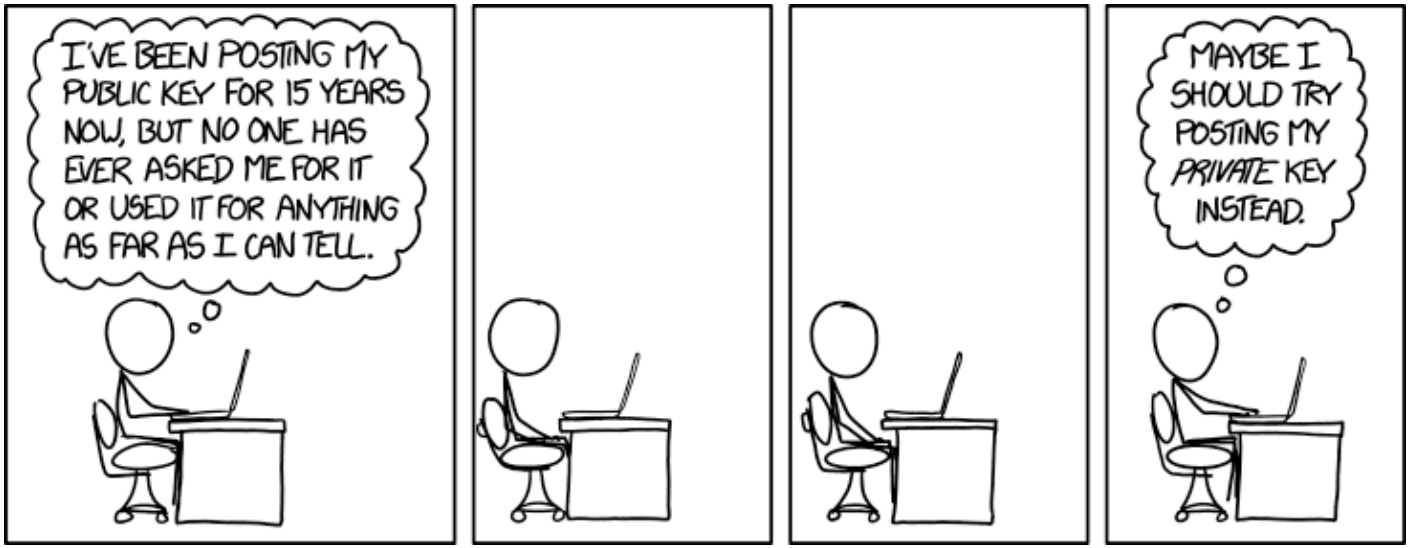
$K = 12^{29} \bmod 53 = 21 \bmod 53$

Generando llave secreta B

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

Criptosistemas de llave pública o asimétrica





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.
  - New Directions in Cryptography
- Desde 1976 varios algoritmos han sido propuestos, muchos de estos son considerados seguros, pero son imprácticos.

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

The development of computer controlled communication networks promises effortless and inexpensive contact between people or computers on opposite sides of the world, replacing most mail and many excursions with telecommunications. For many applications these contacts

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

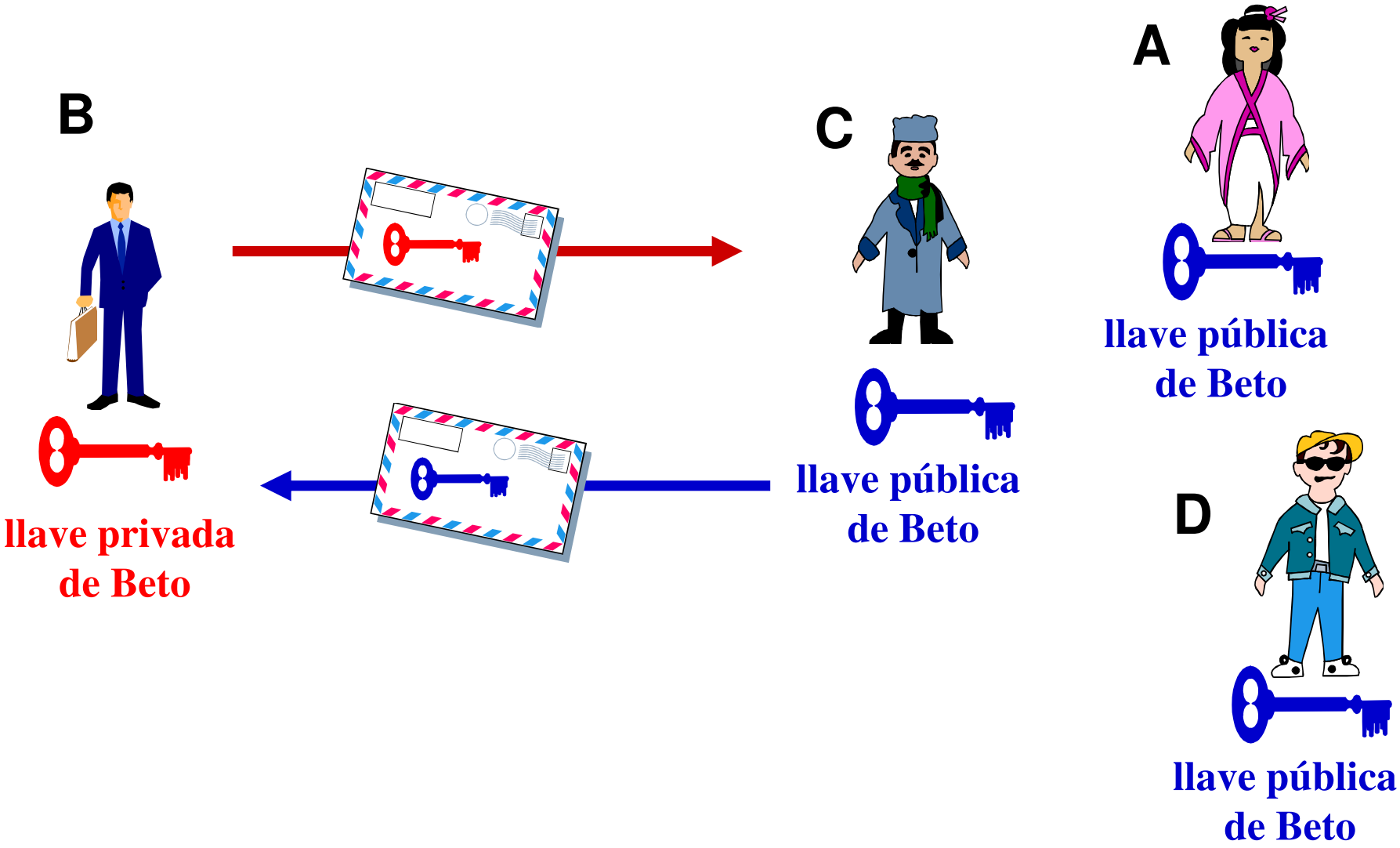
Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D. Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enciphered in such a way that only the intended receiver is able to decipher it. As such, a public key cryptosystem is a multiple access cipher. A private conversation can therefore be held between any two individuals regardless of whether they have ever communicated before. Each one

TECNOLÓGICO DE MONTERREY®

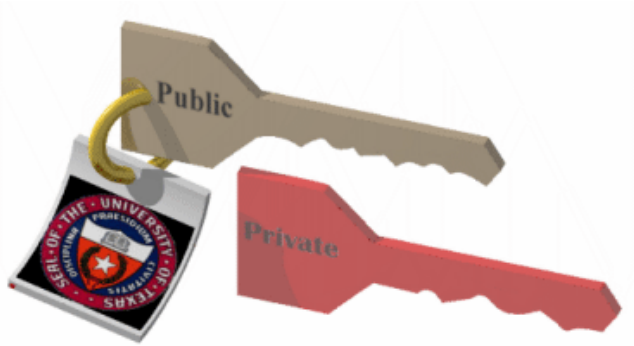
Antecedentes

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

Criptograma llave pública (asimétrico)

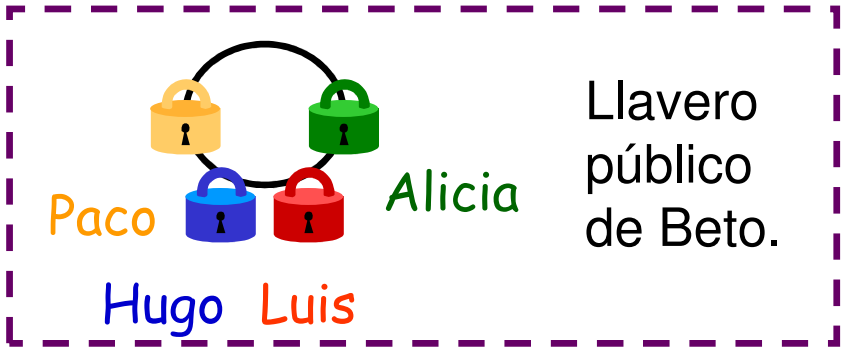


Cifrando con llave pública



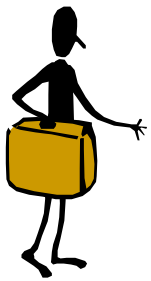
- Emisor no usa sus llaves
- Necesario contar con la llave pública del receptor
- Llaves relacionadas matemáticamente
  - Teoría de números
  - Funciones unidireccionales con puerta trasera
- Dos funciones usadas
  - Producto de números enteros, cuya inversa es la factorización del número obtenido (RSA)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

Cifrado con llave pública

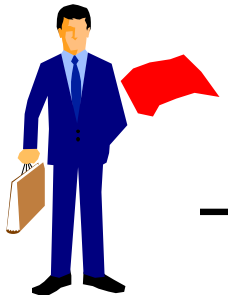


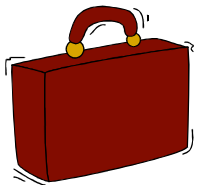
5.Hugo desasegura la caja con un su llave secreta

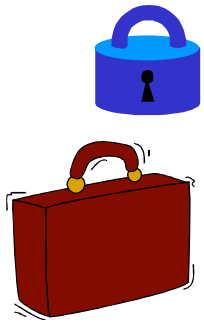
3. Beto asegura la caja con el candado de Hugo

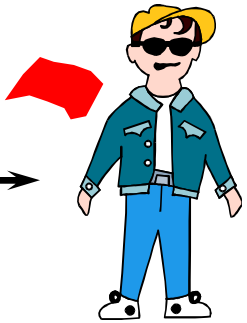


1. Beto escribe documento









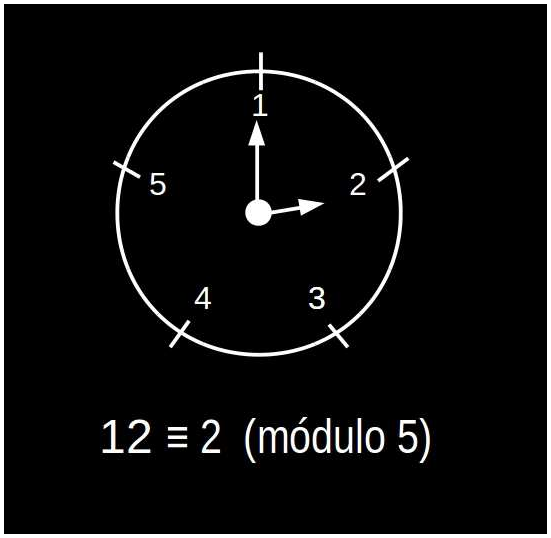
4. La caja se trans-porta hacia Hugo

2. Beto coloca el documento en la caja fuerte

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*.



TECNOLÓGICO DE MONTERREY®

Ejemplo suma modular 10

- $5 + 5 = 10 \bmod 10 = 0$
- $3 + 9 = 12 \bmod 10 = 2$
- $2 + 2 = 4 \bmod 10 = 4$
- $9 + 9 = 18 \bmod 10 = 8$

TECNOLÓGICO DE MONTERREY®

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

TECNOLÓGICO DE MONTERREY®

Encripción usando suma modular

- Suma modulo 10 puede usarse como esquema de encripción de dígitos.
- Encripción:

  digito + <constante> mod 10
- Se mapea cada dígito decimal a uno diferente de tal forma que es reversible.
- La constante es la llave secreta
- Decripción:

  digito - <constante> mod 10

  si el resultado es menor a cero => sumar 10

TECNOLÓGICO DE MONTERREY®

Ejemplo encripción suma modular

- Llave secreta: 5
- Encripción:

  $7 + 5 = 12 \bmod 10 = 2$

  $8 + 5 = 13 \bmod 10 = 3$

  $3 + 5 = \ \ 8 \bmod 10 = 8$

- Decripción:

  $2 - 5 = -3 + 10 = 7$

  $3 - 5 = -2 + 10 = 8$

  $8 - 5 = \ \ 3$

TECNOLÓGICO DE MONTERREY®

Cifrado 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 mod 10 = 0
- Si la llave pública es 4:
  - Para cifrar se añade 4 mod 10
  - Para descifrar se añade 6 mod 10

Ejemplo cifrado inversa aditiva

- Llave pública: 4
- Encripción:

  $7 + 4 \bmod 10 = 11 \bmod 10 = 1$

  $8 + 4 \bmod 10 = 12 \bmod 10 = 2$

  $3 + 4 \bmod 10 = 7 \bmod 10 = 7$

- 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 encripción: 4

Llave decripción: 6

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

TECNOLÓGICO DE MONTERREY®

Cifrado con multiplicación modular

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

TECNOLÓGICO DE MONTERREY®

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

TECNOLÓGICO DE MONTERREY®

¿Cómo decriptar?

- No es posible aplicar el mismo principio de encripción 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
- ¿Cúales números se pueden elegir para encriptar y decriptar?

TECNOLÓGICO DE MONTERREY®

¿Es posible usar el 5 y el 8?

Encriptando con 5

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

Encriptando con 8

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

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

TECNOLÓGICO DE MONTERREY®

Ejemplos inversos multiplicativos

- Se van a usar los números que cuenten con un inveso multiplicativo: {1,3,7,9}
- Ejemplo 1:
  - 7 es el inverso multiplicativo de 3

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

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

TECNOLÓGICO DE MONTERREY®

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

TECNOLÓGICO DE MONTERREY®

Primera observación

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

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

TECNOLÓGICO DE MONTERREY®

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. 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 constraste 6, 2, 4, 5 y 8 son primos en 10 ya que:
  - 2 divide a 6 y 10, i.e. mcd(6,10) = 2
  - 2 divide a 2 y 10, i.e. mcd(2,10) = 2
  - 2 divide a 4 y 10, i.e. mcd(4,10) = 2
  - 5 divide a 5 y 10, i.e. mcd(5,10) = 5
  - 2 divide a 8 y 10, i.e. 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.

TECNOLÓGICO DE MONTERREY®

El mcd y los números relativamente primos a n

$\exists$ inverso a^{-1} en mod n *ssi* 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

TECNOLÓGICO DE MONTERREY®

La función totient de Euler

- ¿Cuantos números a n pueden ser relativamente primos a n?
  - Respuesta: función totient $\Phi(n)$
  - to = total tient = quotient (cociente)
- Si n es primo:

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

existen n-1 números relativamente primos a n

- Si n es un producto de dos números primos (p y q)

$$\Phi(n) = \Phi(pq) = \Phi(p) \times \Phi(q)$$

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

existen (p-1)(q-1) números relativamente primos a n

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...

TECNOLÓGICO DE MONTERREY®

Criptosistema RSA

- Primera realización del modelo de Diffie-Hellman
- Realizado por Rivest, Shamir y Adleman en 1977 y publicado por primero vez en 1978
  - Se dice que un método casi idéntico fue creado por Clifford Cocks 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

TECNOLÓGICO DE MONTERREY®

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:

   $mcd\ [e, \phi(n)] = 1$.
5. Cada usuario calcula la llave privada que cumpla:

   $d = inv\ [e,\phi(n)]$.
6. Se hace público el número n y la llave e.

   Kpub = (e,n)
7. Se guarda en secreto la llave d.

   Kpriv = (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 decriptar 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


Alicia

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:

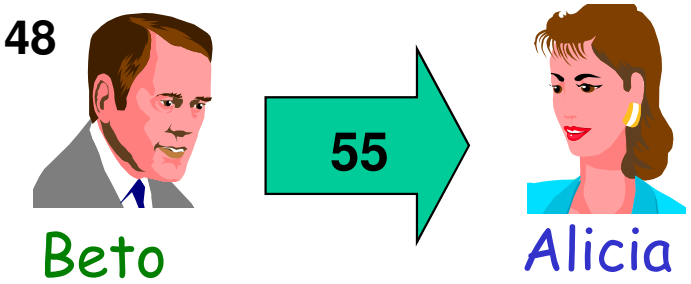
   $\text{mcd}\,[e, \phi(n)] = \text{mcd}[5,72] = 1$
5. Se calcula una llave privada

   $d = \text{inv}\,[e,\phi(n)] = \text{inv}\,[5,72] = 29$
6. Se envía a Beto la llave pública (5,91)
7. Permanece en secreto 29

Ejemplo encripción/decripción RSA

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

$$C = M^e \bmod n$$
$$C = 48^5 \bmod 91$$
$$C = 5245.803.968 \bmod 91$$
$$C = 55$$

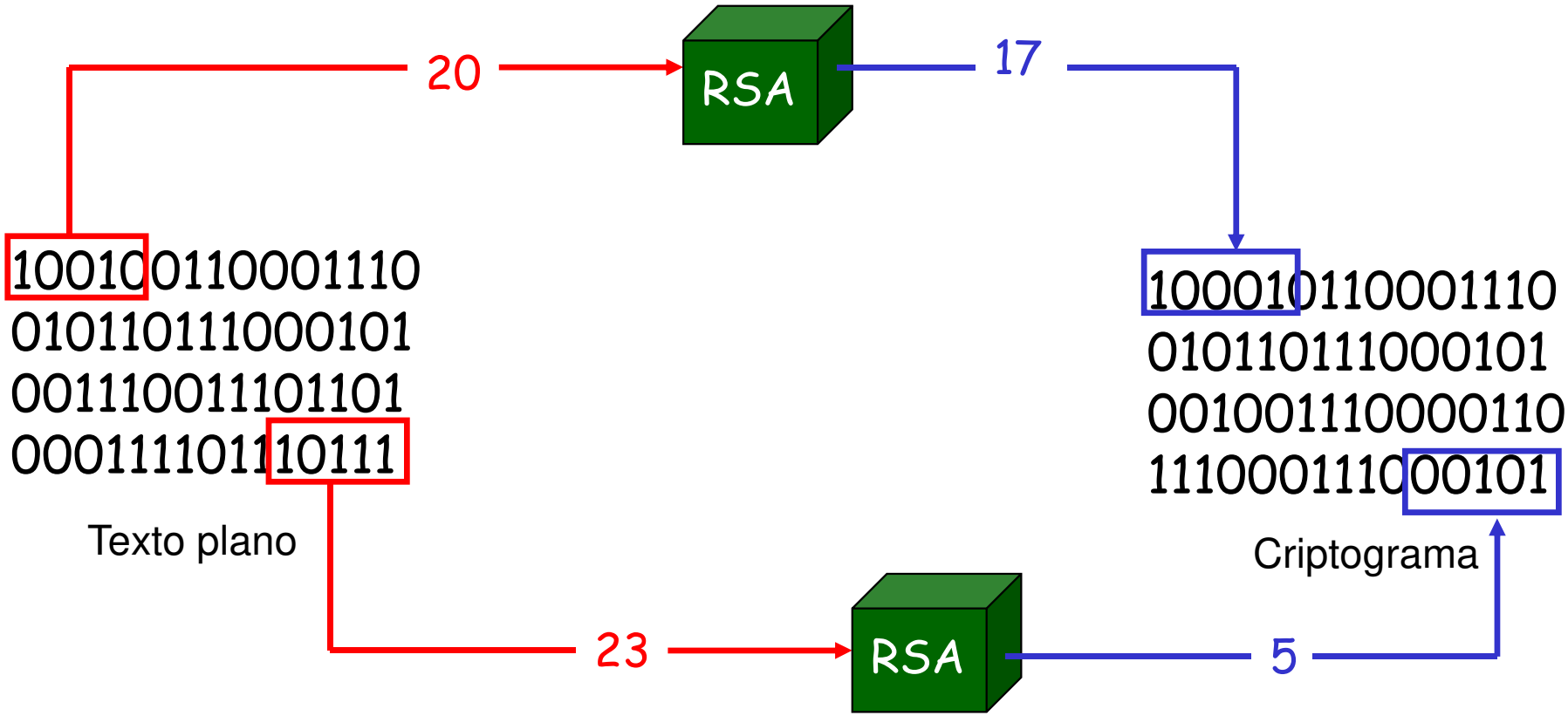


- Se envía el mensaje 55 al receptor
- Para decriptar C, Alicia toma la llave privada (29, 91)

$$M = C^d \bmod n$$
$$M = 55^{29} \bmod 91$$
$$M = 2.954x10^{50} \bmod 91$$
$$M = 48$$

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 => 5 bits

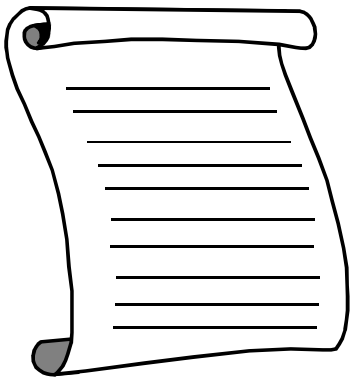


Sistemas Hibridos

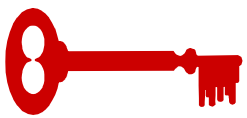
- Un algoritmo simétrico con una llave de sesión aleatoria es usada para encriptar un mensaje.
- Un algoritmo de llave pública es usado para encriptar la llave de sesión aleatoria.

Encripción sistema hibrido

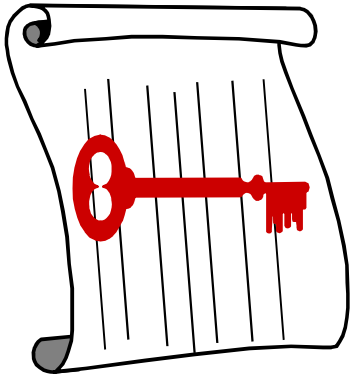
1. Escribir mensaje a enviar



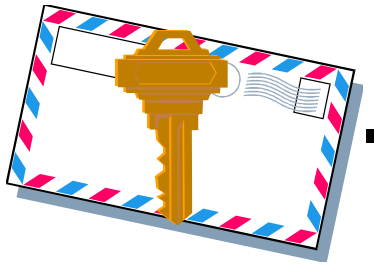
2. Generar una llave simétrica aleatoria



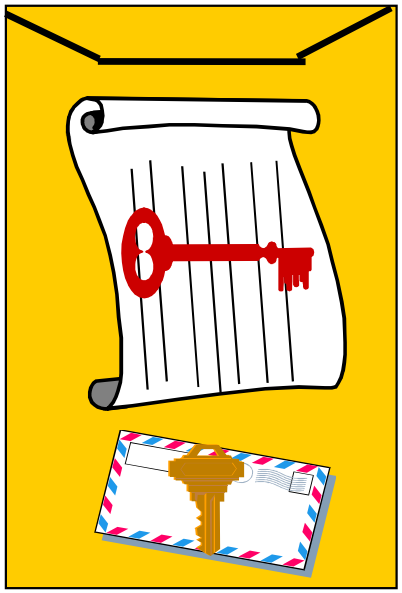
3. Encriptar mensaje con llave simétrica



4. Tomar llave pública destinatario y encripar llave simetrica

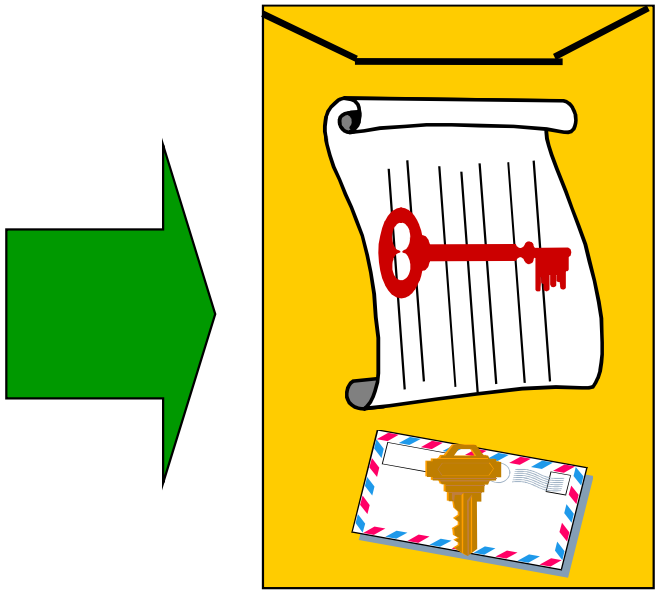


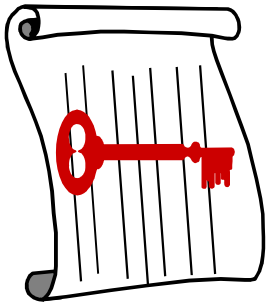
5. Poner mensaje y llave encriptados en un solo mensaje y enviarlo



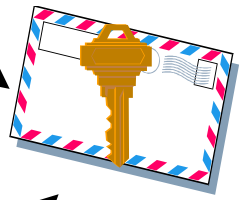
Decripción sistema hibrido

1. Se recibe el mensaje

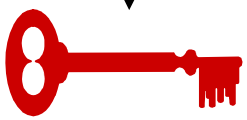




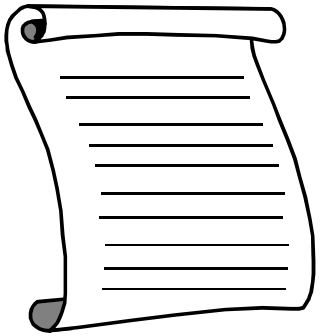
2. Se separan mensaje encriptado y llave encriptada



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?

TECNOLÓGICO DE MONTERREY®

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

TECNOLÓGICO DE MONTERREY®

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 dia 19 de noviembre de 1999
pretendo anunciar que se termino el presente texto
para pruebas de programas hash.

Atte

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

TECNOLÓGICO DE MONTERREY®

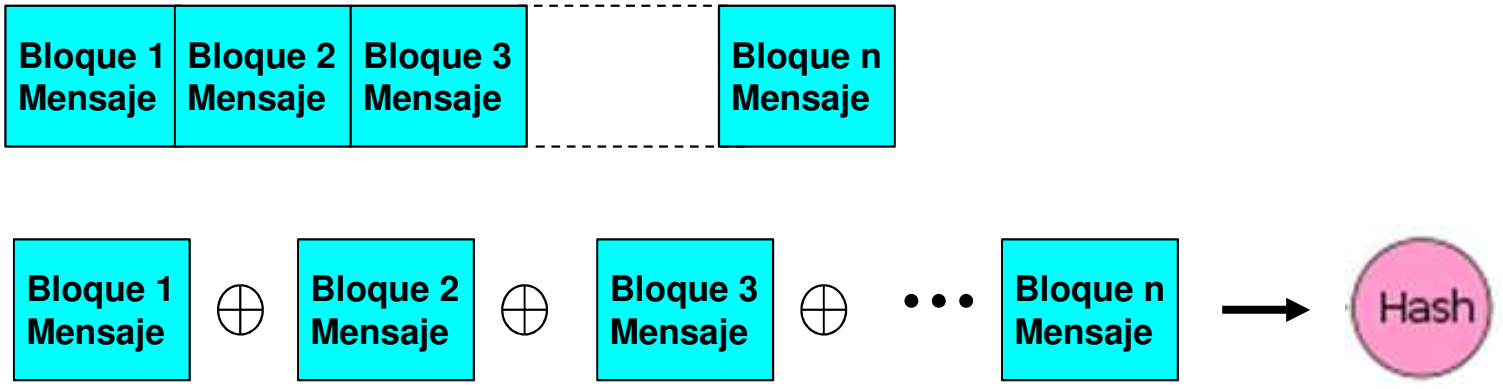
Propiedades de una función hash

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

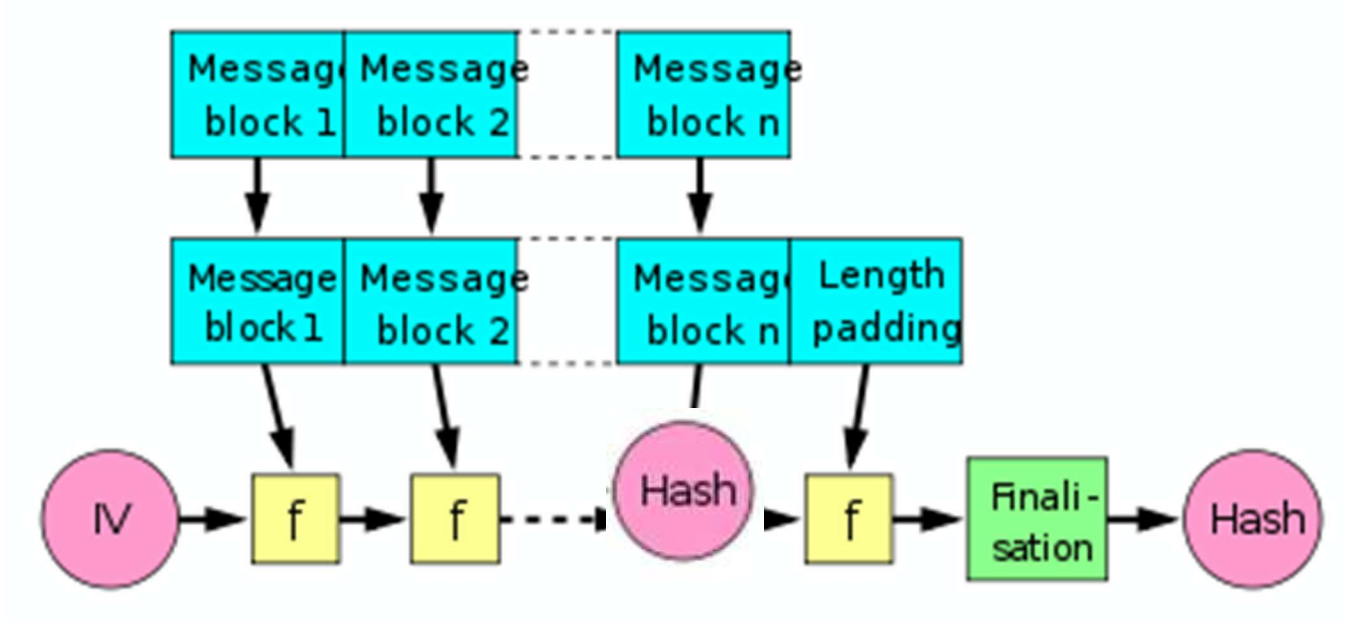


Pseudocódigo

```
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");
     }
}
```

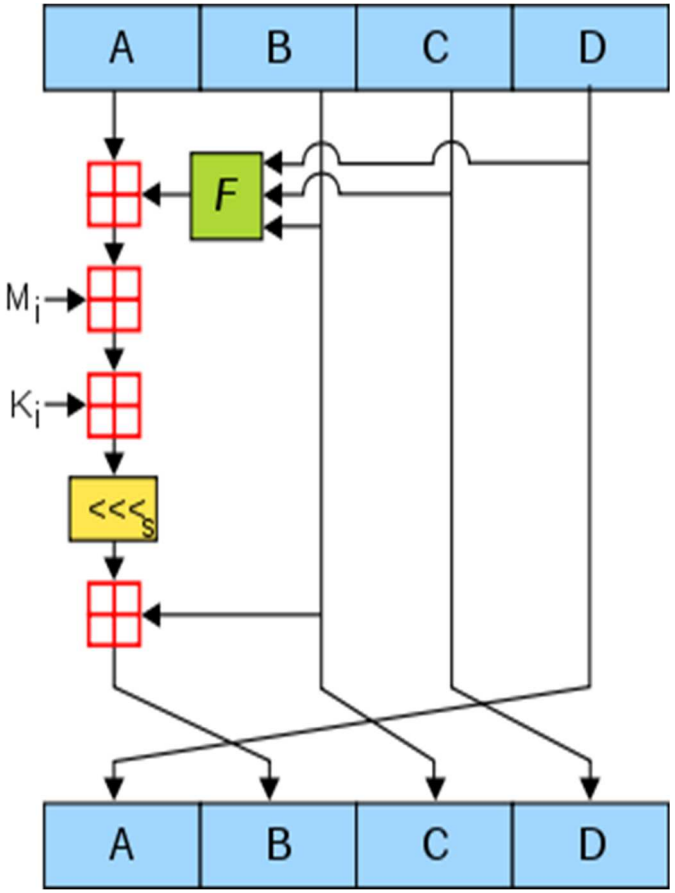
Merkle-Damgard



- Entrada dividida en bloques de igual tamaño y será la entrada a funciones de compresión.
- Añadir relleno: 1000…0 || longitud mensaje
- Finalisation: Opcional.
- Usado en todas las funciones hash anteriores al 2004
  - MD4, MD5, RIPE-MD, RIPE-MD160, SHA0, SHA1, SHA2

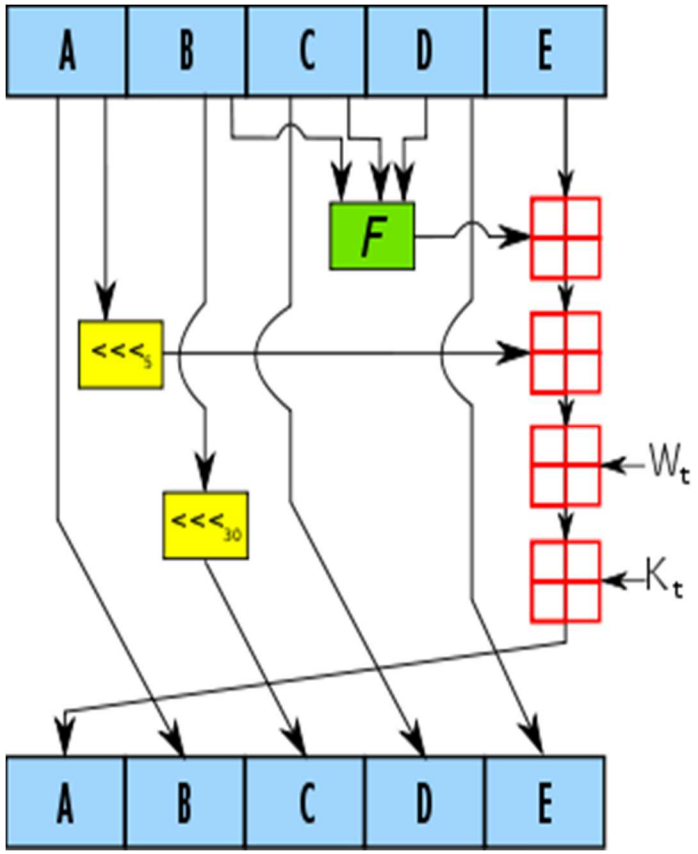
MD5 y SHA-1

64 rounds of:



128 bits

80 rounds of:



160 bits

TECNOLÓGICO DE MONTERREY®

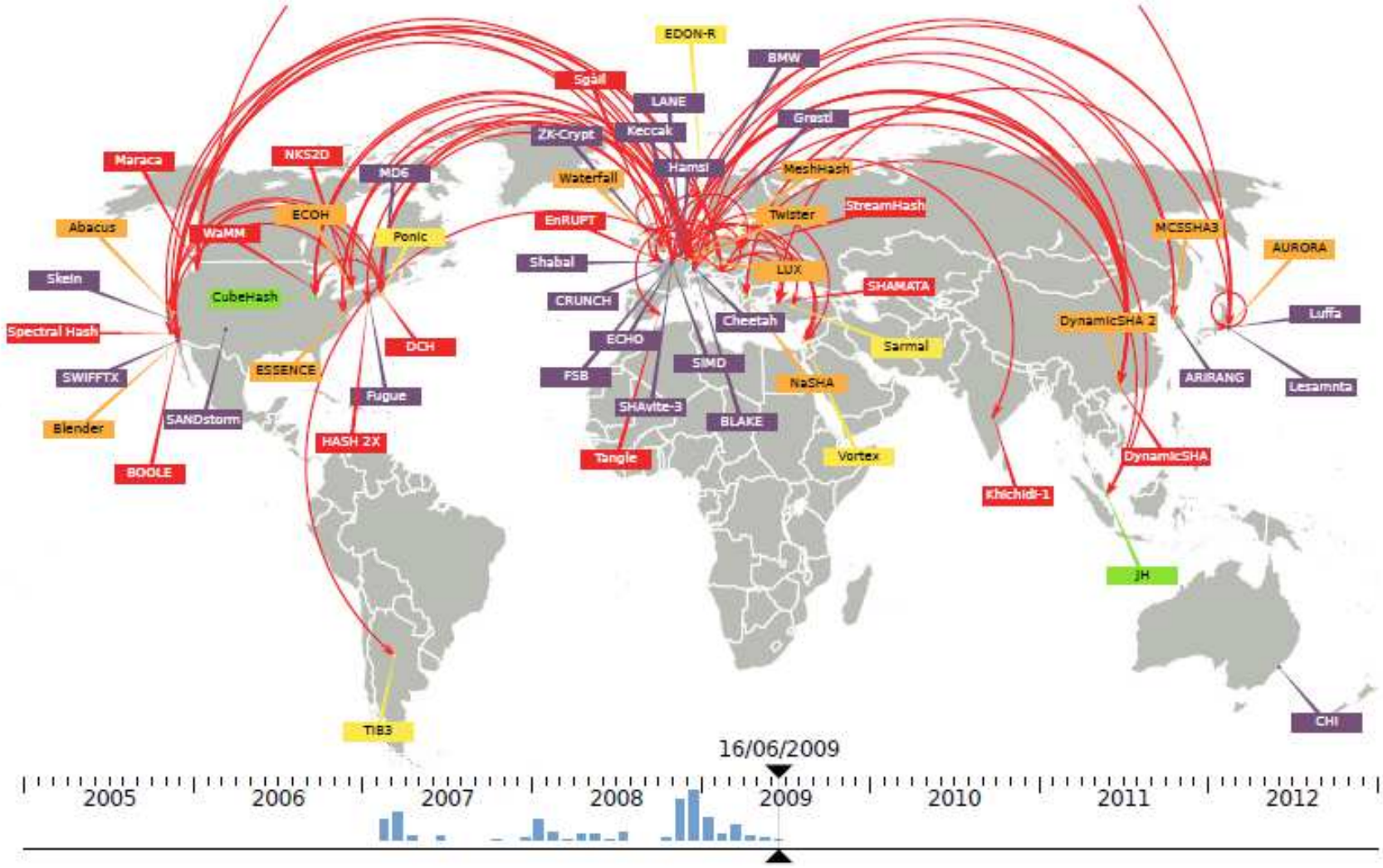
Ataques a funciones hash

- 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?

TECNOLÓGICO DE MONTERREY®

El campo de batalla



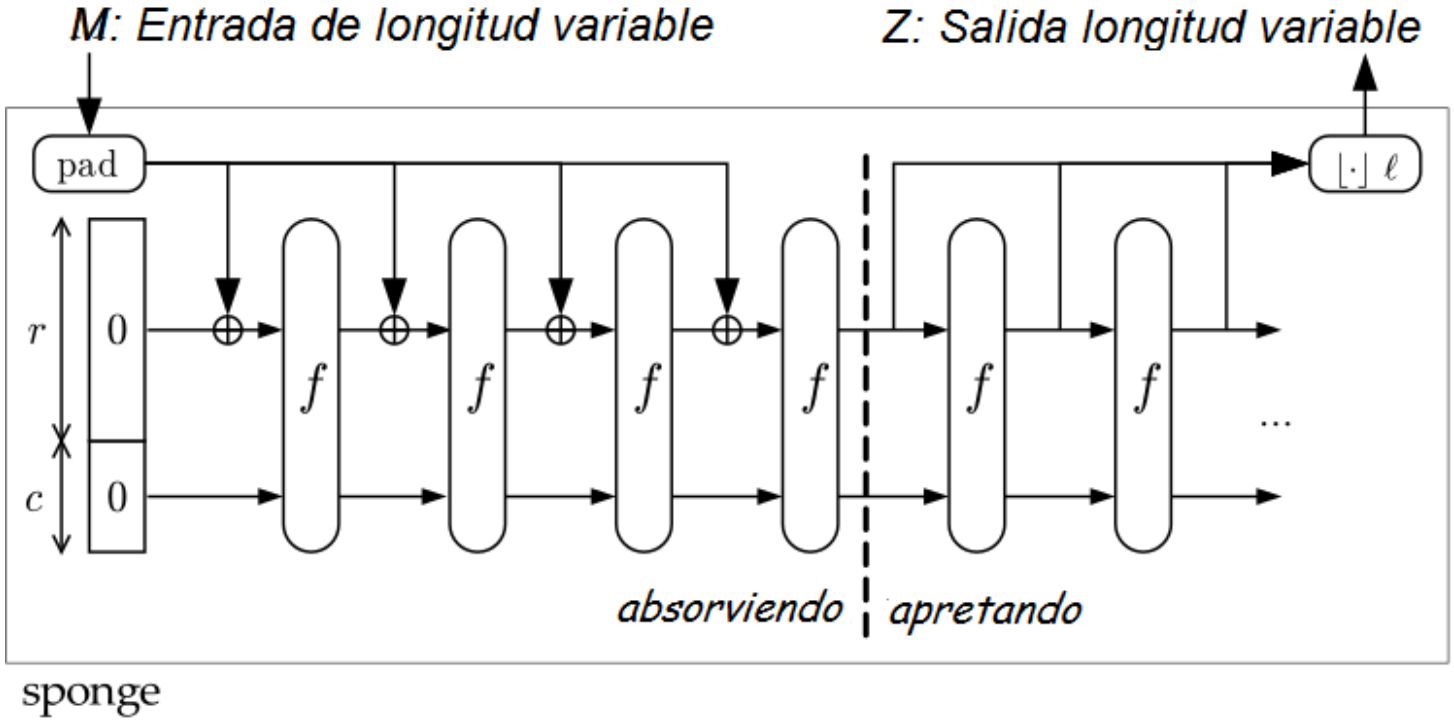
Cortesía de Christophe De Canniere

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

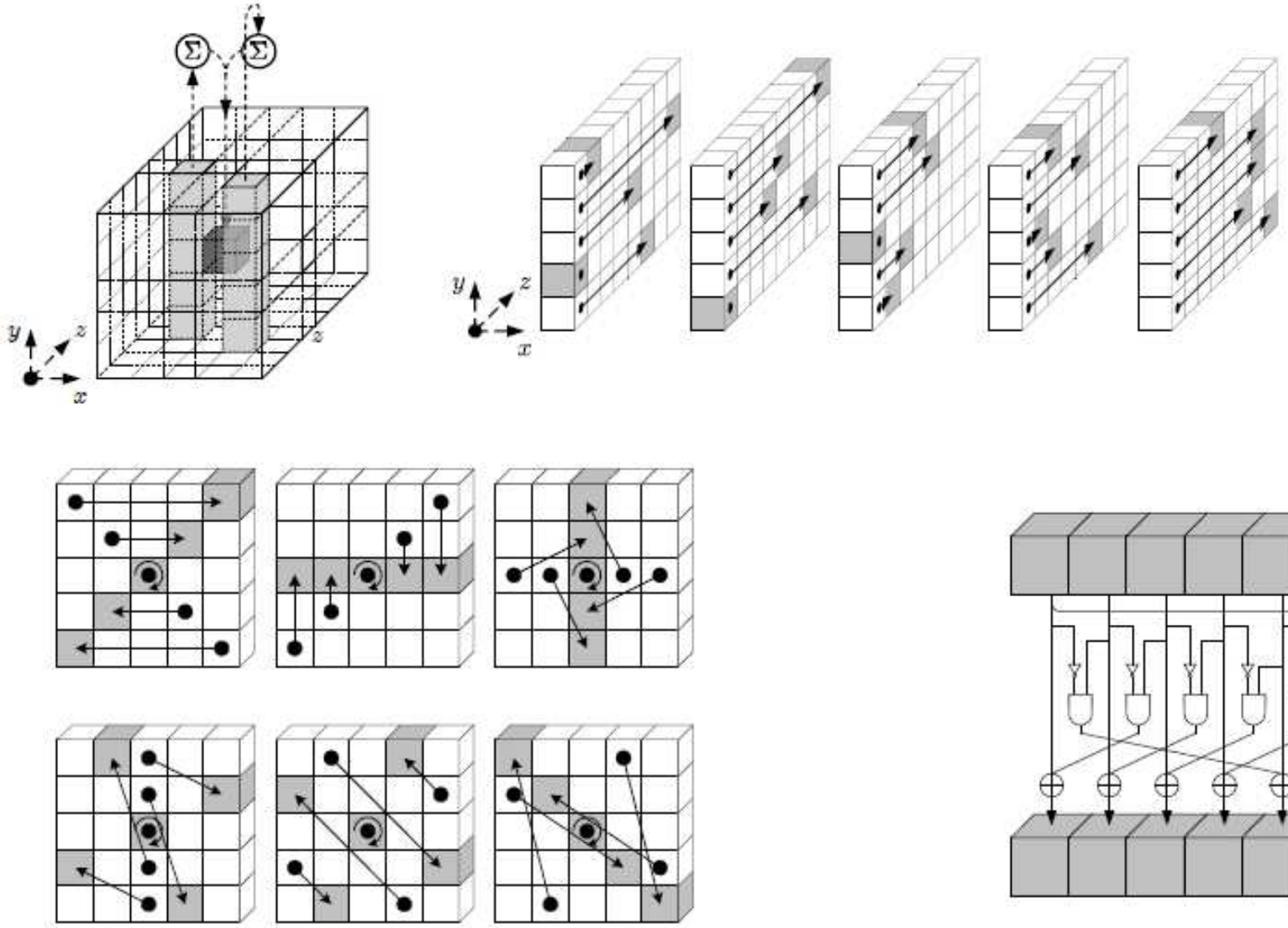


sponge

- 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.

TECNOLÓGICO DE MONTERREY®

Permutaciones en Keccak



TECNOLÓGICO DE MONTERREY®

¿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

TECNOLÓGICO DE MONTERREY®

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

TECNOLÓGICO DE MONTERREY®

Integridad y huellas digitales

TECNOLÓGICO DE MONTERREY®

¿Cómo se puede autenticar una comunicación?

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

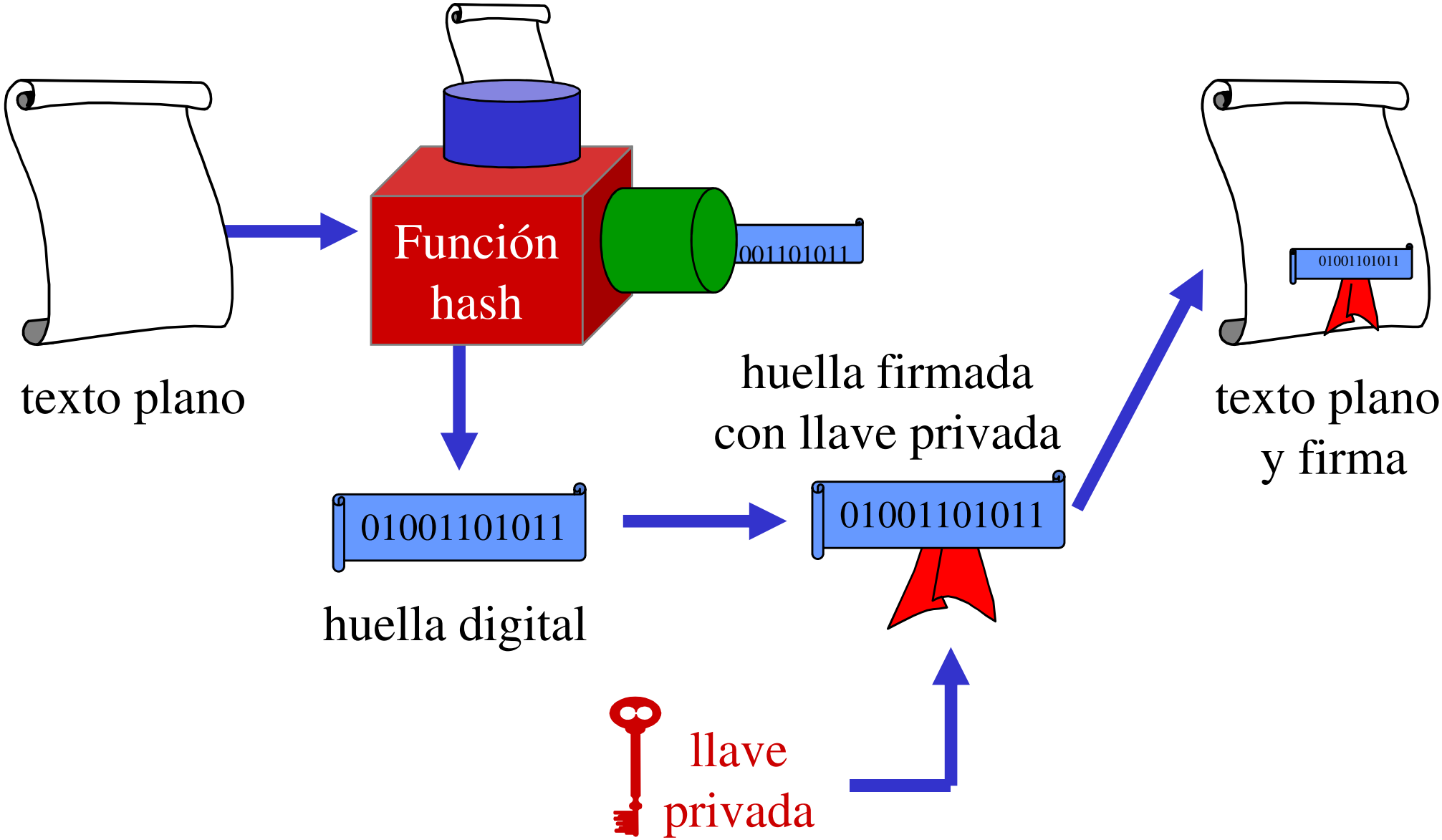
Un esquema de autenticación

TECNOLÓGICO DE MONTERREY®

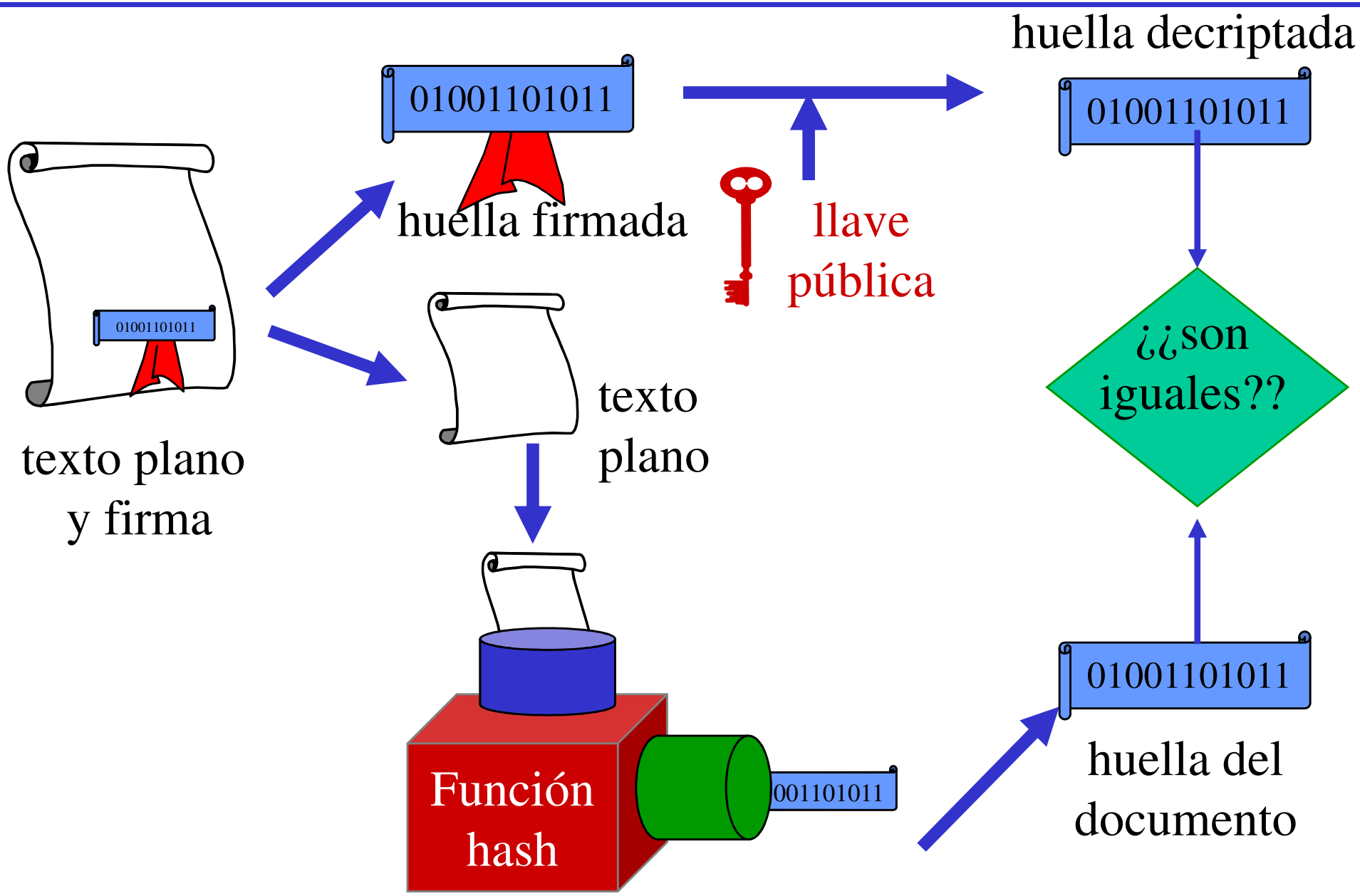
Firmas digitales

- 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)



TECNOLÓGICO DE MONTERREY®

Estándares firmas digitales

- Existen tres algoritmos aprovados 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).

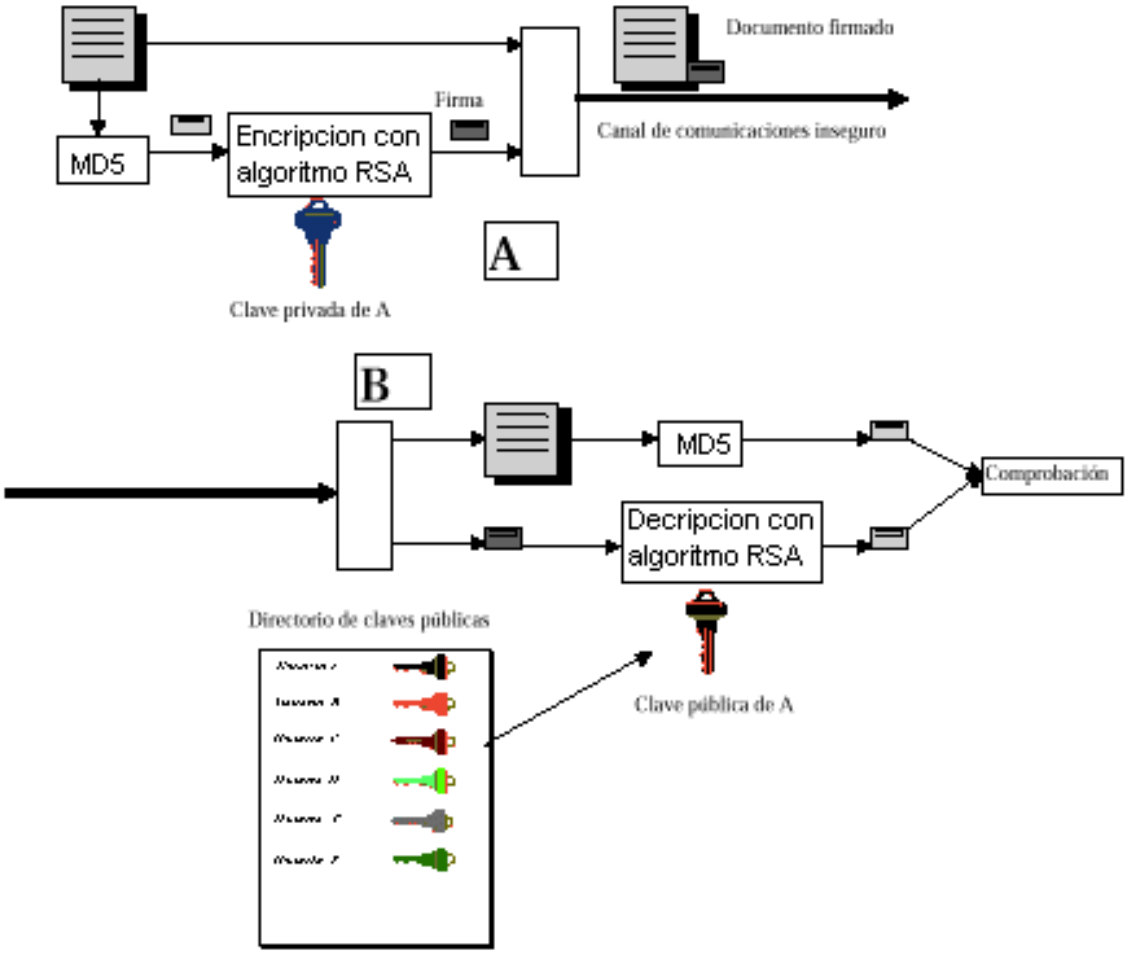
TECNOLÓGICO DE MONTERREY®

Diferencias RSA y DSS

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

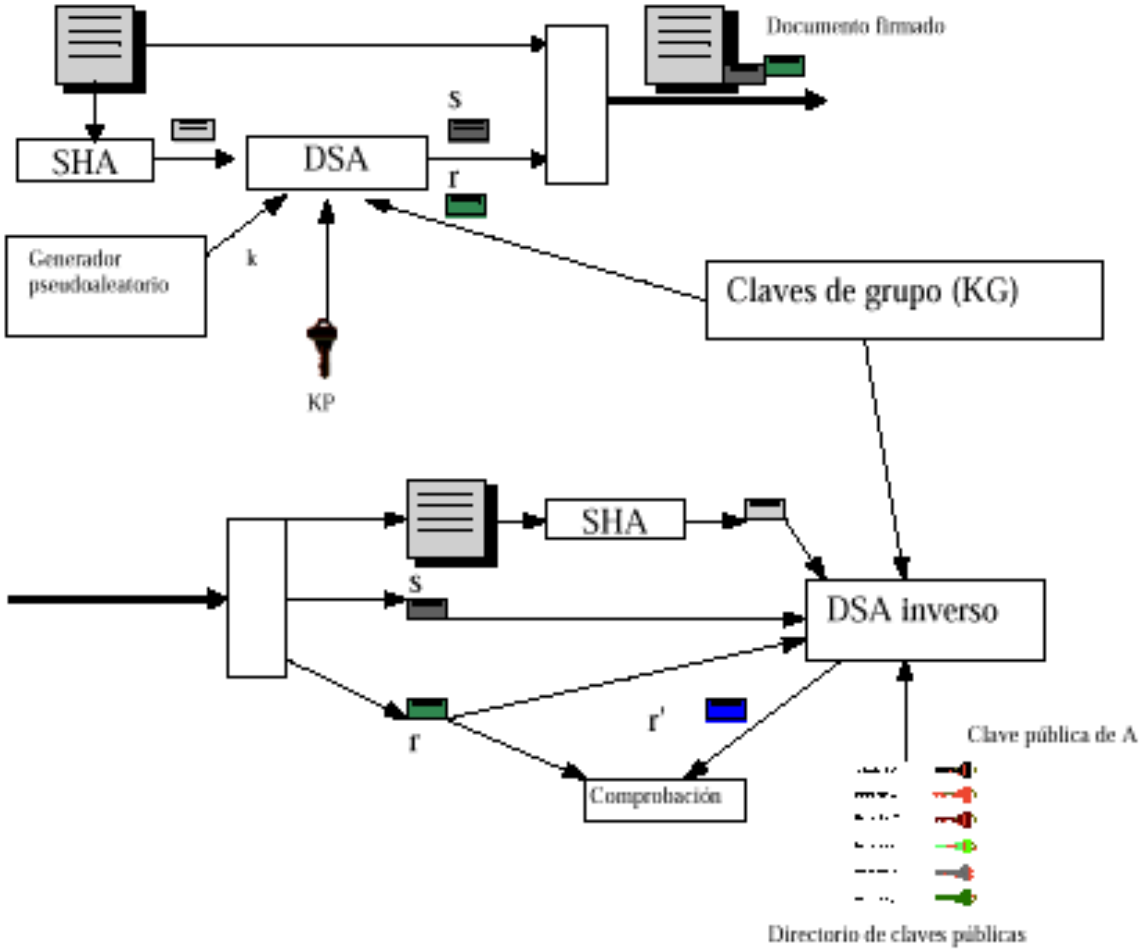
Algoritmo firma digital RSA

- Mismo principio de la firma
  - Algoritmo huella digital: MD5
  - Algoritmo encripción/decripción: RSA



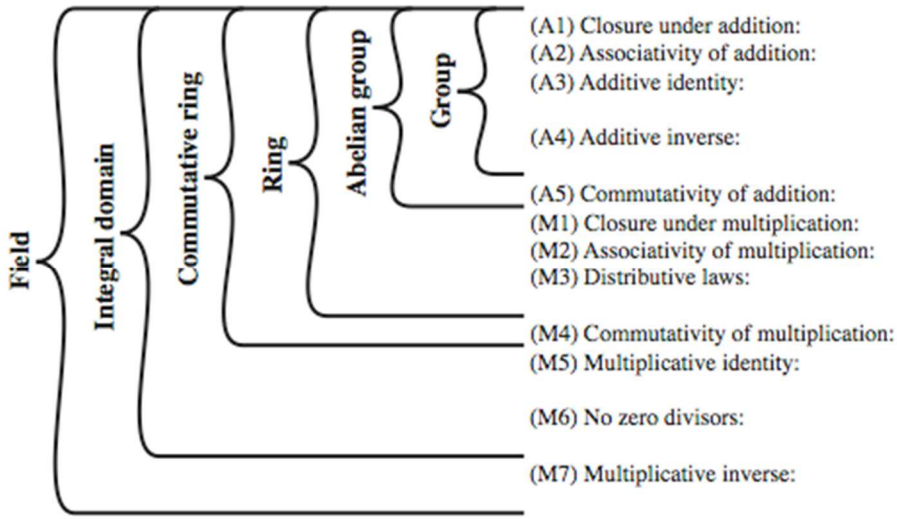
Algoritmo firma digital DSS

- Huella Digital
  - SHA-1
- Encripción/decripción
  - DSA



Curvas elípticas y criptografia

- Algoritmos basado en logaritmos discretos han sido adaptados a curvas elípticas, reemplazando los campos de Galois por curvas elípticas
- Propuesta en 1985 por Neal Koblitz y Victor Miller.



Algoritmo	Significado	Descripción
ECDSA	Elliptic Curve Digital Signature Algorithm	Basado en DSA
EdSA	Edwards-curve Digital Signature Algorithm	Basado en algoritmo de Schnorr y usa curvas Twisted Edwards
ECPVS	Elliptic Curve Pintsov Vanstone Signature	Mas eficiente que RSA
ECDH	Elliptic Curve Diffie-Hellman	Variante DH

TECNOLÓGICO DE MONTERREY®

Motivación

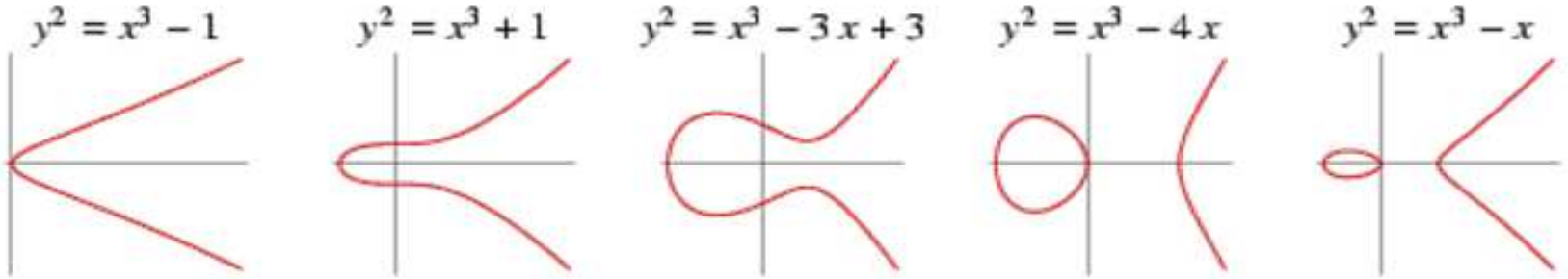
- Ambiente
  - Criptosistemas de llave pública
  - Especialmente los basados en el problema del logaritmo discreto
- Un criptosistema basado en curva elíptica puede lograr:
  - Menores longitudes de las llaves
    - Mayor rapidez de cálculo
    - Menos memoria y ahorro en transferencia
  - Con seguridad equivalente cuando se compara con criptosistemas clásicos, como RSA.

Forma general de una Curva Elíptica

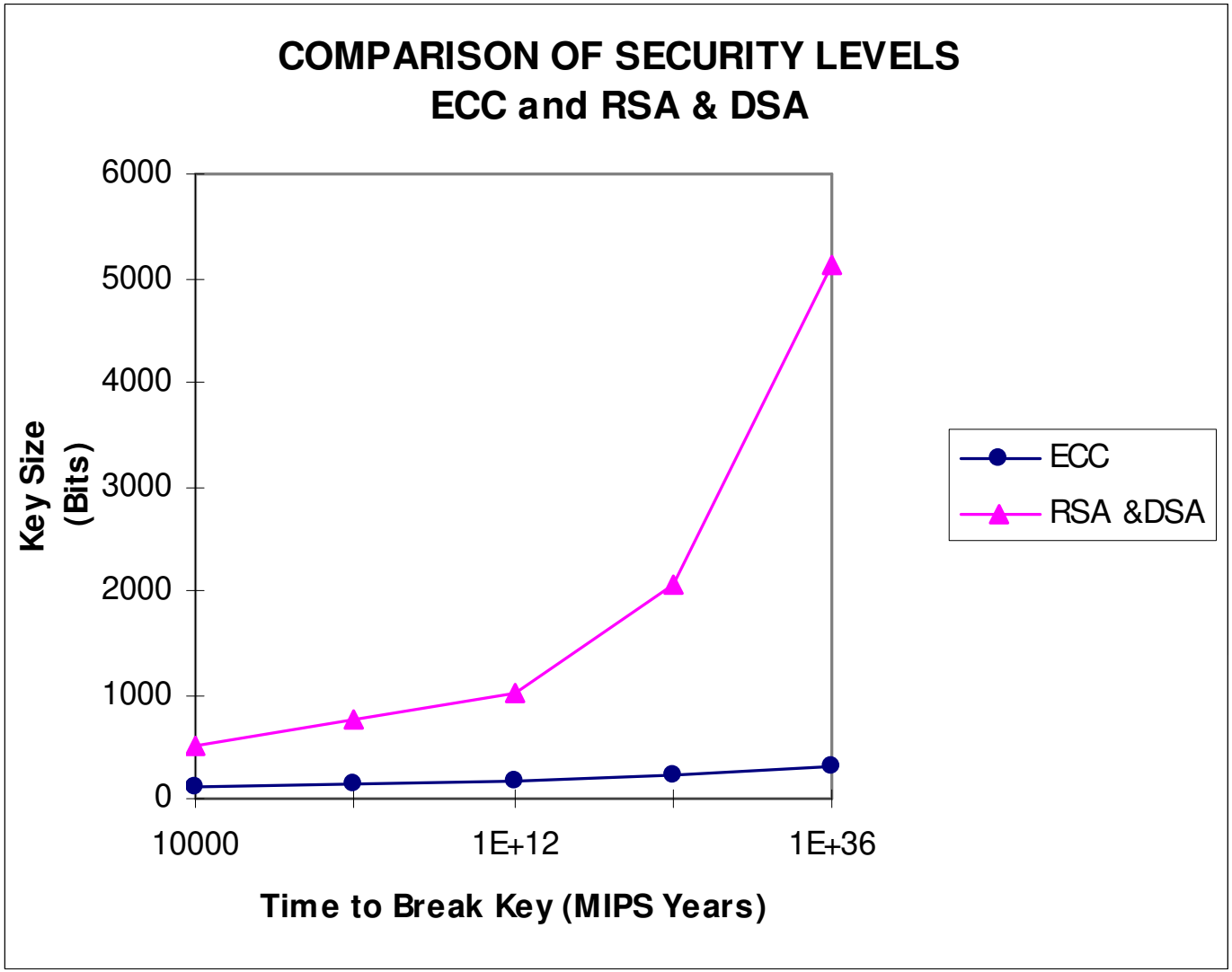
- Una curva elíptica es una curva definida por una ecuación de la forma

$$y^2 = x^3 + ax + b$$

- Los elementos de la ecuación pertenecen a un campo de números racionales, campos finitos (Fp) o campos de Galois ($GF(2^n)$).
- Ejemplos



¿Porqué las curvas elípticas?



Referencia: Certicom white paper. Remarks on fhe Security of The Elliptic Curve Criptosystem. Certicom. 1997

TECNOLÓGICO DE MONTERREY®

Tabla comparativa

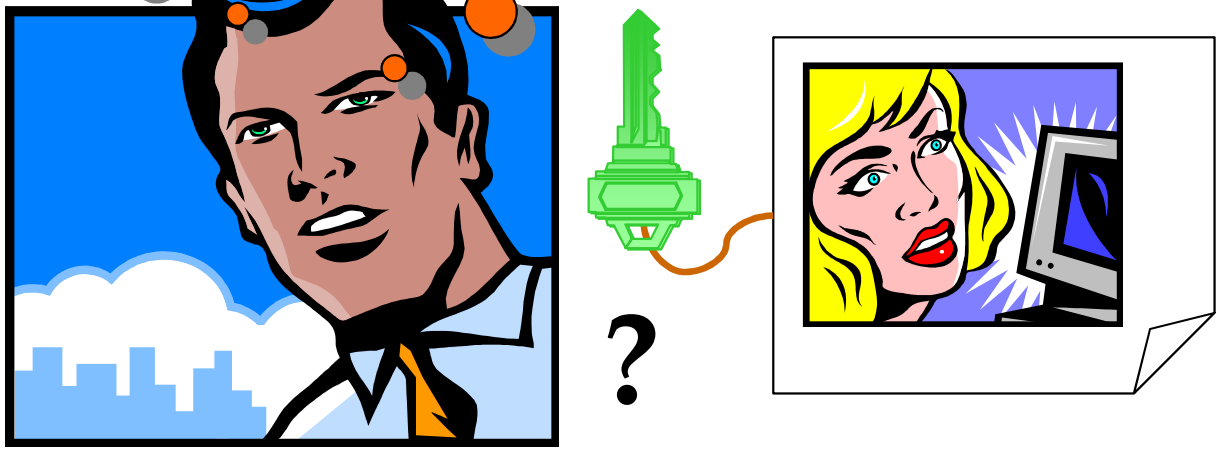
Tamaño llave simétrica (bits)	Tamaño llave de RSA y Diffie-Hellman (bits)	Tamaño llave curva elíptica (bits)
56	512	112
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

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?

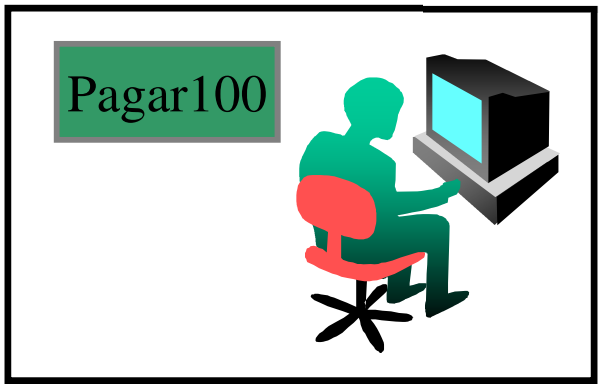
¿Cómo estar seguro de que la llave pública es aún válida?



Solicitando una llave pública

Alicia va a pagarle
100 pesos a Beto

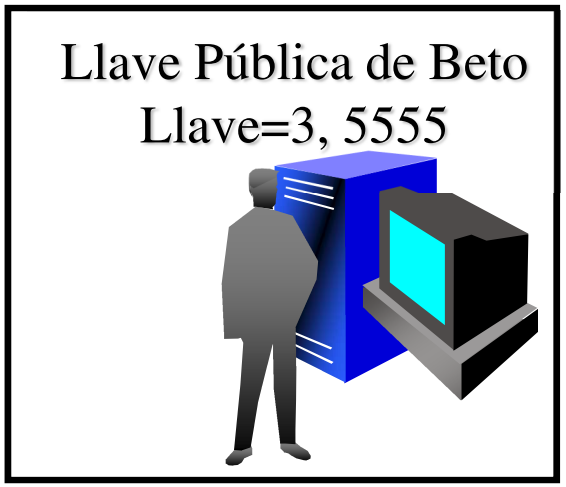
Alicia



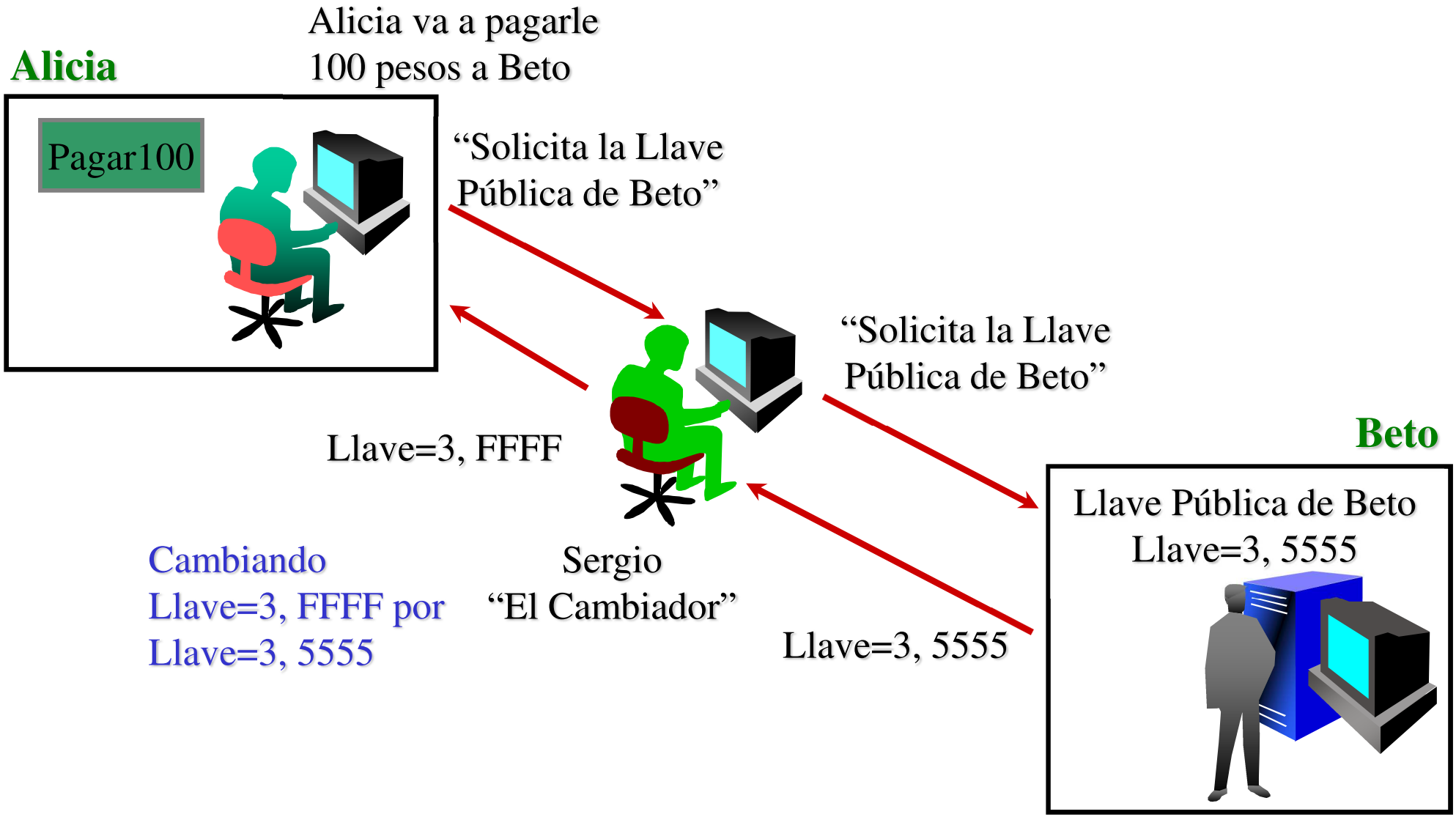
"Solicita la Llave
Pública de Beto"

Entregando llave
públic de Beto
Llave=3, 5555

Beto



El ataque "Man in the Middle" (MIM)



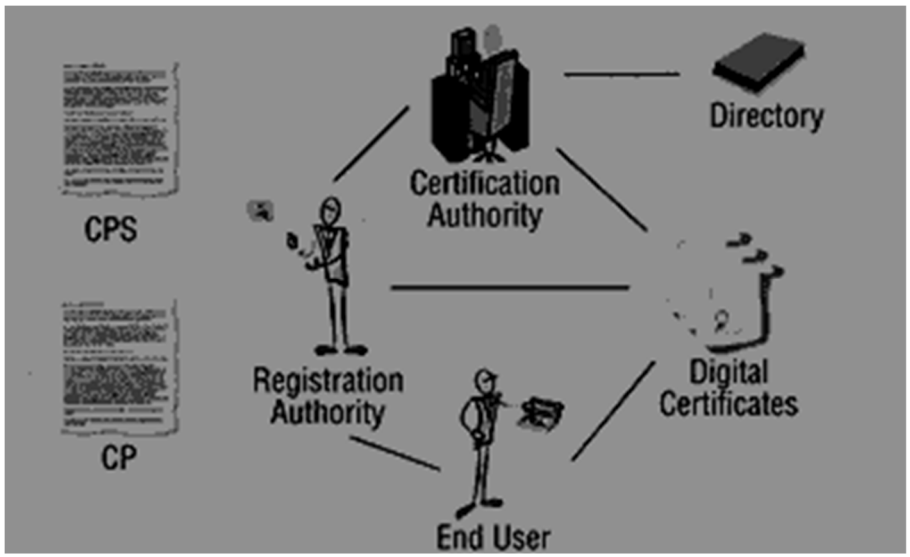
TECNOLÓGICO DE MONTERREY®

Certificados Digitales

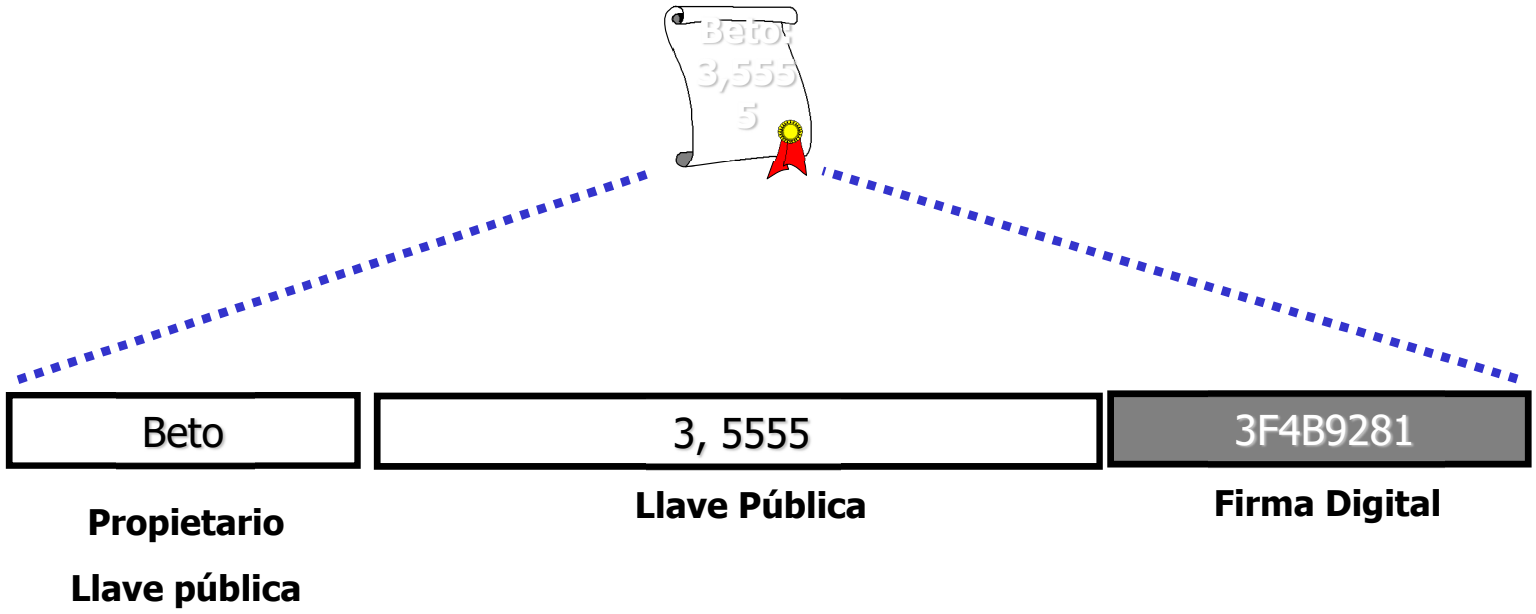
- Solución:
  - Intercambio de llaves públicas firmadas digitalmente con la llave privada de una 3a persona.
  - 3a. persona de confianza que de a conocer su llave pública.
- Certificado digital:
  - Archivo o estructura de datos que funciona como una identificación para el propietario.
  - Amarra la 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

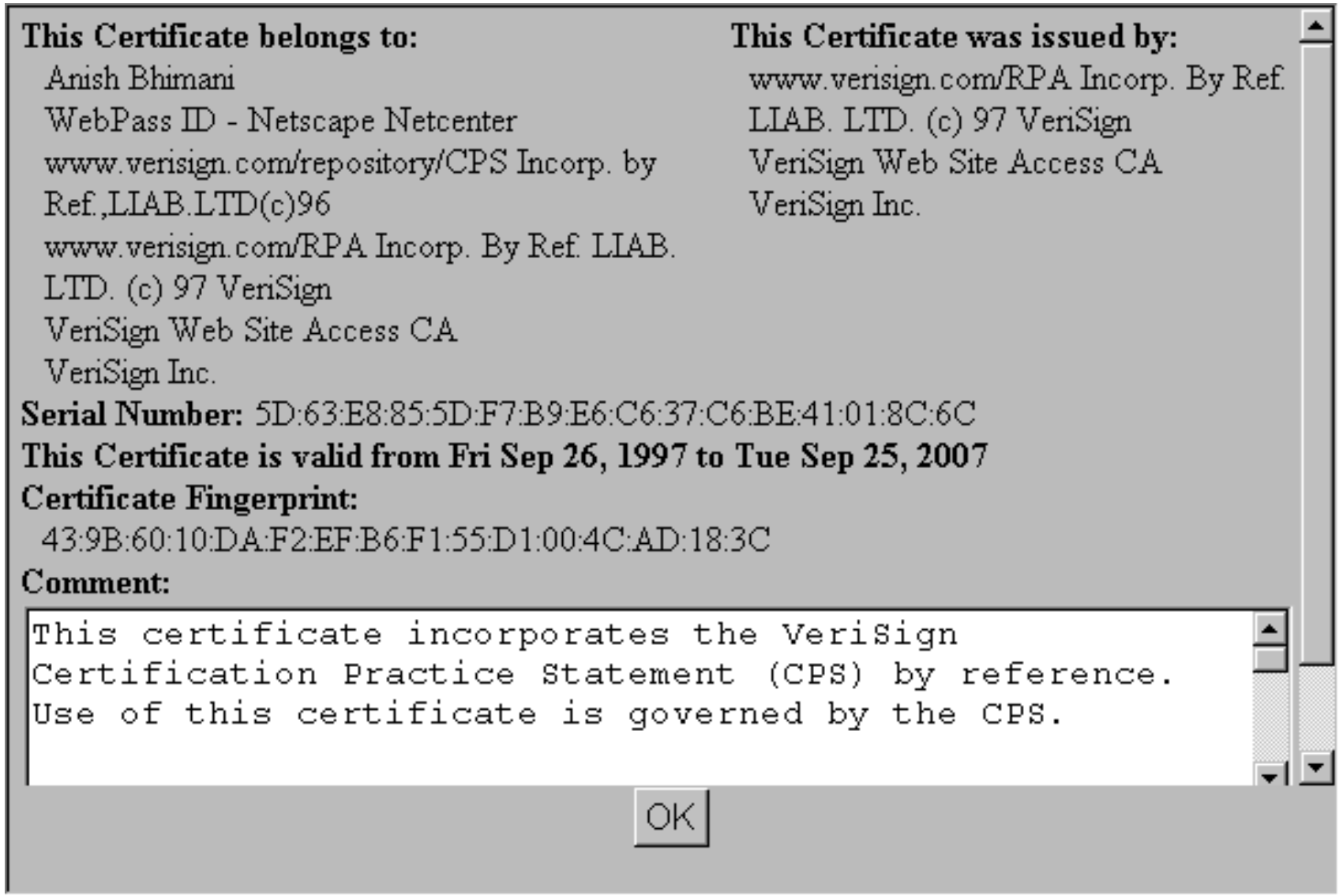


El contenido de un Certificado Digital

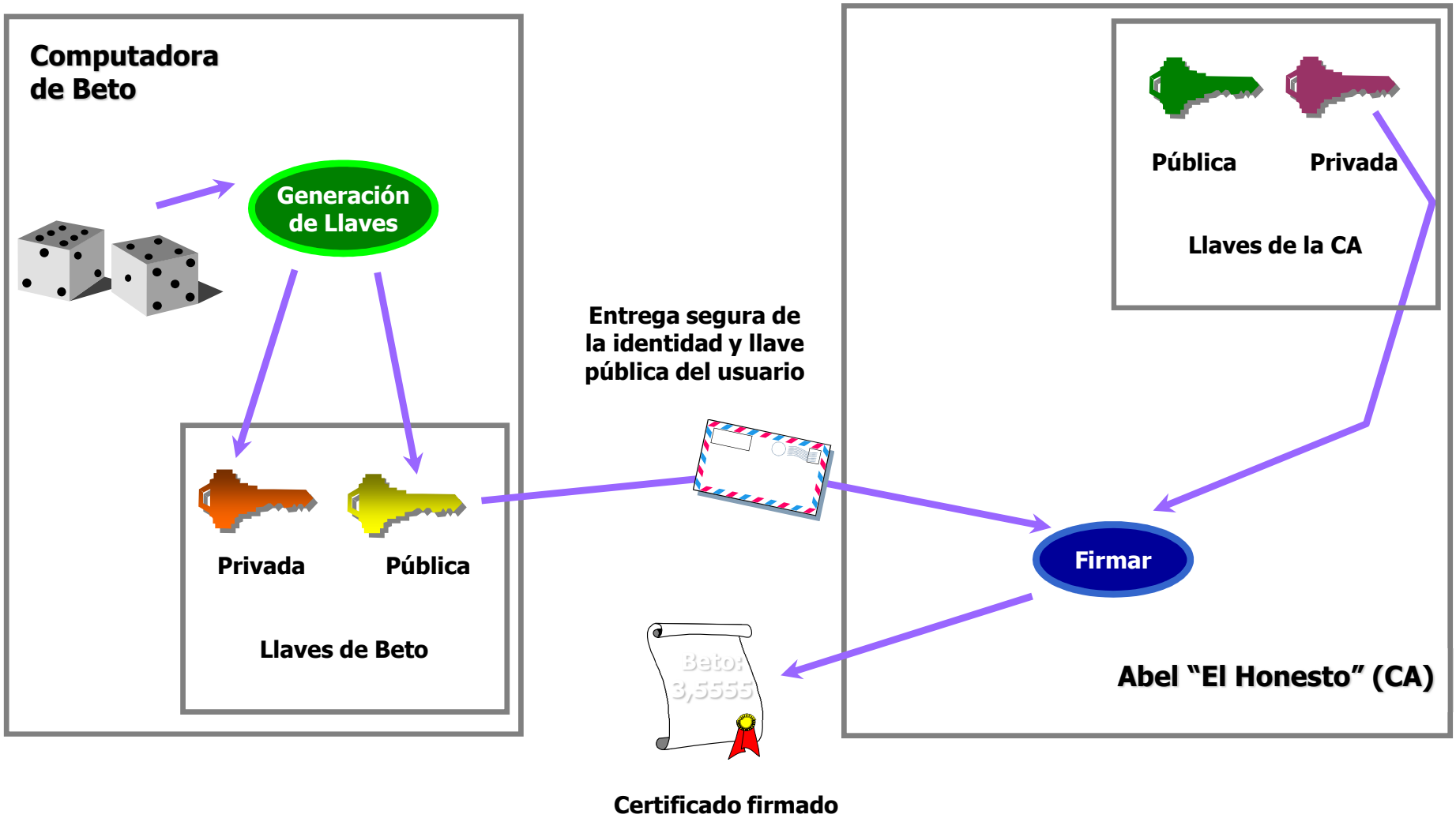


TECNOLÓGICO DE MONTERREY®

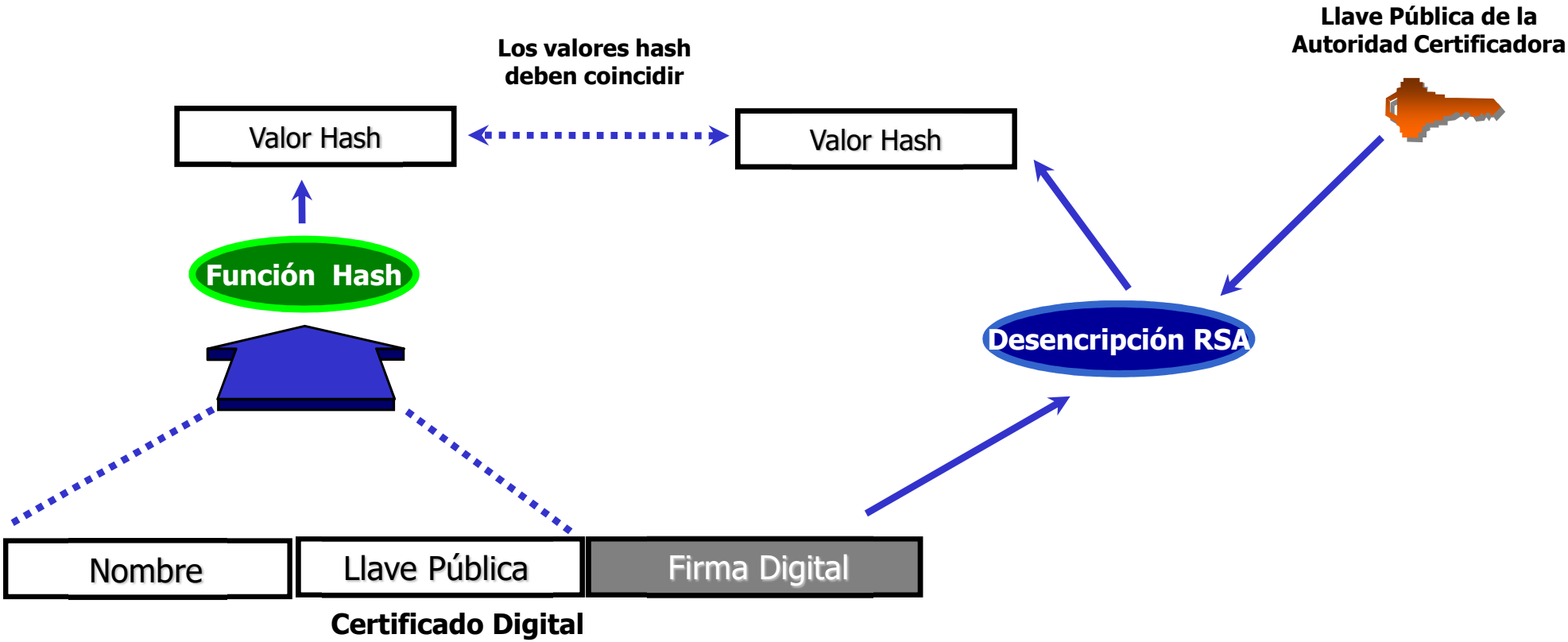
Ejemplo Certificado Digital



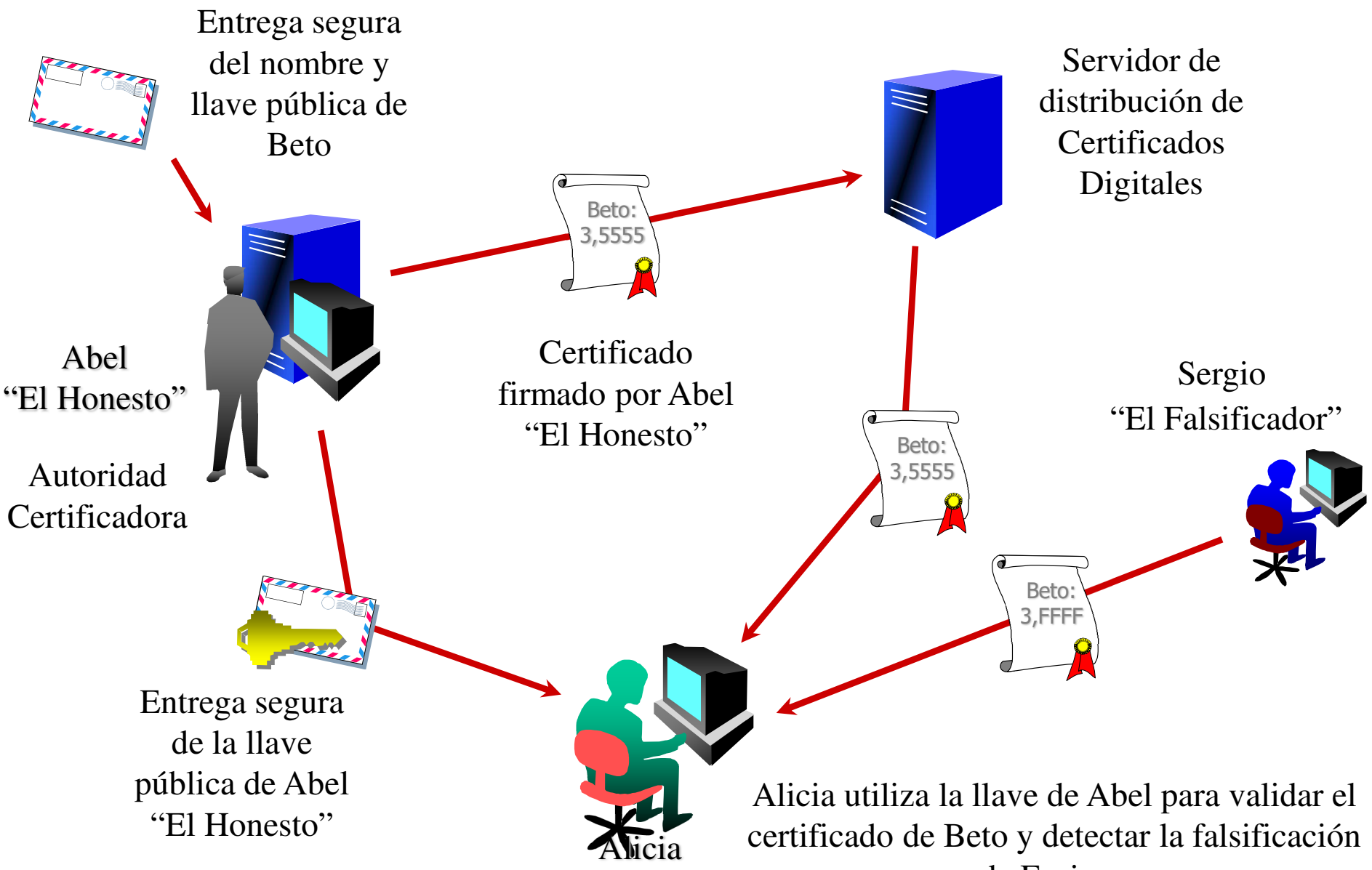
La generación de un certificado digital



La validación de un certificado digital



¿Cómo funciona todo?

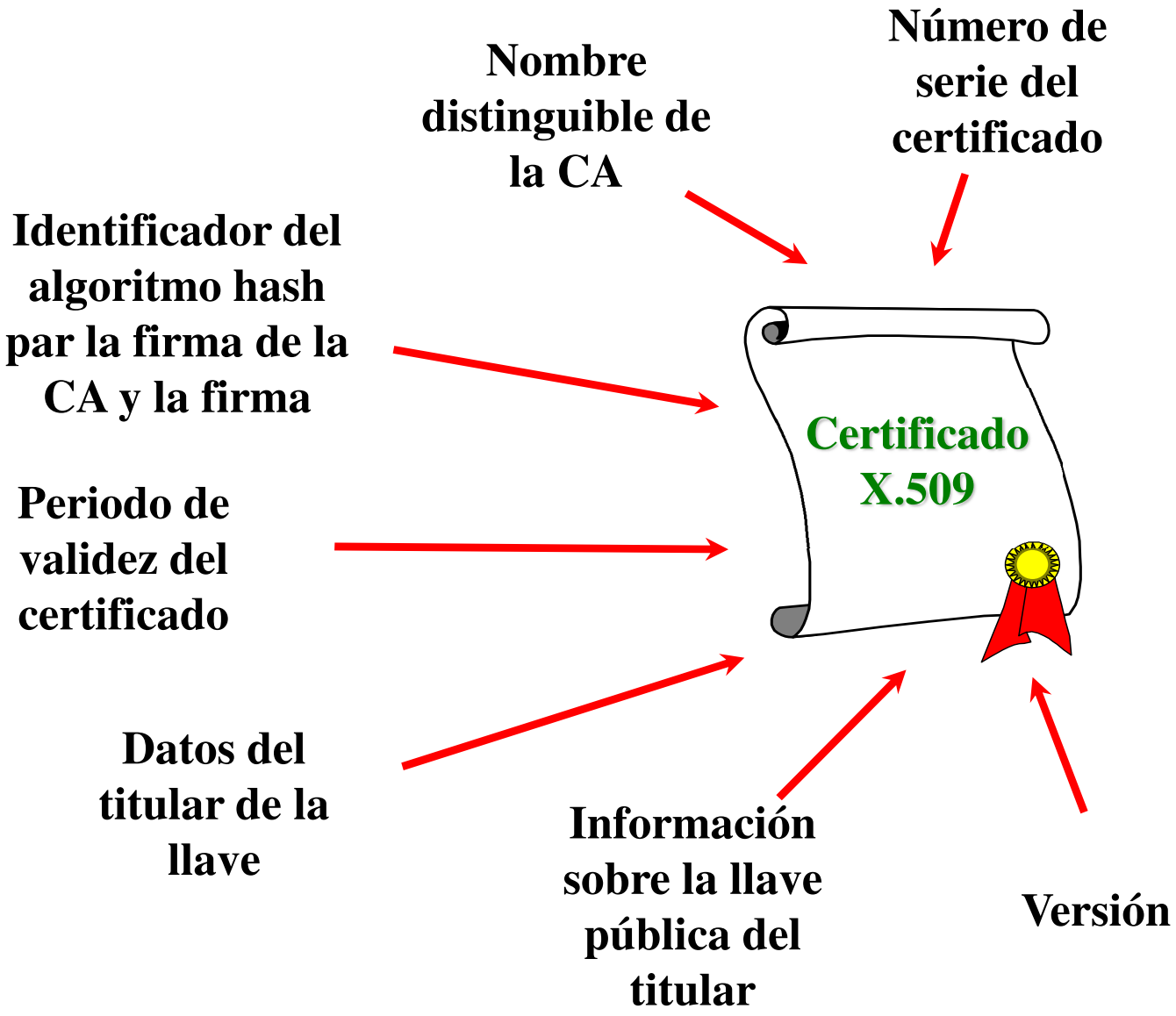


TECNOLÓGICO DE MONTERREY®

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



TECNOLÓGICO DE MONTERREY®

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
```

TECNOLÓGICO DE MONTERREY®

Revocación

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

TECNOLÓGICO DE MONTERREY®

Revocación

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

TECNOLÓGICO DE MONTERREY®

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 (crooss-certification)

Ese momento desafortunado cuando 2 cybernautas se encuentran cara a cara

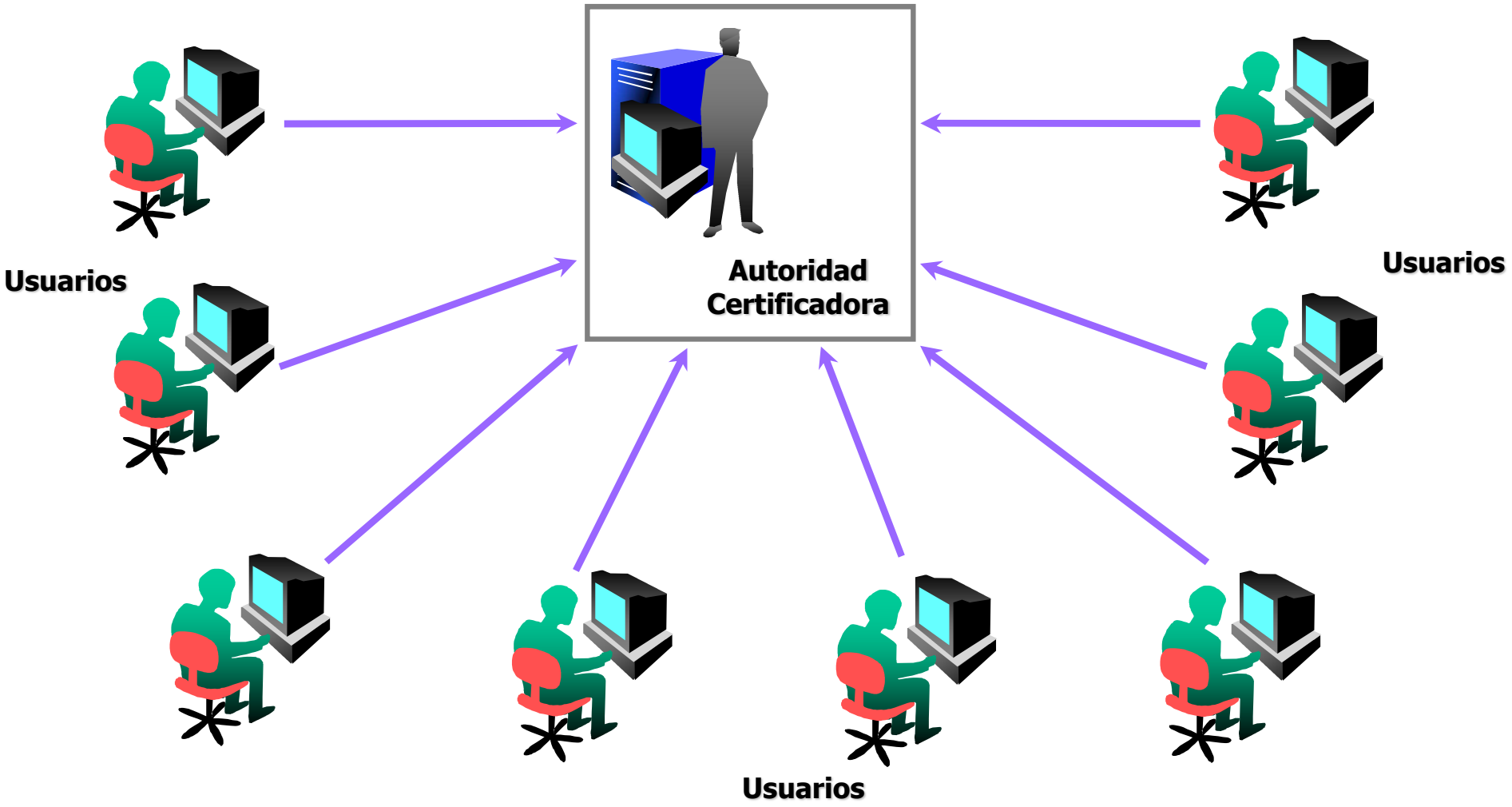
TECNOLÓGICO DE MONTERREY®

Modelos de confianza

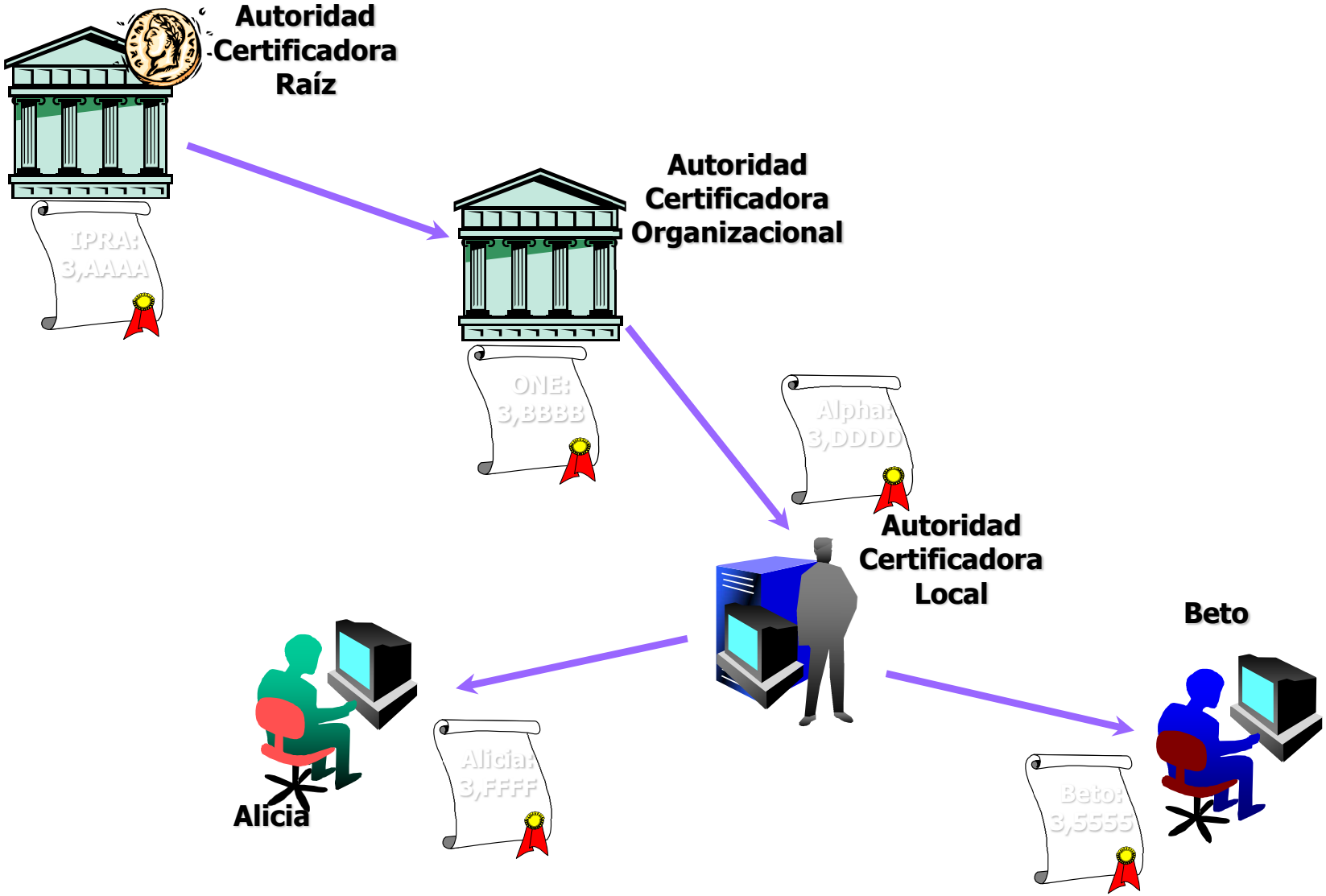
- La entidad “A” confia en la entidad “B” cuando “A” supone y asume que “B” se comportará exactamente como “A” espera.
- Jerárquico
  - Basado en la relación Superior / Subordinado
  - Actualmente es la regla en ambiente de web
  - Mientras mas cercano al nivel root se comprometa una llave mayor será 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

TECNOLÓGICO DE MONTERREY®

Modelo Centralizado

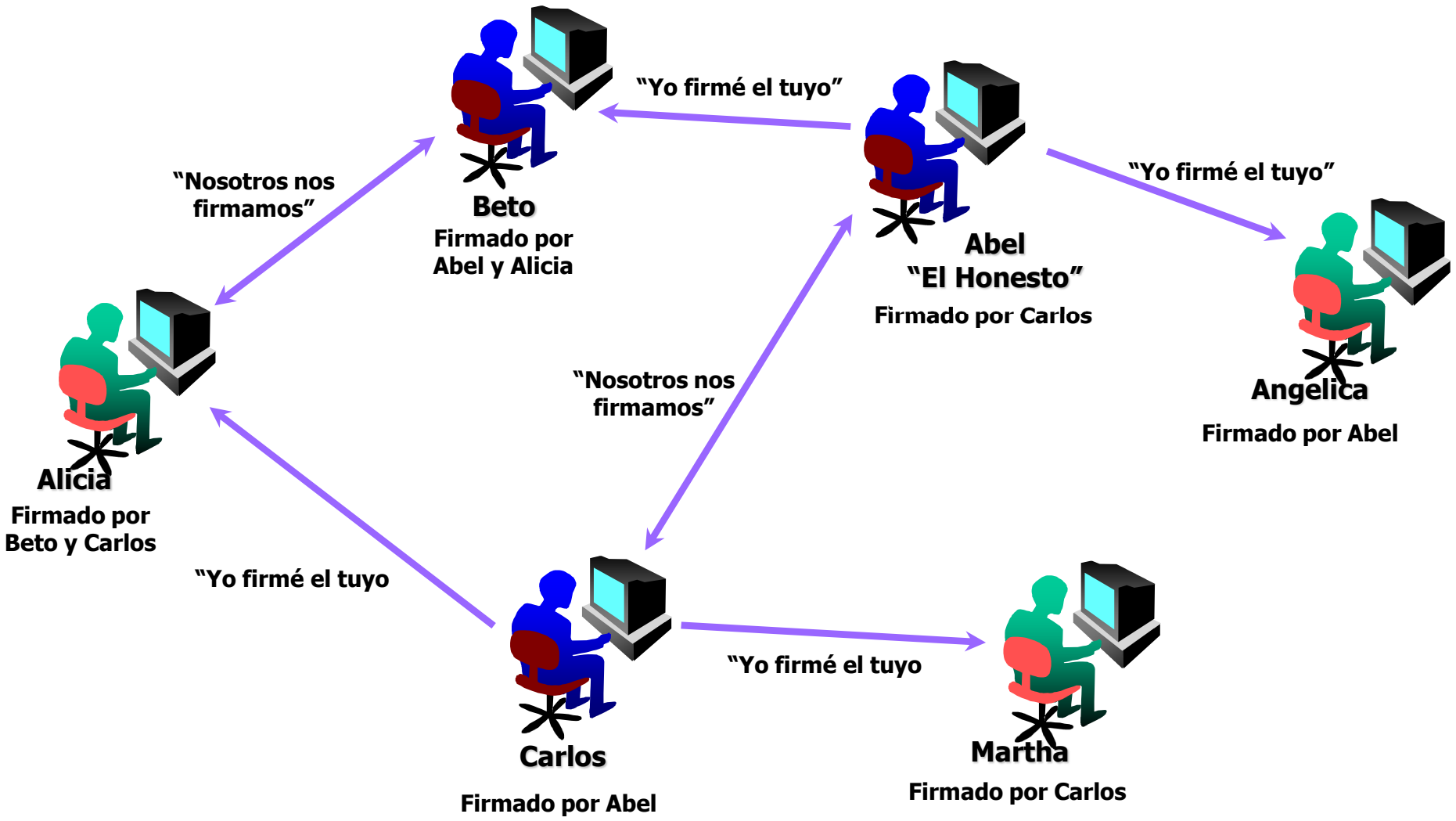


Modelo Jerárquico

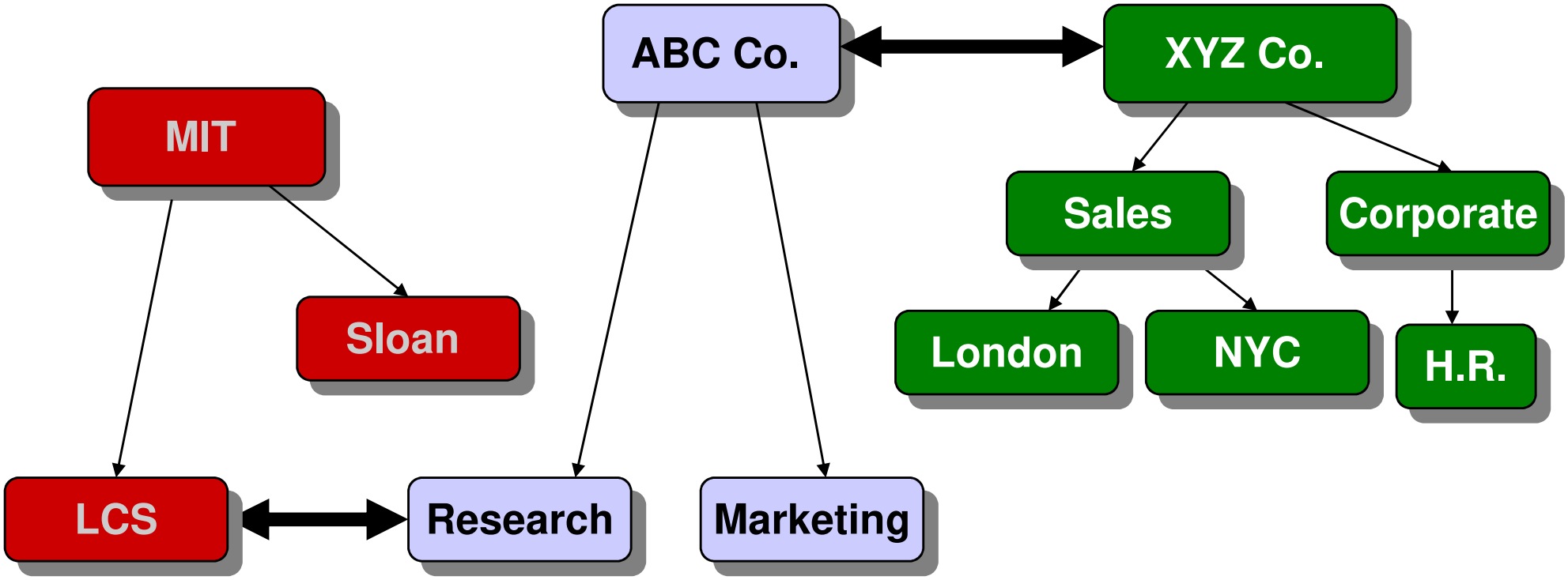


TECNOLÓGICO DE MONTERREY®

"Web of Trust" de PGP



Ejemplo de Cross-Certification



TECNOLÓGICO DE MONTERREY®

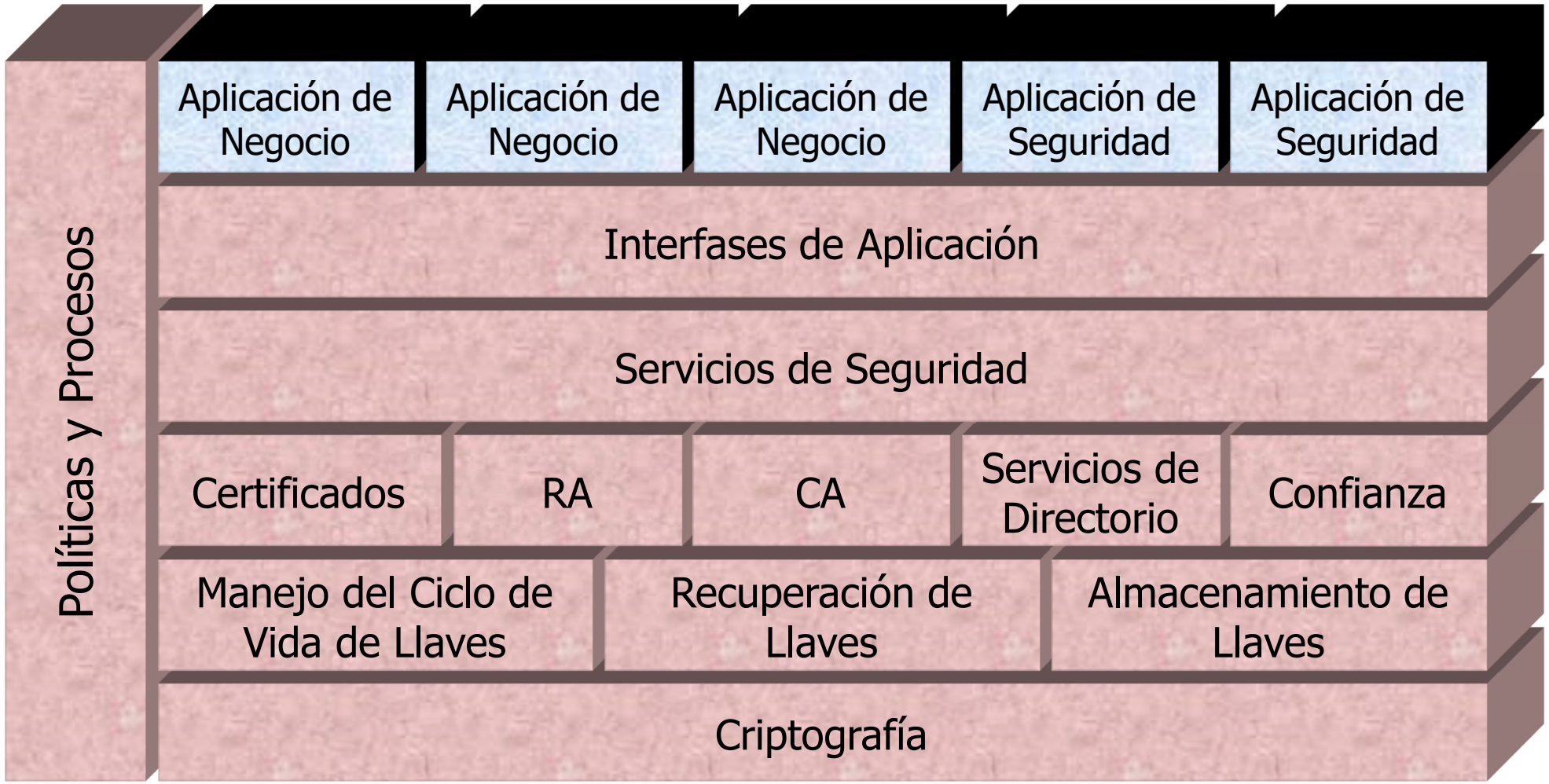
Infraestructura de llave pública (PKI)

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

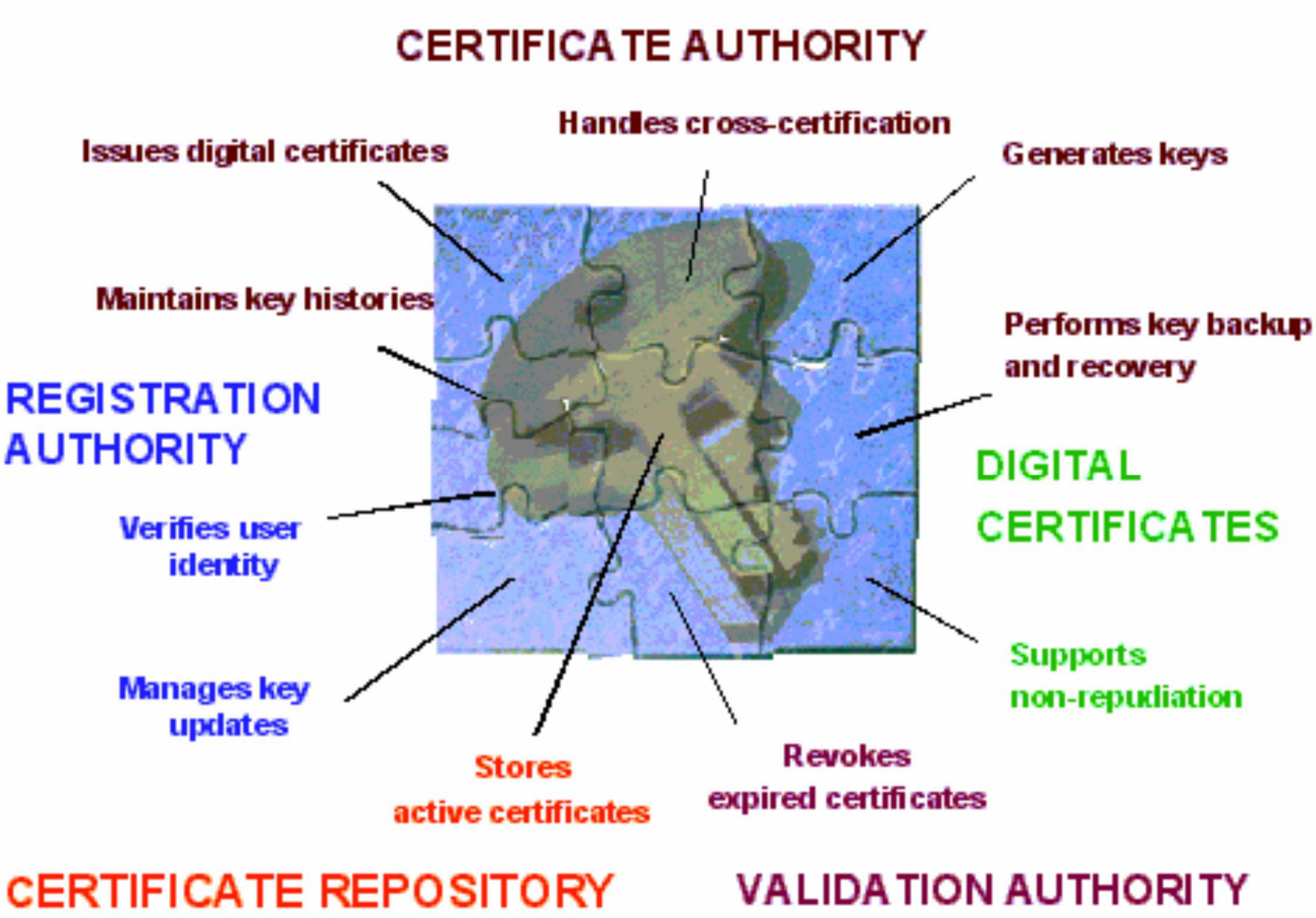
TECNOLÓGICO DE MONTERREY®

Componentes de una PKI



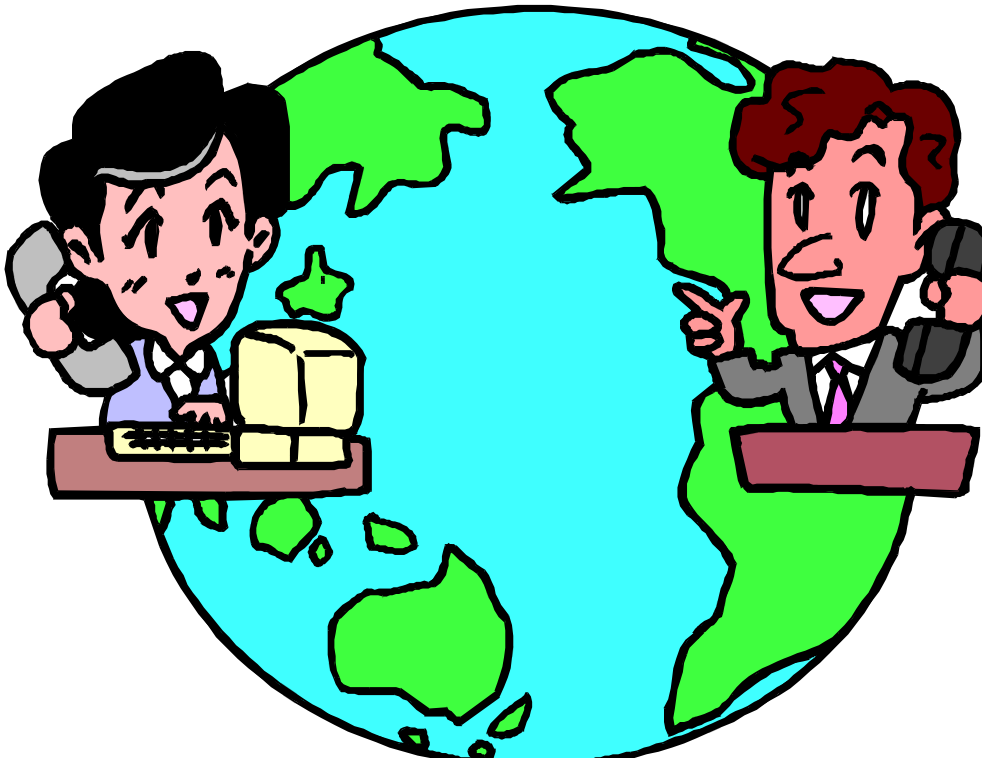
Componentes y funciones de una PKI

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



Criptologia y transmisión datos

Protocolos de transmisión de datos seguros en Internet



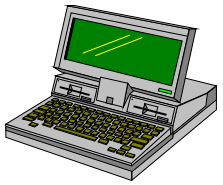
https://www.ssllabs.com/ssltest/

TECNOLÓGICO DE MONTERREY®

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



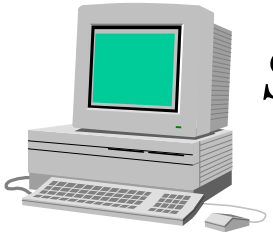
Cliente

Hola

Hola

Como estas

Muy bien



Servidor

No hay autenticación ni privacidad, ni encripción

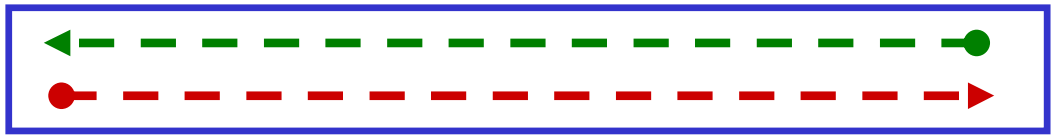
Generando llave simétrica

Quiero pagar

Toma mi llave pública

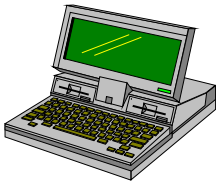
Te envio una llave nueva encriptada con tu llave pública

Hablemos en forma segura

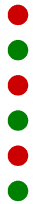


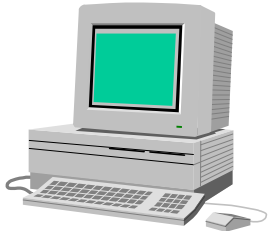
Comunicación encriptada con la llave enviada por el cliente

Otro posible escenario



Cliente



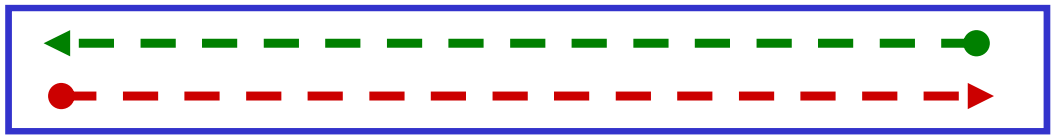


Servidor

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

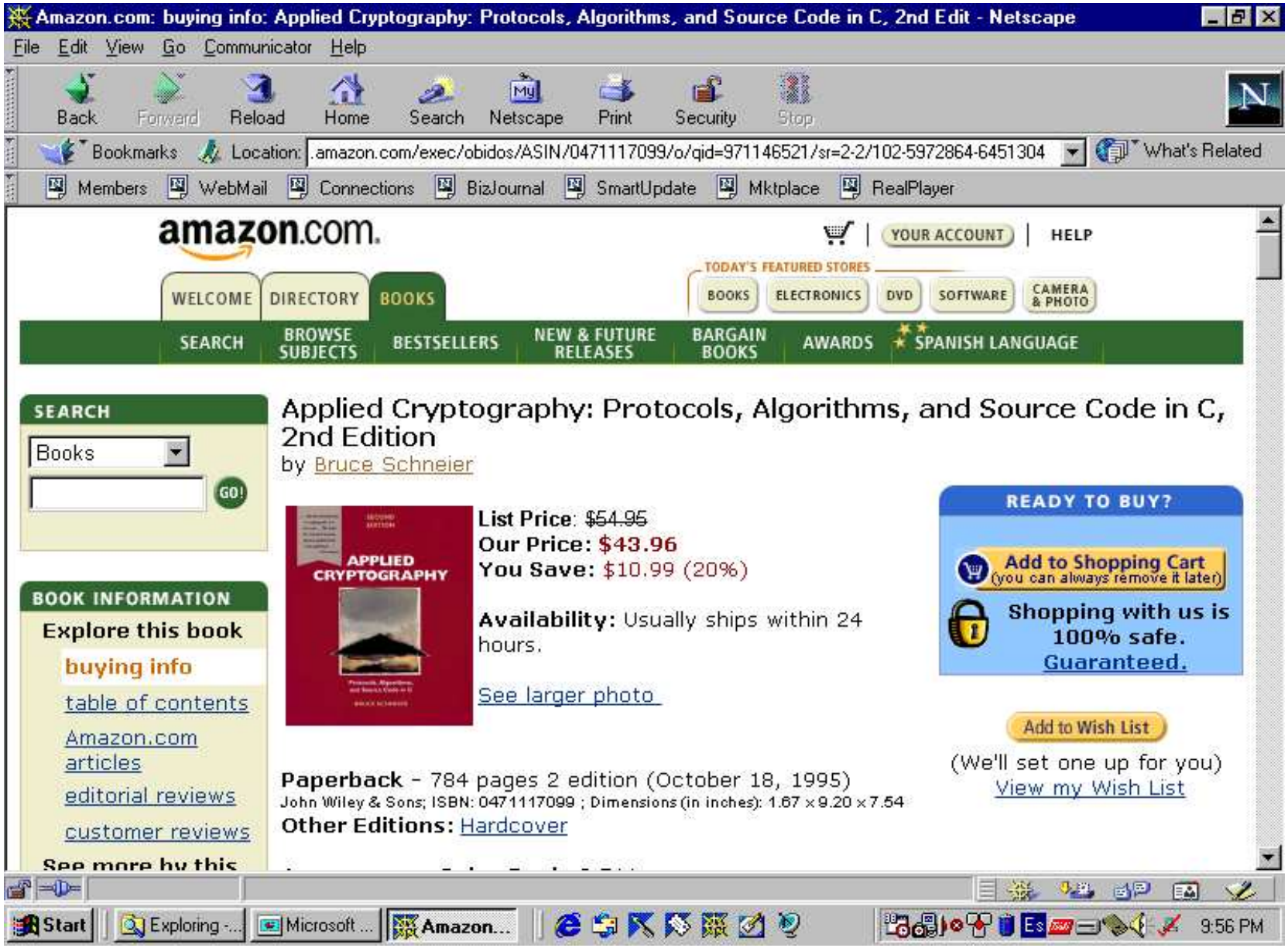
Usando tu llave pública encripte una llave simétrica aleatoria



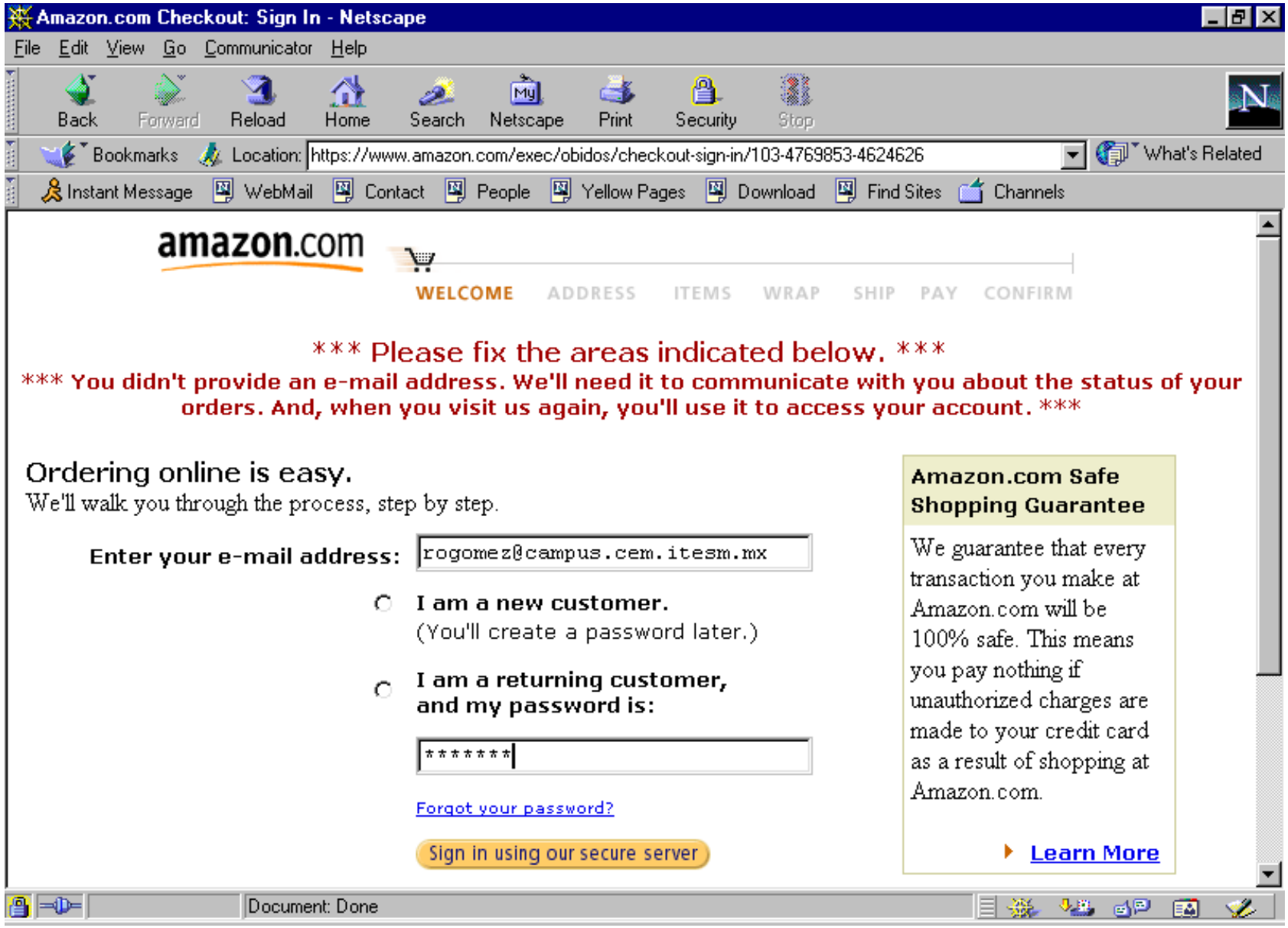
Comunicación encriptada con la llave enviada por el cliente y un hash para autenticación de mensajes

TECNOLÓGICO DE MONTERREY®

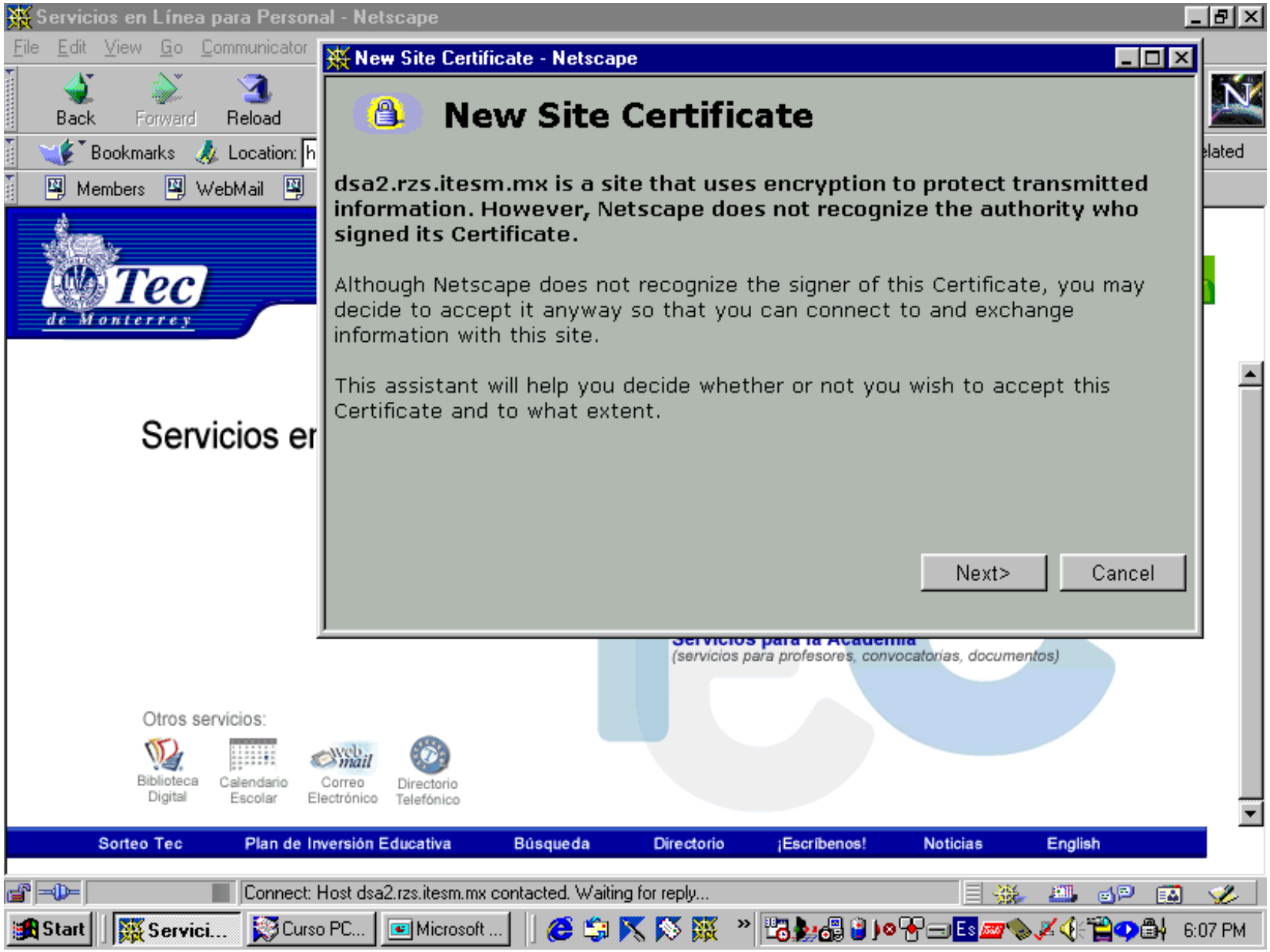
Ejemplo protocolo seguro (1er. paso)

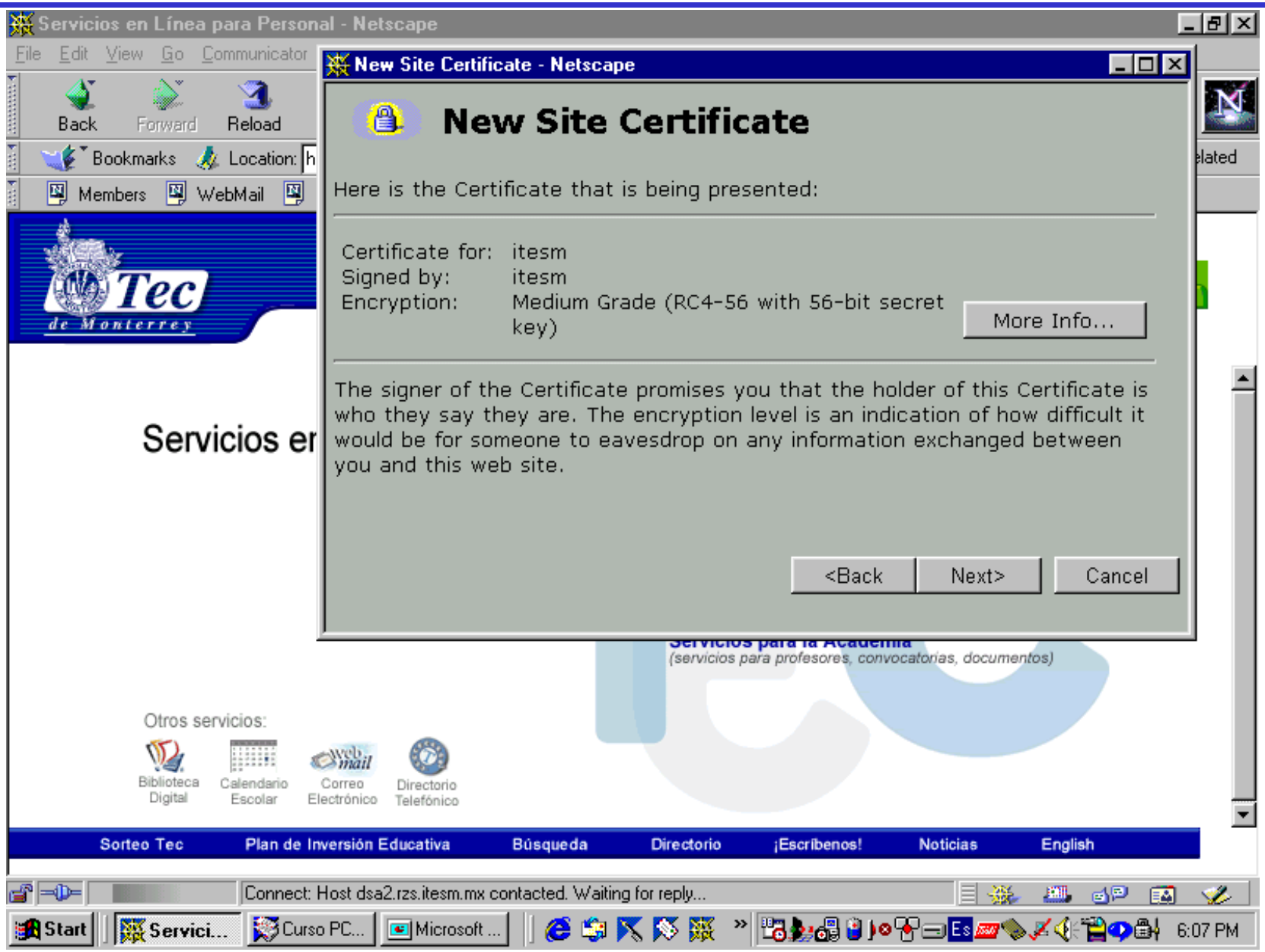


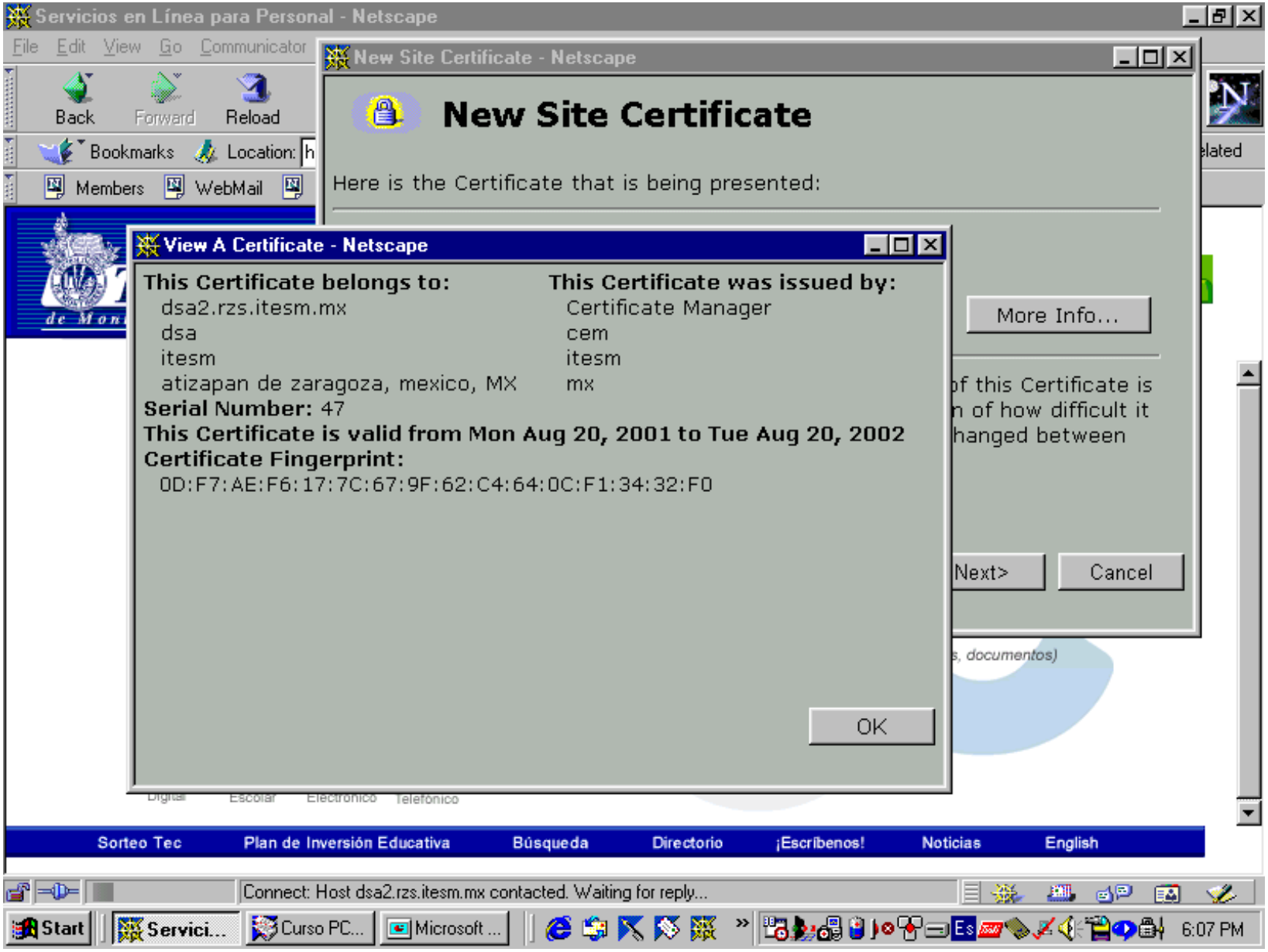
Ejemplo protocolo seguro (2do.paso)

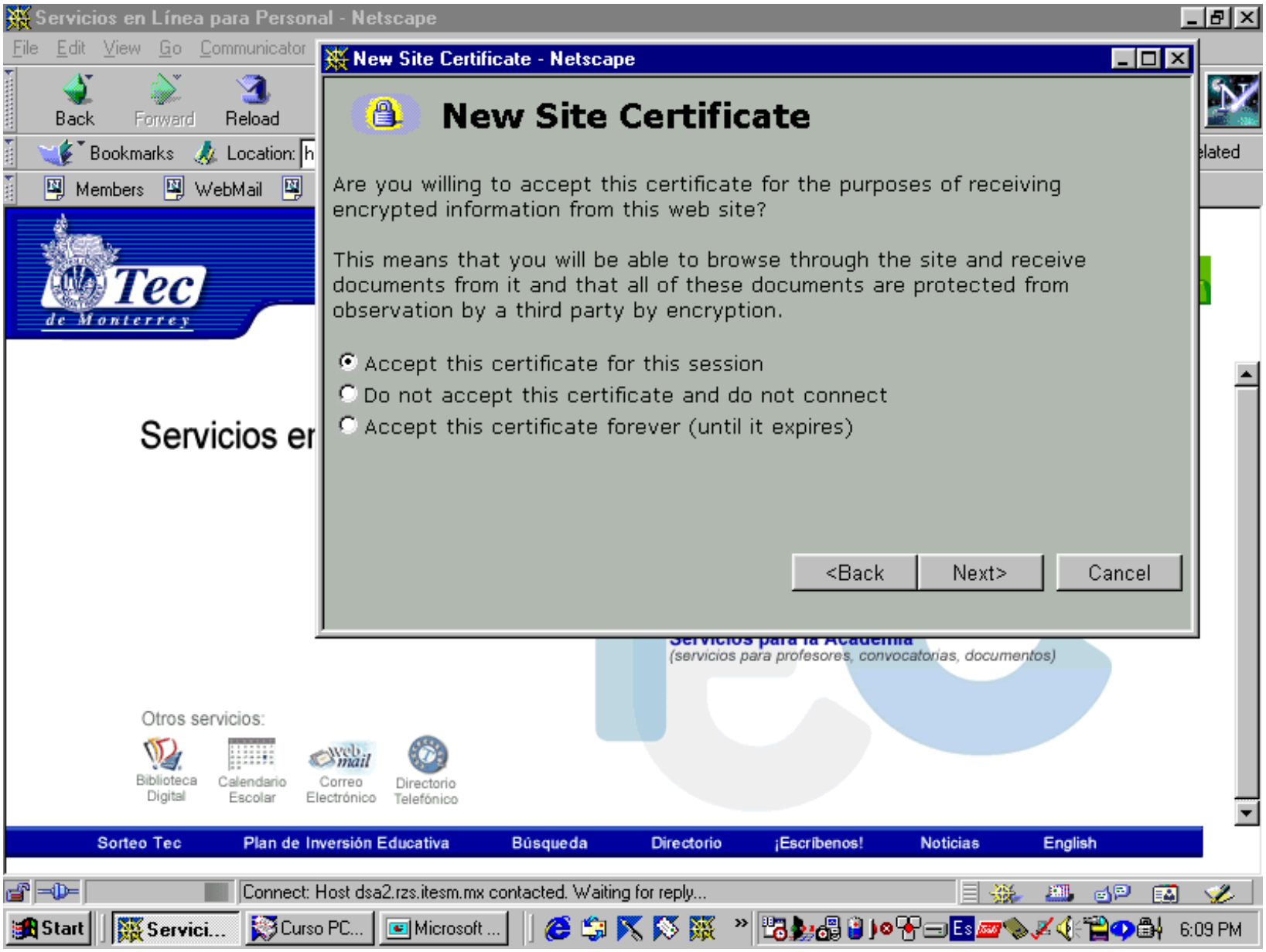


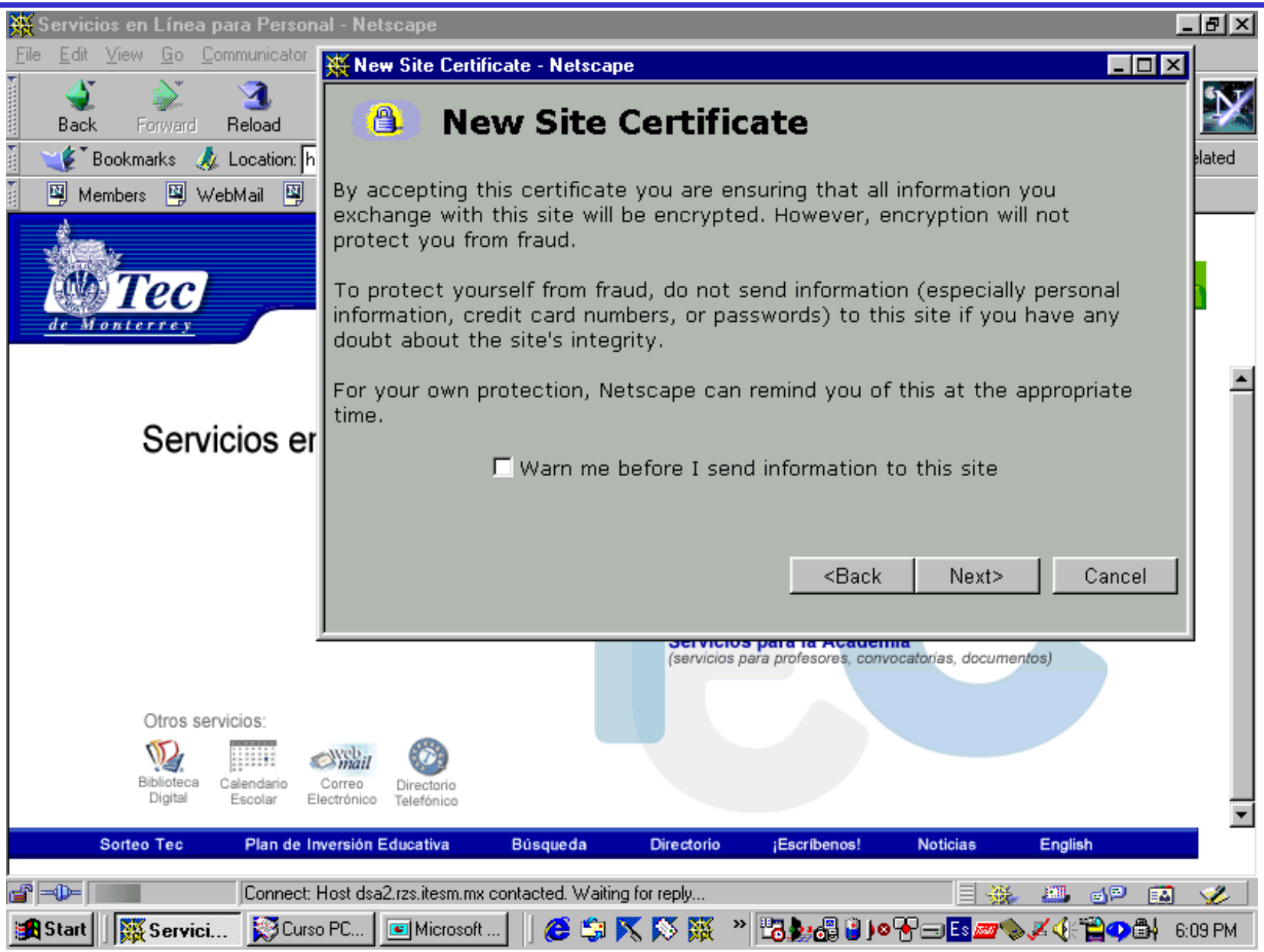
Ejemplo certificado en una página

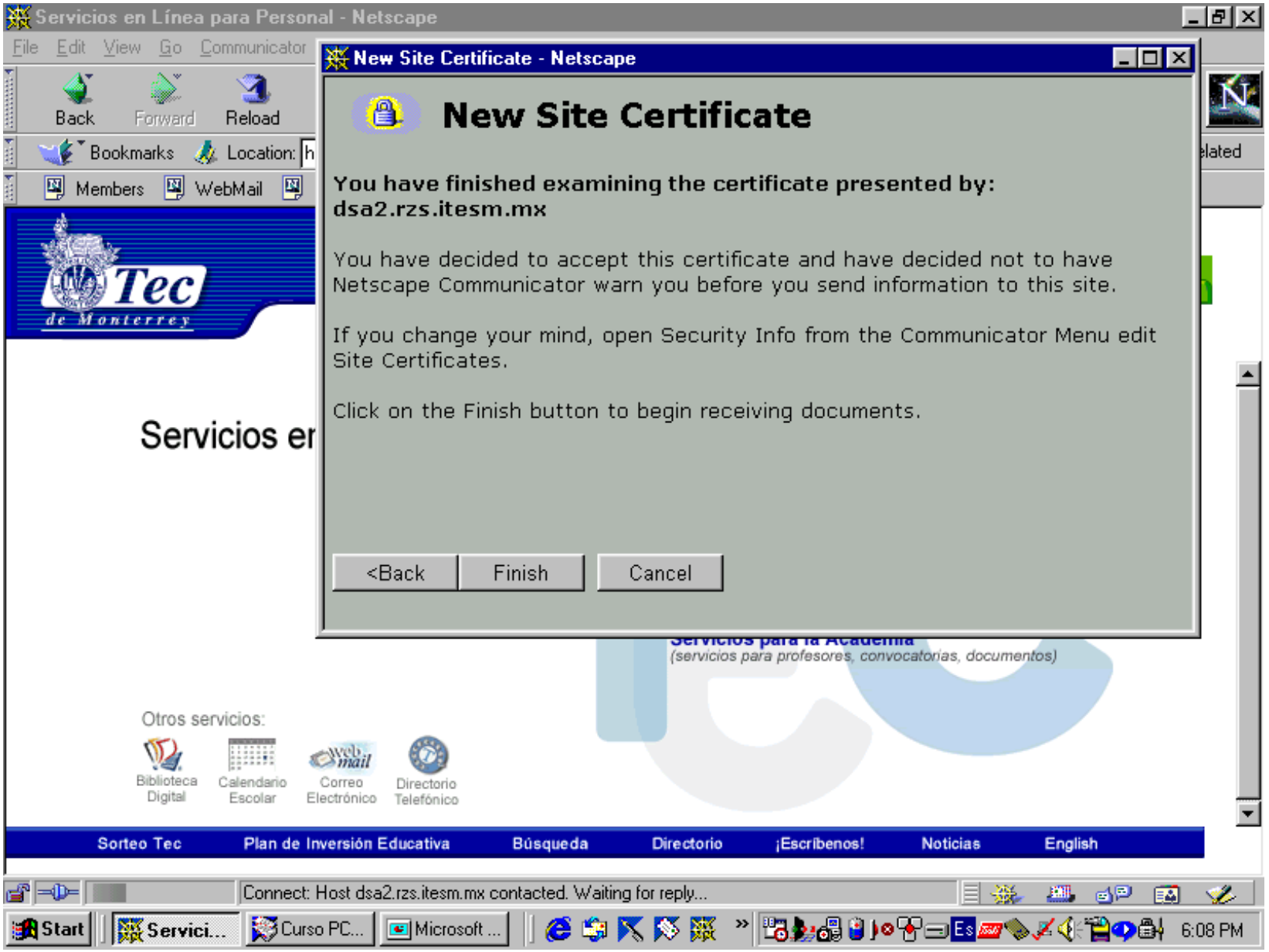


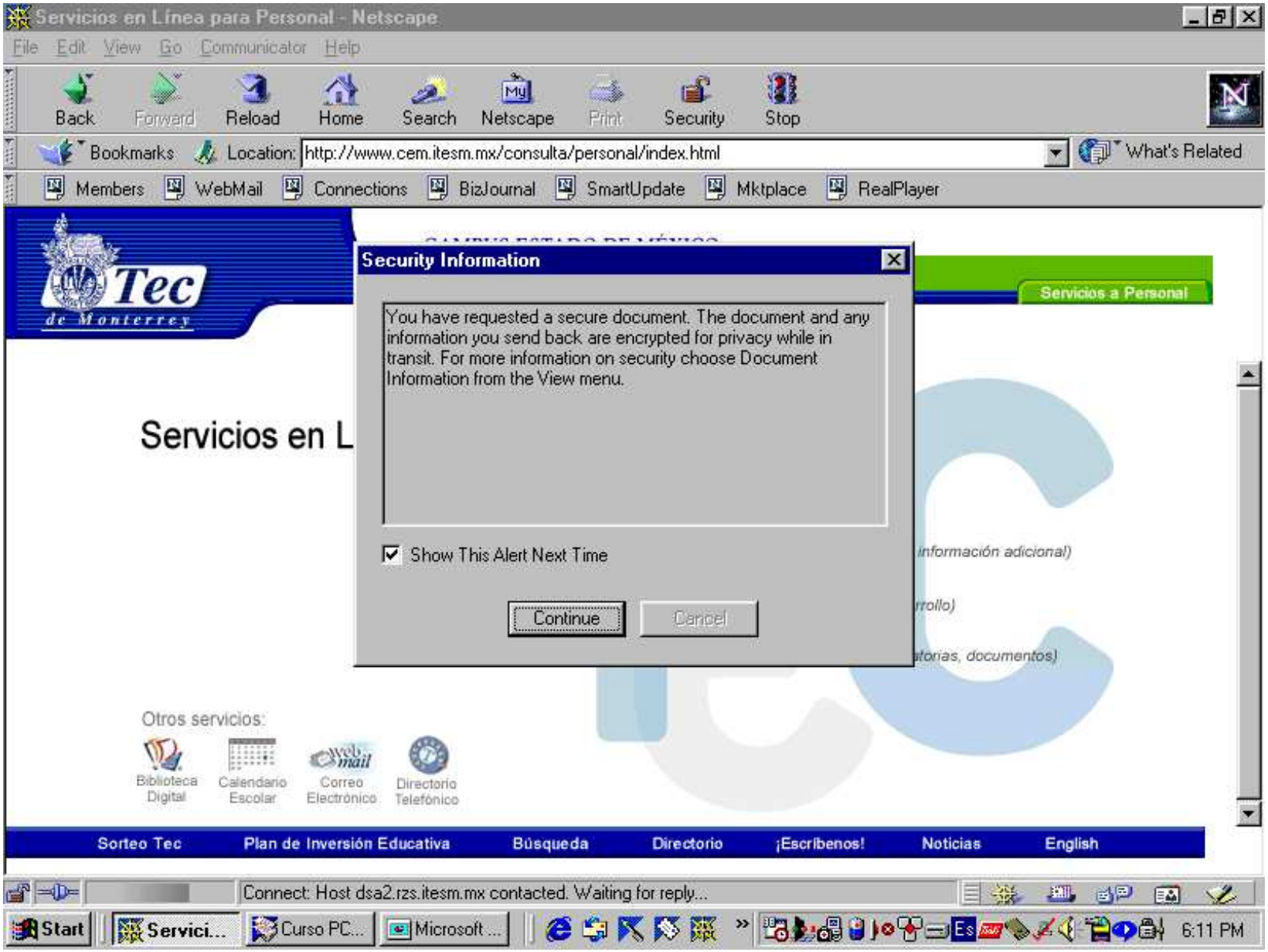

Servicios en Línea para Personal - Netscape
File Edit View Go Communicator
Back Forward Reload
Bookmarks Location:
Members WebMail
New Site Certificate - Netscape
New Site Certificate
Here is the Certificate that is being presented:
Certificate for: itesm
Signed by: itesm
Encryption: Medium Grade (RC4-56 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
¡Escríbenos!
Noticias
English
Connect: Host dsa2.rzs.itesm.mx contacted. Waiting for reply...
Start
Servici...
Curso PC...
Microsoft ...
6:07 PM

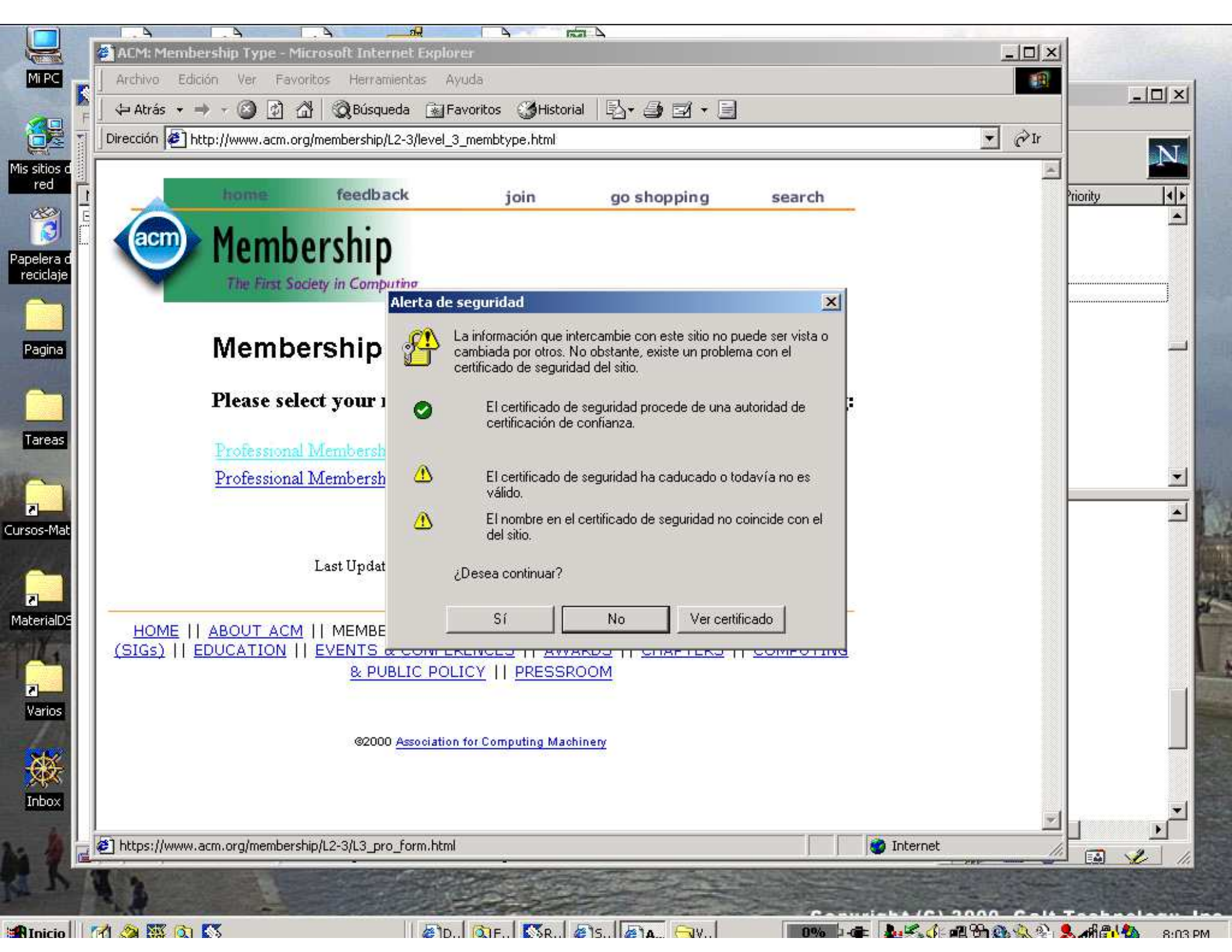

Servicios en Línea para Personal - Netscape
File Edit View Go Communicator
Back Forward Reload
Bookmarks Location:
Members WebMail
New Site Certificate - Netscape
New Site Certificate
Here is the Certificate that is being presented:
More Info...
Next>
Cancel
View A Certificate - Netscape
This Certificate belongs to:
dsa2.rzs.itesm.mx
dsa
itesm
atizapan de zaragoza, mexico, MX
This Certificate was issued by:
Certificate Manager
cem
itesm
mx
Serial Number: 47
This Certificate is valid from Mon Aug 20, 2001 to Tue Aug 20, 2002
Certificate Fingerprint:
0D:F7:AE:F6:17:7C:67:9F:62:C4:64:0C:F1:34:32:F0
OK
Sorteo Tec
Plan de Inversión Educativa
Búsqueda
Directorio
¡Escríbenos!
Noticias
English
Connect: Host dsa2.rzs.itesm.mx contacted. Waiting for reply...
Start
Servici...
Curso PC...
Microsoft ...
6:07 PM


Servicios en Línea para Personal - Netscape
File Edit View Go Communicator
Back Forward Reload
Bookmarks Location:
Members WebMail
New Site Certificate - Netscape
New Site Certificate
Are you willing to accept this certificate for the purposes of receiving encrypted information from this web site?
This means that you will be able to browse through the site and receive documents from it and that all of these documents are protected from observation by a third party by encryption.
Accept this certificate for this session
Do not accept this certificate and do not connect
Accept this certificate forever (until it expires)
<Back
Next>
Cancel
Tec de Monterrey
Servicios er
(servicios para profesores, convocatorias, documentos)
Otros servicios:
Biblioteca Digital
Calendario Escolar
Correo Electrónico
Directorio Telefónico
Sorteo Tec
Plan de Inversión Educativa
Búsqueda
Directorio
¡Escríbenos!
Noticias
English
Connect: Host dsa2.rzs.itesm.mx contacted. Waiting for reply...
Start
Servici...
Curso PC...
Microsoft ...
6:09 PM


Servicios en Línea para Personal - Netscape
File Edit View Go Communicator
Back Forward Reload
Bookmarks Location:
Members WebMail
Tec de Monterrey
Servicios er
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 profesores, convocatorias, documentos)
Otros servicios:
Biblioteca Digital
Calendario Escolar
Correo Electrónico
Directorio Telefónico
Sorteo Tec
Plan de Inversión Educativa
Búsqueda
Directorio
¡Escríbenos!
Noticias
English
Connect: Host dsa2.rzs.itesm.mx contacted. Waiting for reply...
Start
Servici...
Curso PC...
Microsoft ...
6:09 PM


Servicios en Línea para Personal - Netscape
File Edit View Go Communicator
Back Forward Reload
Bookmarks Location:
Members WebMail
Tec de Monterrey
Servicios er
New Site Certificate - Netscape
New Site Certificate
You have finished examining the certificate presented by:
dsa2.rzs.itesm.mx
You have decided to accept this certificate and have decided not to have Netscape Communicator warn you before you send information to this site.
If you change your mind, open Security Info from the Communicator Menu edit Site Certificates.
Click on the Finish button to begin receiving documents.
<Back
Finish
Cancel
(servicios para profesores, convocatorias, documentos)
Otros servicios:
Biblioteca Digital
Calendario Escolar
Correo Electrónico
Directorio Telefónico
Sorteo Tec
Plan de Inversión Educativa
Búsqueda
Directorio
¡Escríbenos!
Noticias
English
Connect: Host dsa2.rzs.itesm.mx contacted. Waiting for reply...
Start
Servici...
Curso PC...
Microsoft ...
6:08 PM


Servicios en Línea para Personal - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://www.cem.itesm.mx/consulta/personal/index.html What's Related
Members WebMail Connections BizJournal SmartUpdate Mktplace RealPlayer
Tec de Monterrey
Servicios a Personal
Security Information
You have requested a secure document. The document and any information you send back are encrypted for privacy while in transit. For more information on security choose Document Information from the View menu.
Show This Alert Next Time
Continue
Cancel
Servicios en L
Otros servicios:
Biblioteca Digital
Calendario Escolar
Correo Electrónico
Directorio Telefónico
Sorteo Tec
Plan de Inversión Educativa
Búsqueda
Directorio
¡Escríbenos!
Noticias
English
Connect: Host dsa2.rzs.itesm.mx contacted. Waiting for reply...
Start
Servici...
Curso PC...
Microsoft ...
6:11 PM


ACM: Membership Type - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Historial
Dirección http://www.acm.org/membership/L2-3/level_3_membtype.html
Ir
home feedback join go shopping search
acm
Membership
The First Society in Computing
Membership
Please select your
Professional Membersh
Professional Membersh
Last Updat
HOME || ABOUT ACM || MEMBE
(SIGs) || EDUCATION || EVENTS
& PUBLIC POLICY || PRESSROOM
©2000 Association for Computing Machinery
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?
Sí
No
Ver certificado
https://www.acm.org/membership/L2-3/L3_pro_form.html
Internet
Mi PC
Mis sitios de red
Papelera de reciclaje
Pagina
Tareas
Cursos-Mat
MaterialDS
Varios
Inbox
Priority
Inicio
8:03 PM

TECNOLÓGICO DE MONTERREY®

Introducción a la criptologia

Roberto Gómez Cárdenas

rogomez@itesm.mx

http://cryptomex.org