

LOS DELITOS CIBERNÉTICOS Y LA COMPUTACIÓN FORENSE

Criptología y Esteganografía

Roberto Gómez Cárdenas

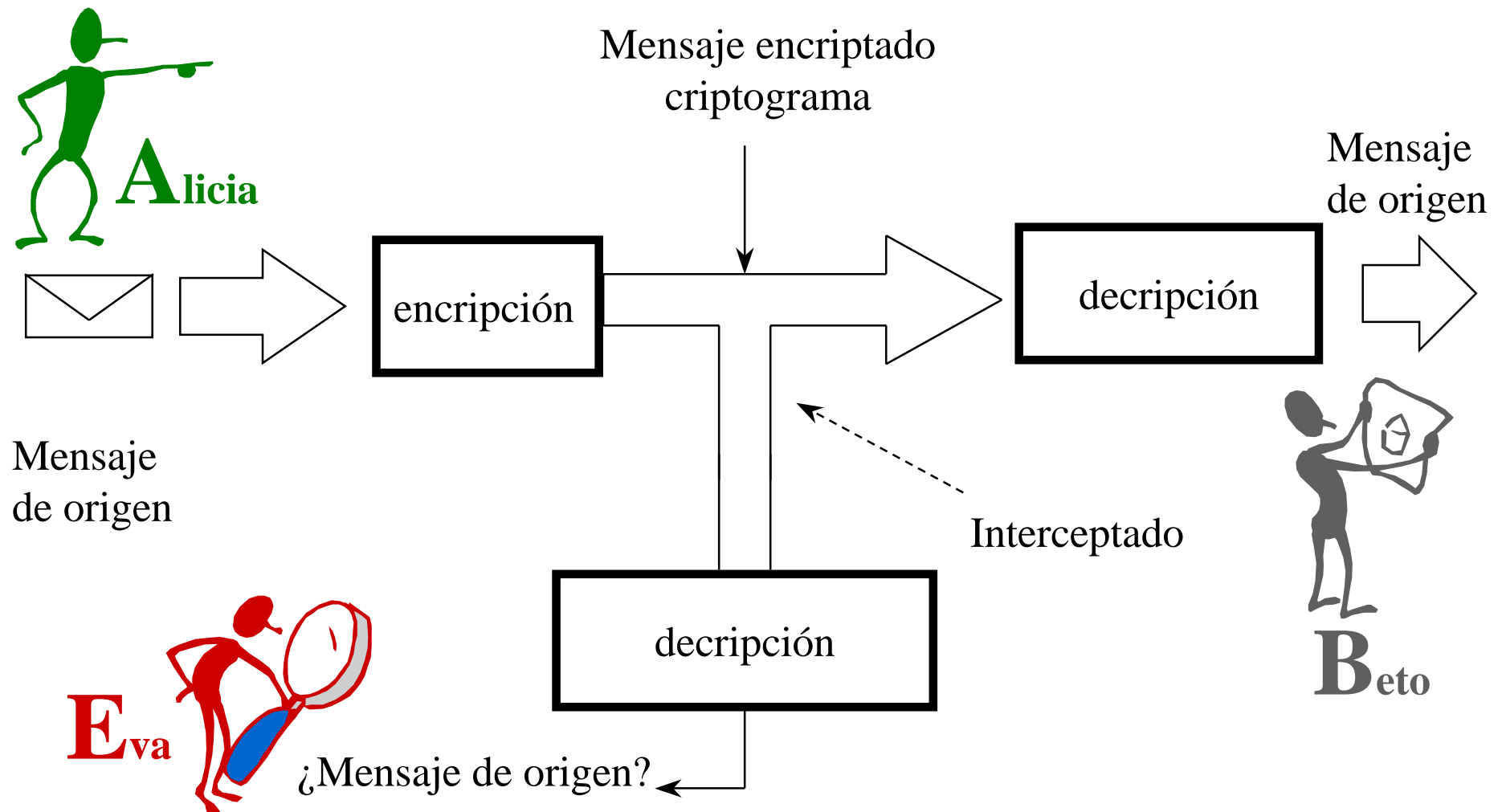
`rogomez@itesm.mx`

<http://campus.cem.itesm.mx/ac/rogomez>

La criptología

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

Proceso encriptación/decriptación

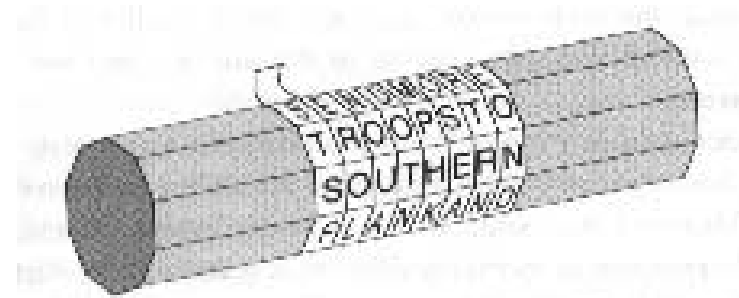


Criptografía y seguridad

- 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 un tiempo de cálculo en años que excede cualquier valor razonable.”*
- Objetivos
 - mantener la confidencialidad del mensaje la información contenida en el mensaje permanezca secreta
 - garantizar la autenticidad tanto del mensaje como del par remitente/destinatario

Procedimientos clásicos de encriptación

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



Mensaje: SENDMORETROOPSTOSOUTHERNFLANKAND...
Criptograma: STSFEROLNOUADOTNMPHKOSEARTRNEOND

Ejemplo transposición: “rail fence”

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

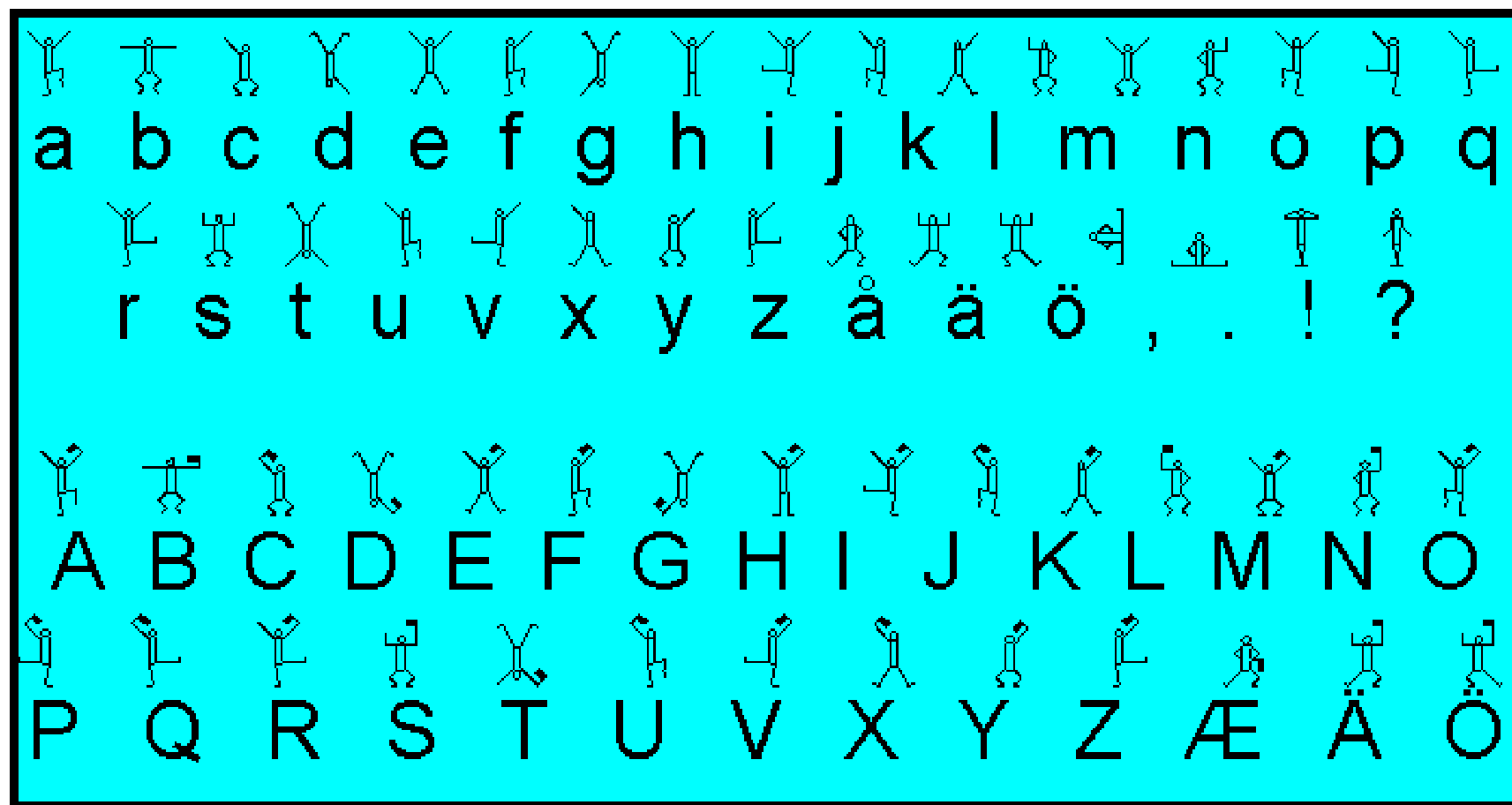
hola \longrightarrow **h l**
o a

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

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

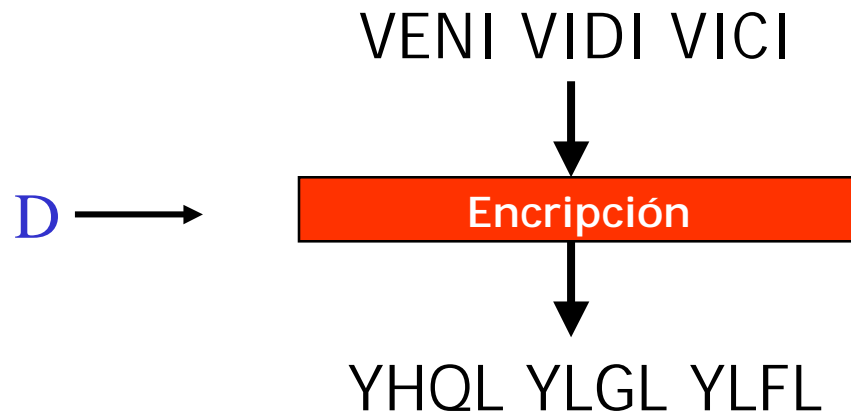
- criptograma: **mematrhtgpryeteftaoaat**

Criptosistema de Adventures Dancing Men



Ejemplos substitución: Cesar y Vigenere

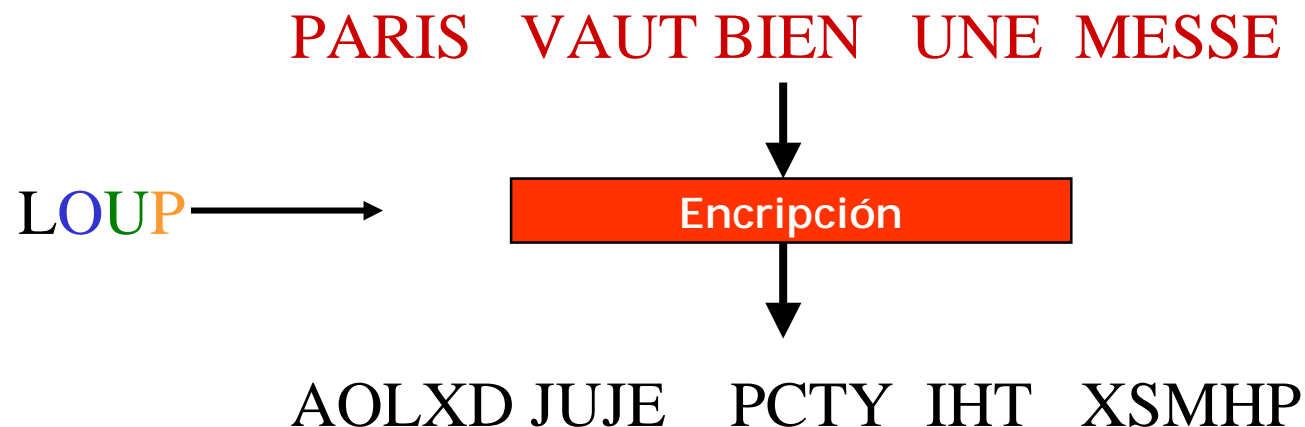
Criptosistema Cesar:



CAESAR'S CIPHER

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

Criptosistema Vigenere:



Otros criptosistemas clásicos

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

Encriptando con una computadora

- La computadora “*maneja*” números en lugar de letras
 - solo números binarios (digitos binarios = bits)
- $a = 1100001$
 $! = 0100001$
 $\& = 0100110$
- La encriptación se realiza bajo mismo principio de sustitución y transposición
 - elementos del mensaje son substituidos por otros elementos, o sus posiciones son intercambiadas o ambas

Encriptación por computadora

- Convertir mensaje a ASCII

Texto claro:

HELLO = 1001000 1000101 1001100 1001100 1001111

- Transposición: intercambiar las letras en un orden predeterminado

Texto claro:

HELLO = 10010001000101100110010011001001111

Criptograma:

LHOEL = 10011001001000100111110001011001100

- La transposición puede darse a nivel de bits

Letra original: 1001000

Letra encriptada: 0010010

Utilizando una llave

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

DAVID = 1000100 1000001 1010110 1001001 1000100

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

Texto claro: HELLO

Texto ASCII: 10010001000101100110010011001001111

Llave: 10001001000001101011010010011000100

Criptograma: 00011000000100001101000001010001011

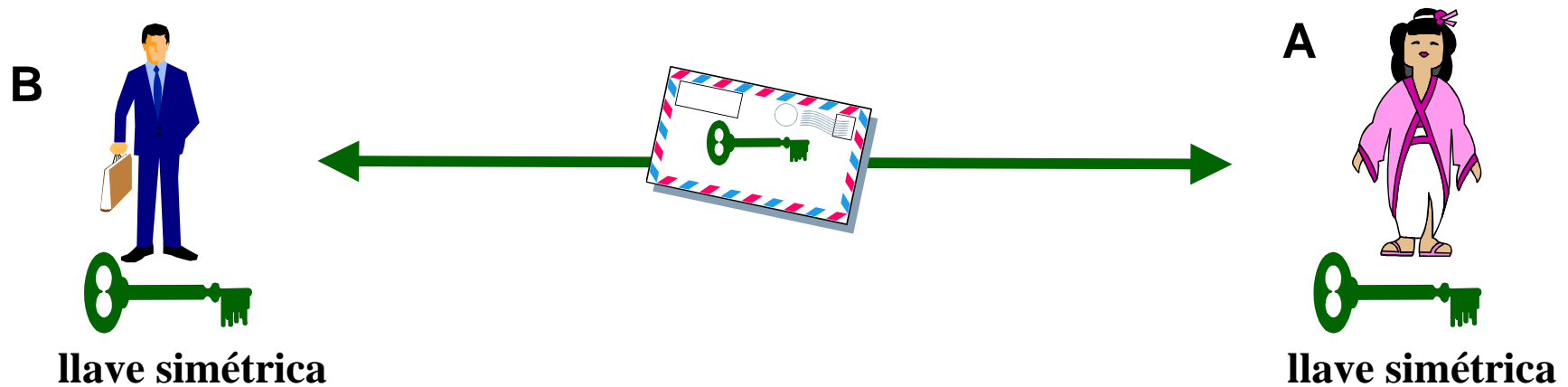
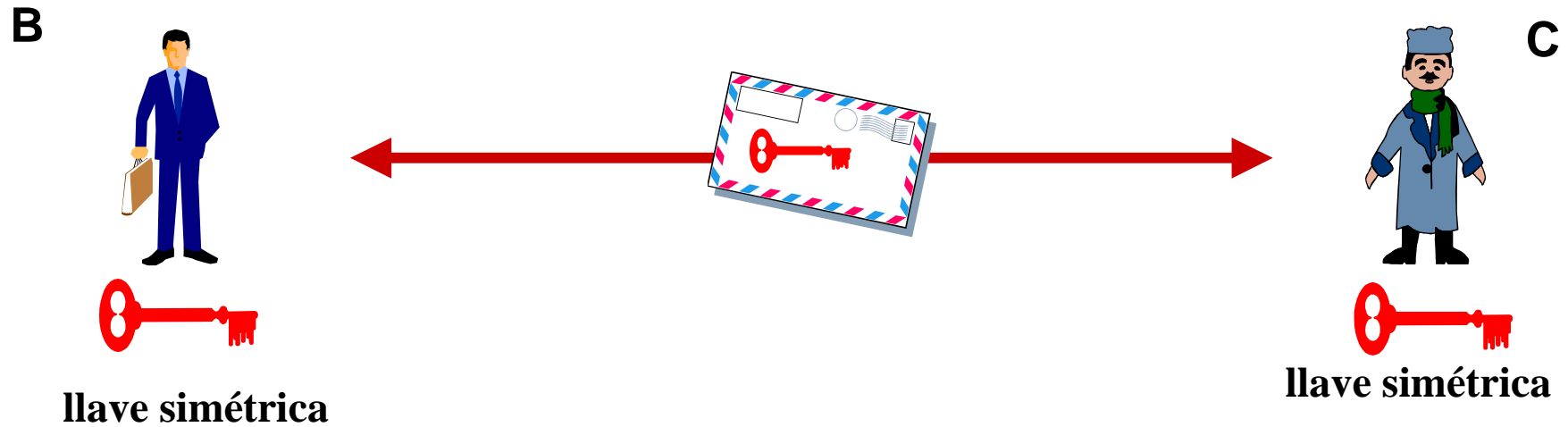
Métodos criptográficos modernos

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

Sinónimos métodos

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

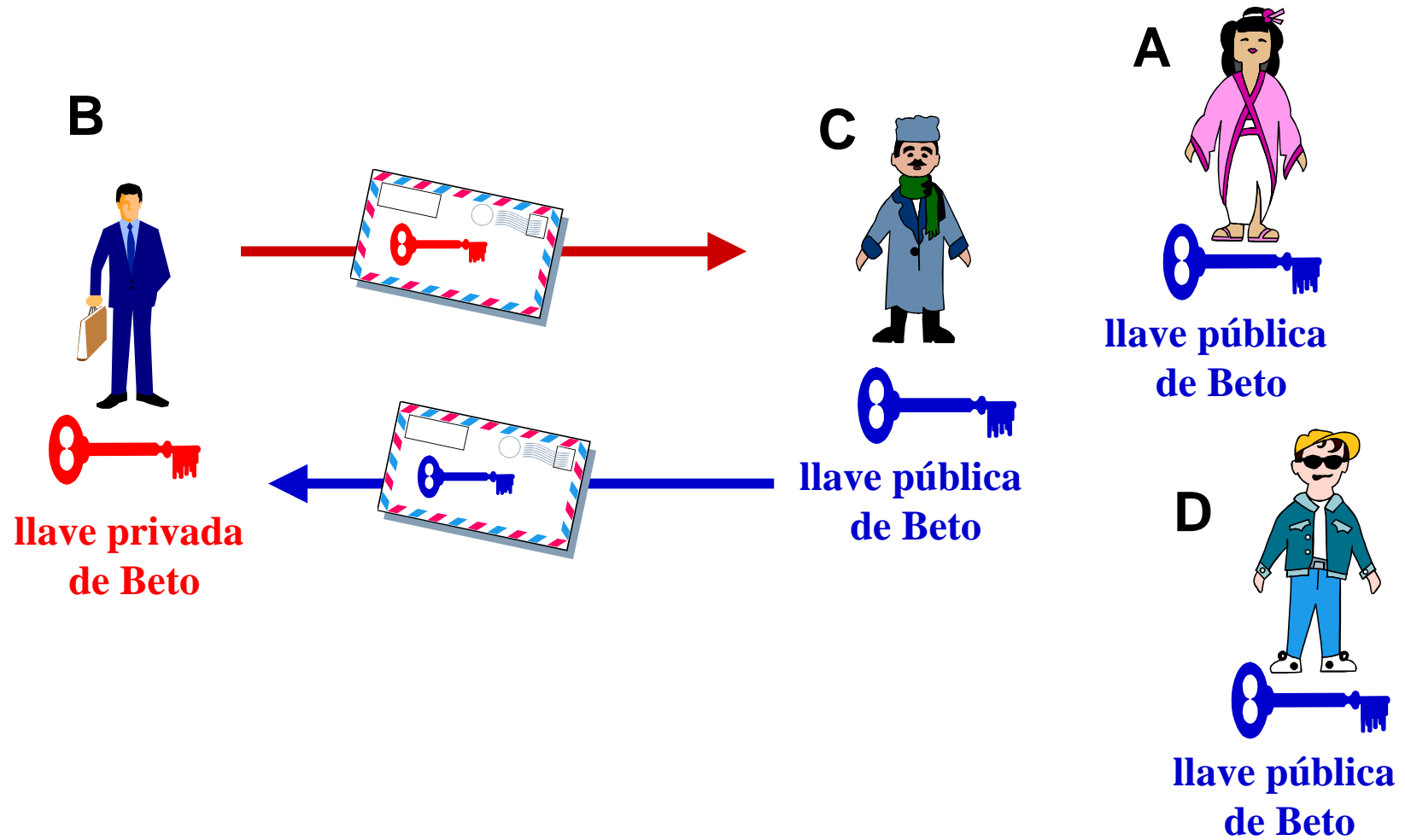
Esquema general encriptación llave secreta



Desventajas llave secreta

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

Criptograma llave pública (asimétrico)



Ejemplo de una llave pública



Oliver Roberts - My PGP Public Key - Netscape

File Edit View Go Communicator Help

Bookmarks Location: <http://www.nanunanu.org/~oliver/pgpkey.html> What's Related

PGP Public Key

SOFTWARE

- WarpJPEG
- WarpPNG
- xpkBZP2
- SoloControl
- SoloUp
- F1GP-Ed
- SnapshotF1GP
- f1gp.library
- ButtonMenu
- CDRun
- ARexx Scripts

Buy from **HiSOFT**

[IBrowse 2.2](#)
[DOpus Magellan II](#)
[MakeCD](#)

W3C HTML 4.01

My PGP Public Key

If you want to add my PGP public key to your PGP keyring, then it may be easier if you download my key as a separate [ASCII text file](#).

PRIVACY Now! PGP

Type	Bits/KeyID	Date	User ID
pub	1024/8C0C5D61	1996/07/20	Oliver Roberts <oliver@futura.co.uk>
			Oliver Roberts <oliver.roberts@iname.com>
			Oliver Roberts <oliver@nanunanu.org>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i

```
mQCNAzHxRgUAAAEEMiIn19TTDRUFVB2vhYUm4hgzi0f29b/s/YA6L8gSEKSEJWs
SkZZewdQkcjAfzS3Fk1PZjwFkKD0Q7pCd2GBnN/TnGS1fupVB3ydkspodPlhU4iD
y8lao2hfEy9bHScI5lKu9DhGXUZGurz3m3NEoYoYtGiAEEZk9N37cgqaMDFlhAAUR
tCVPbG12ZXIqUm9iZXJ0cyA8b2xpdVYQZ1dGF1cmEuY28udWs+iQCVAwUQOTZL
BH7cgqaMDFlhAQF2ogP/Vrsiumv704zfkg3+ruvzXwNwUQ1ecmAJd0kPrR/5VOYR
8tHmDb/eWhv8t8TUeu6b833SWAsZnT3mbLYAyyioJV10wekRx1VNxQIQpaXUbf3+
sjNw+QKLCFJbqlpUEPKpwYCo9Kwx10XpoUTFb0eJ4Pm0kLo/yYaczq6M1WaaGa0
KU9saXZ1ciBSb2J1cnRzIDxvbg12ZXIucm9iZXJ0c0BpbmFtZS5jb20+iQCVAwUQ
NXSGMH7cgqaMDFlhAQFcXAQAg2gZ017KmOD78BAqyqAoXh/v0lrrshJqW30BknCY
2XsHFaCgw6NjpEgOn0h40NQx69K4jinzH/v7emyRs9BXsaDhELN6BwduwIGwcnF
TwIp2HomjvhtCxf5mKR66qN9GLAhQWQjWZ86xQALMw5RoBD4cjAr7VsJF0ir8XHA
0j+0JE9saXZ1ciBSb2J1cnRzIDxvbg12ZXJAbmFudW5hbnUub3JnPokA1QMFEDVO
iHB+3IKmjAxdYQEBMgOEALxjx9PpRjwTrFyIKX7bnTLK7KBuA0K0YyPx15dRn/Qf
5x1aLxGlsjRxTxSvBlUKESiEiVbaGkPXBEIPuXVTG15BoktA+sX3/vthYfyfR00a
9XGOCMxiJh7QUMDb6s4awA8tEkuP4iS96GsaTBYwiI3q6z4k5YblhoezXt4+ezy
=EWwi
```

-----END PGP PUBLIC KEY BLOCK-----

Document: Done

Start | Ex... | Mi... | Dr... | O... | Ne... | 9:51 PM

Las funciones hash

- Basadas en el concepto de funciones de un solo sentido (one-way hash function)
 - función toma una variable de tamaño variable (cientos o miles de bits) y una salida de tamaño fijo (p.e. 160 bits)
- Función asegura que, si la información es cambiada (aún en sólo un bit) un valor completamente diferente es producido.
- También se conocen como compendio de mensajes o digestión.

Ejemplo función hash: MD5

rogomez@armagnac:464>more toto
ULTRA SECRETO

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

Atte;

RGC

rogomez@armagnac:465>md5 toto

MD5 (toto) = 0c60ce6e67d01607e8232bec1336cbf3

rogomez@armagnac:466>

rogomez@armagnac:467>more toto
ULTRA SECRETO

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

Atte

RGC

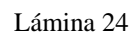
rogomez@armagnac:468>hash1 toto
MD5 (toto) = 30a6851f7b8088f45814b9e5b47774da
rogomez@armagnac:469>

Otras funciones hash de un solo sentido

- Algoritmo MD2
- Algoritmo MD4
- SHA-1
- RIPE MD-160
- HMAC
- N-Hash
- Havalk

La huella digital

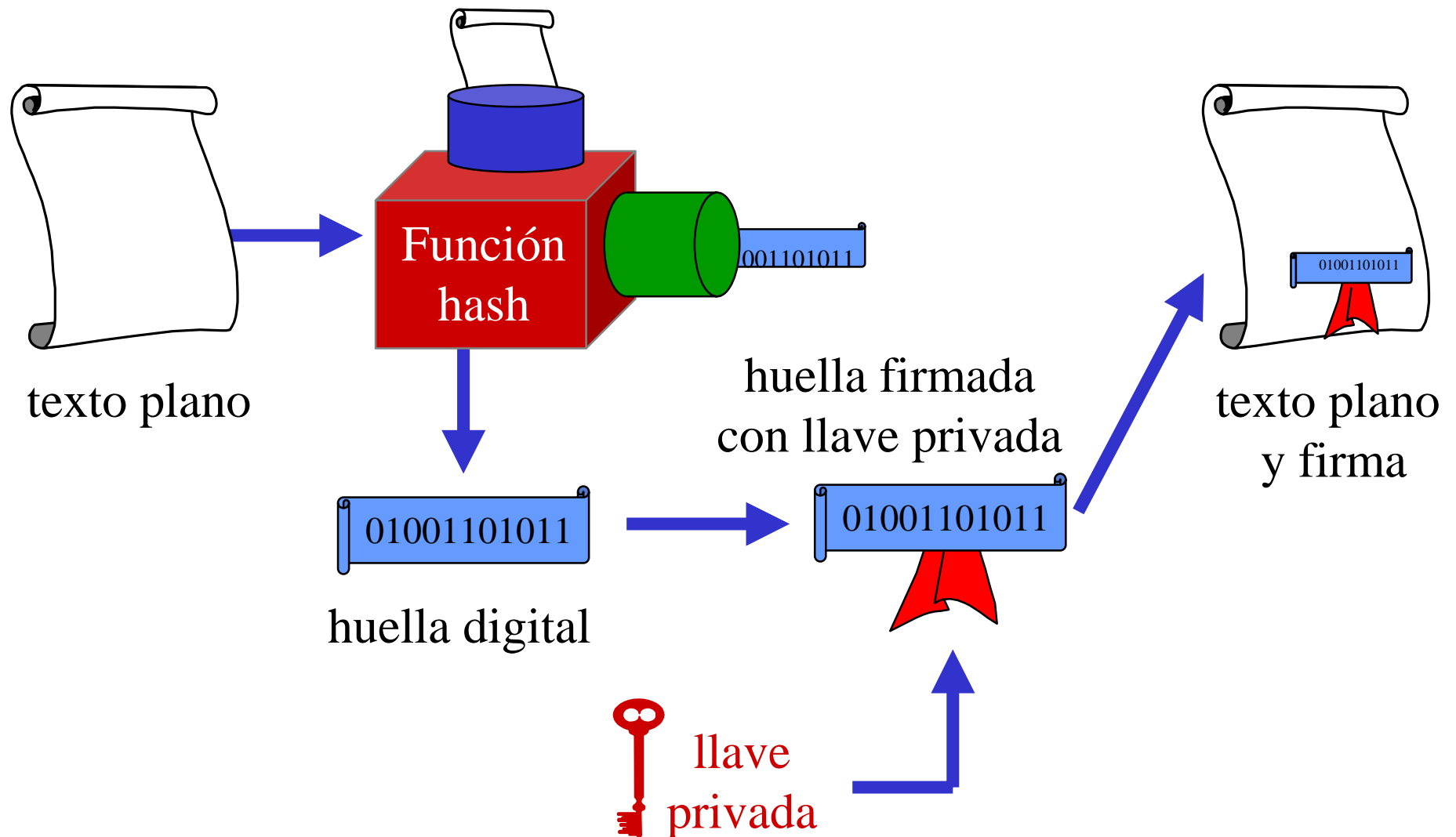
- La salida producida por una función hash aplicada a un documento, es conocida con el nombre de huella digital de dicho documento
- Cualquier cambio en el documento produce una huella diferente
- Huella digital también es conocida como compendio de mensaje (cuando el documento es un mensaje)



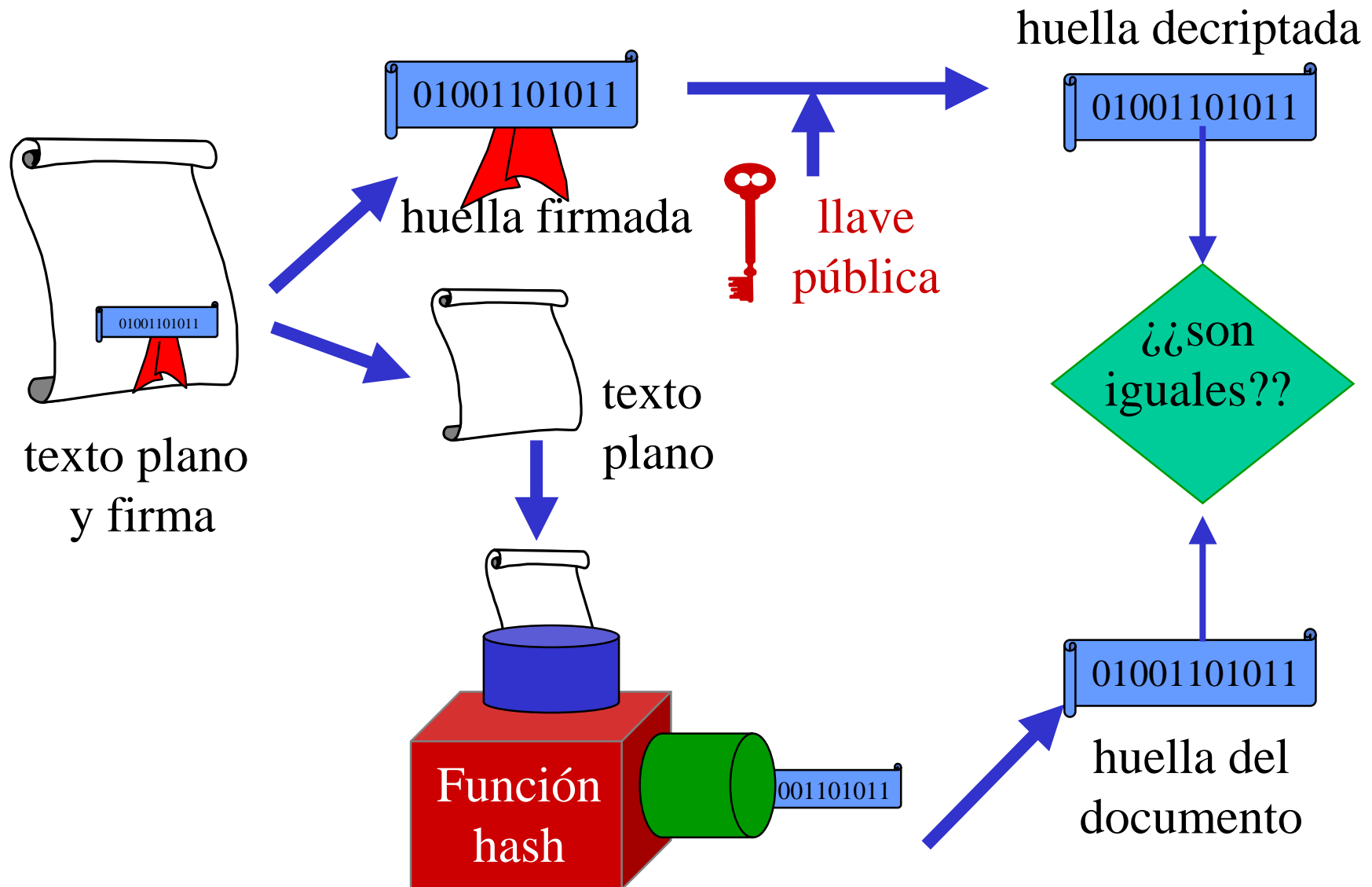
Firmas y huellas digitales

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

Firma digital segura (envío)



Firma digital segura (recepción)



Solicitando una llave pública

Alicia

Alicia va a pagarle
100 pesos a Beto

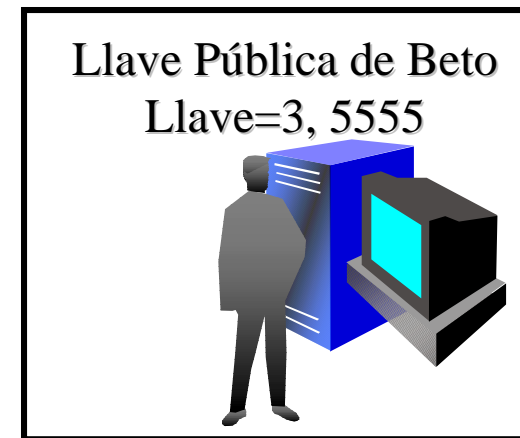


“Solicita la Llave
Pública de Beto”

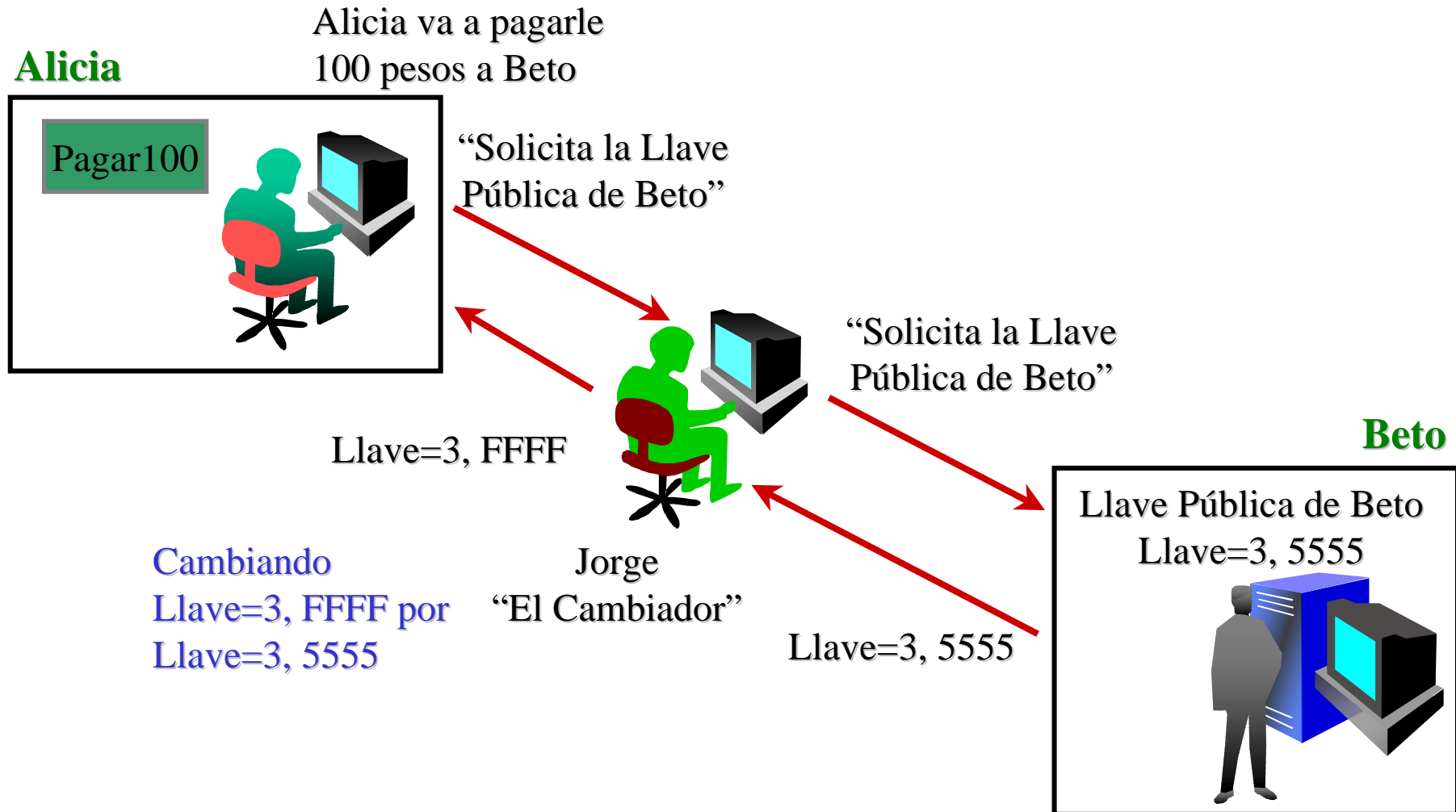
Entregando llave
públic de Beto
Llave=3, 5555

Beto

Llave Pública de Beto
Llave=3, 5555



El ataque “Man in the Middle” (MIM)



Los Certificados Digitales

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

Ejemplo Certificado Digital

This Certificate belongs to: Anish Bhimani WebPass ID - Netscape Netcenter www.verisign.com/repository/CPS Incorp. by Ref.,LLAB.LTD(c)96 www.verisign.com/RPA Incorp. By Ref. LLAB. LTD. (c) 97 VeriSign VeriSign Web Site Access CA VeriSign Inc.	This Certificate was issued by: www.verisign.com/RPA Incorp. By Ref. LLAB. LTD. (c) 97 VeriSign VeriSign Web Site Access CA VeriSign Inc.
Serial Number: 5D:63:E8:85:5D:F7:B9:E6:C6:37:C6:BE:41:01:8C:6C	
This Certificate is valid from Fri Sep 26, 1997 to Tue Sep 25, 2007	
Certificate Fingerprint: 43:9B:60:10:DA:F2:EF:B6:F1:55:D1:00:4C:AD:18:3C	
Comment: This certificate incorporates the VeriSign Certification Practice Statement (CPS) by reference. Use of this certificate is governed by the CPS.	
<input type="button" value="OK"/>	

Autoridades Certificadoras (CAs)

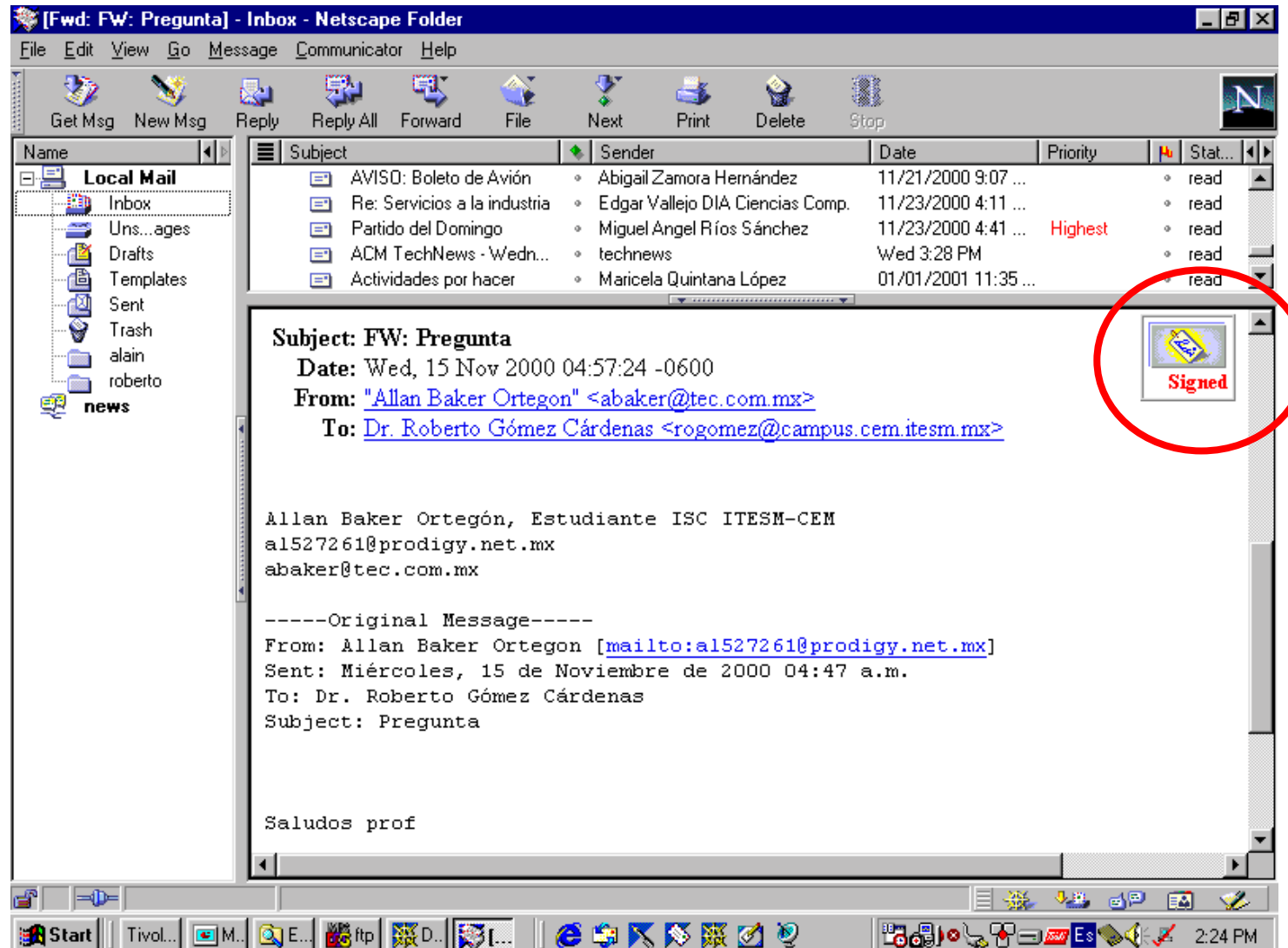
- Los certificados son expedidos por autoridades confiables conocidas como *Autoridades Certificadoras*, (CA por sus siglas en inglés).
- Estas entidades son responsables de certificar la identidad de un individuo y su posesión de una llave pública.
- Generan y administran certificados y los publican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

Infraestructura de llave pública (PKI)

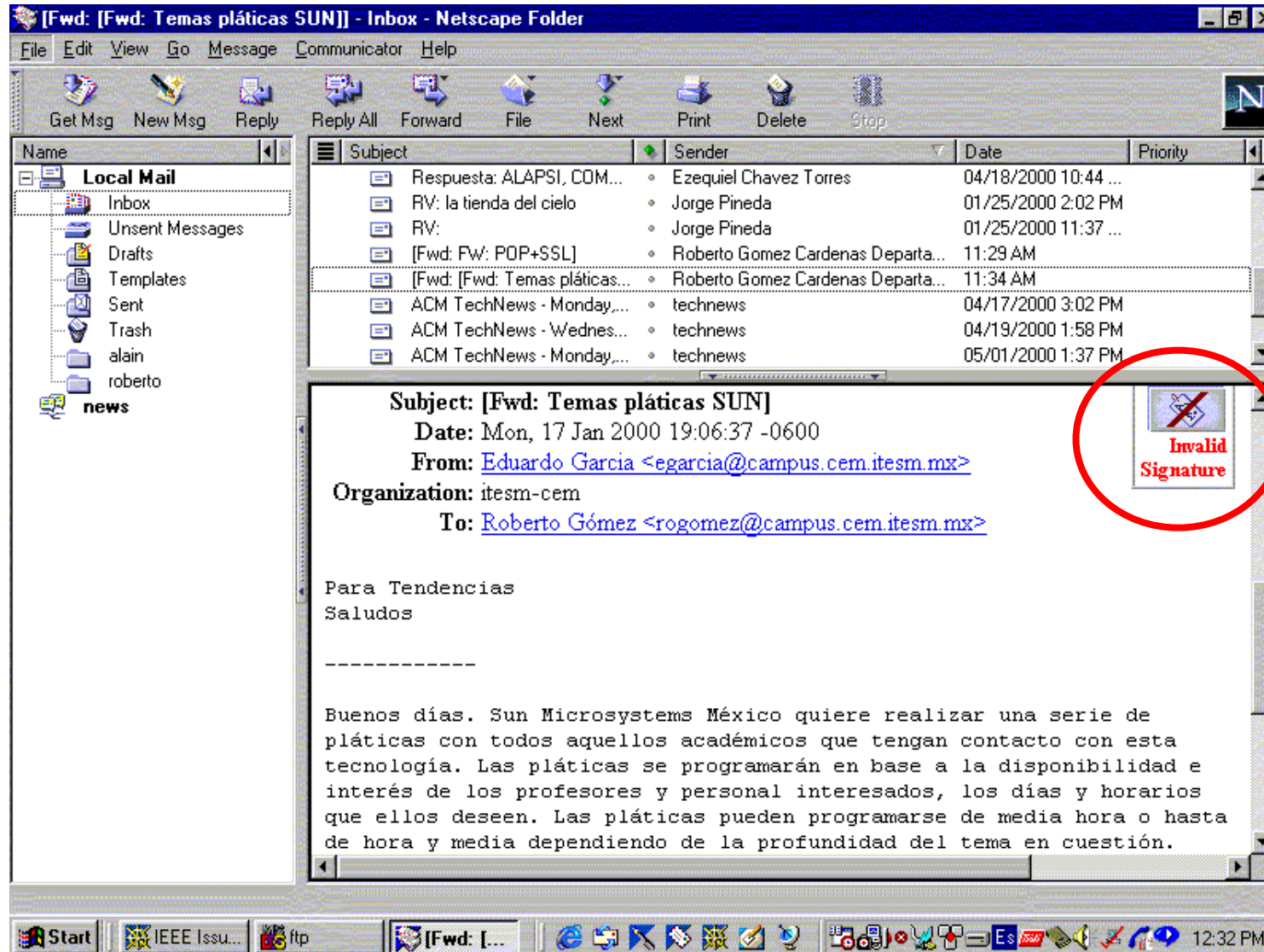
Una infraestructura de llave pública (PKI) es la arquitectura, organización, tecnología, prácticas, políticas y procedimientos que en conjunto soportan la implantación y operación de un sistema criptográfico de llave pública basado en certificados.

PKI's son 80% políticas y 20% tecnología

Verificando una firma



Verificando una firma



Criptosistemas simétricos vs asimétricos

Cifrado Simétrico

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

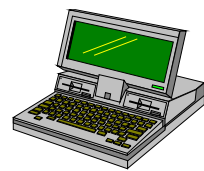
Cifrado Asimétrico

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

Protocolos transmisión segura

- 1994: SSL V 2.0 (Netscape)
microsoft descubre un problema en SSL
- 1995: PCT V 1.0
- 1996: SSL V 3.0
- 1997: PCT V 4.
se decide terminar con la pelea: Microsoft y
Netscape deciden sacar un protocolo en común
- 1999: TLS V 1.0

¿Cómo funciona?

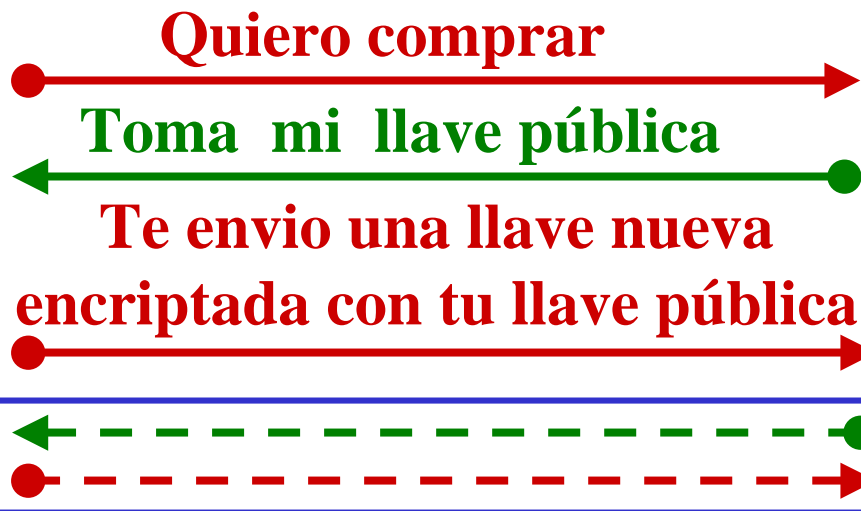


Cliente



Servidor

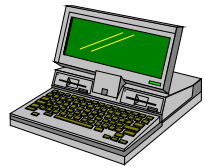
No hay autenticación
ni privacidad, ni
encriptación



Hablemos en forma
segura

Comunicación encriptada con la llave enviada por el cliente

Otro posible escenario



Cliente

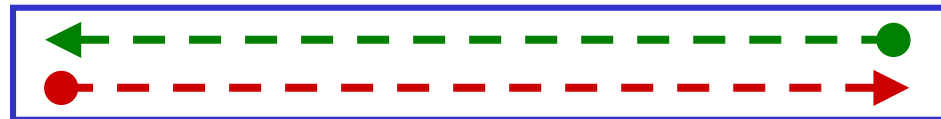


Servidor

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

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

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

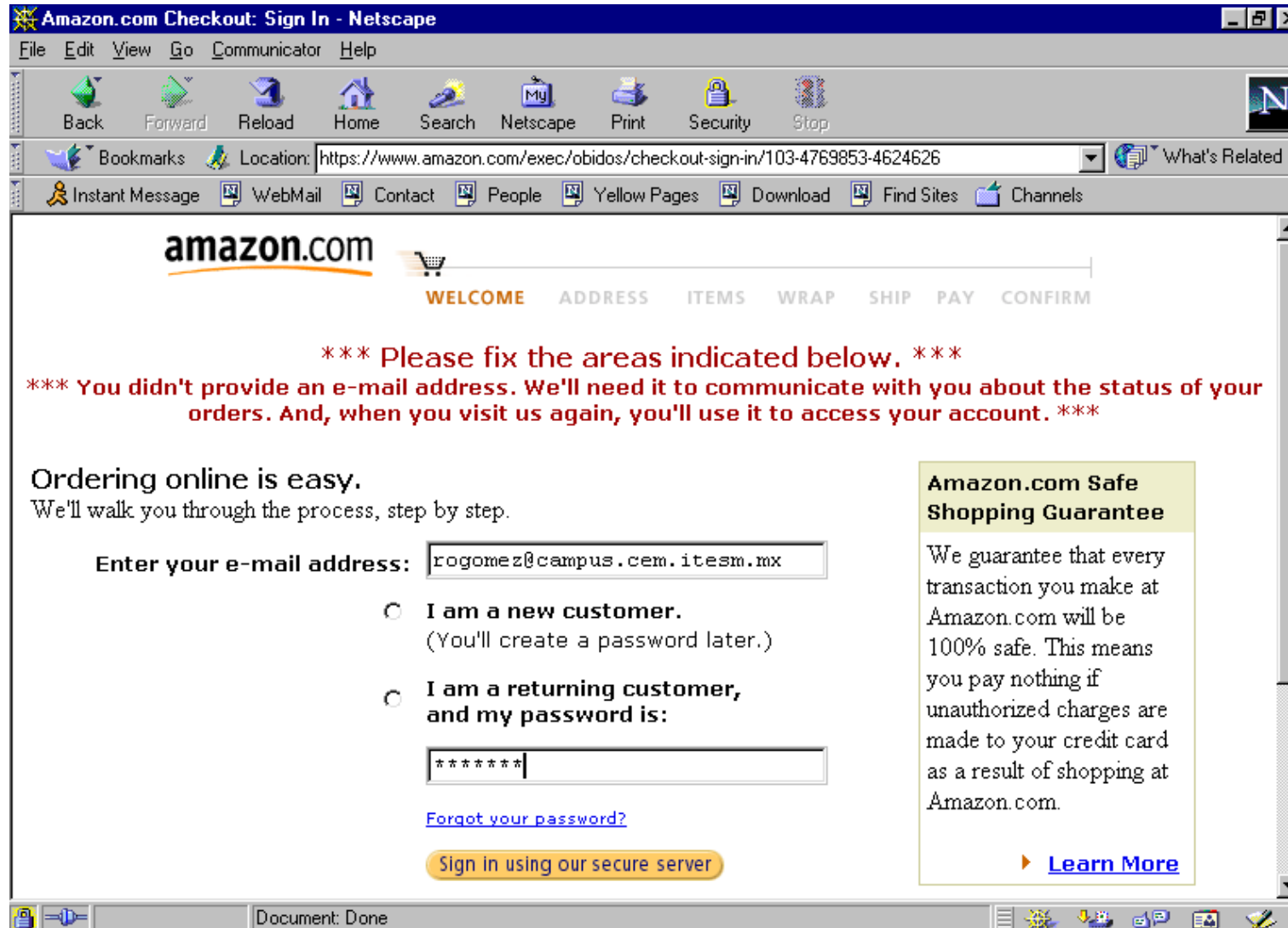


*Comunicación encriptada con la llave enviada por el cliente
y un hash para autenticación de mensajes*

Ejemplo protocolo seguro (1er. paso)



Ejemplo protocolo seguro (2do.paso)



Amazon.com Checkout: Sign In - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

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

Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels

amazon.com

WELCOME ADDRESS ITEMS WRAP SHIP PAY CONFIRM

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

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

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

Enter your e-mail address:

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

☐ I am a returning customer,
and my password is:

[Forgot your password?](#)

[Sign in using our secure server](#)

Amazon.com Safe Shopping Guarantee

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

[Learn More](#)

Document: Done

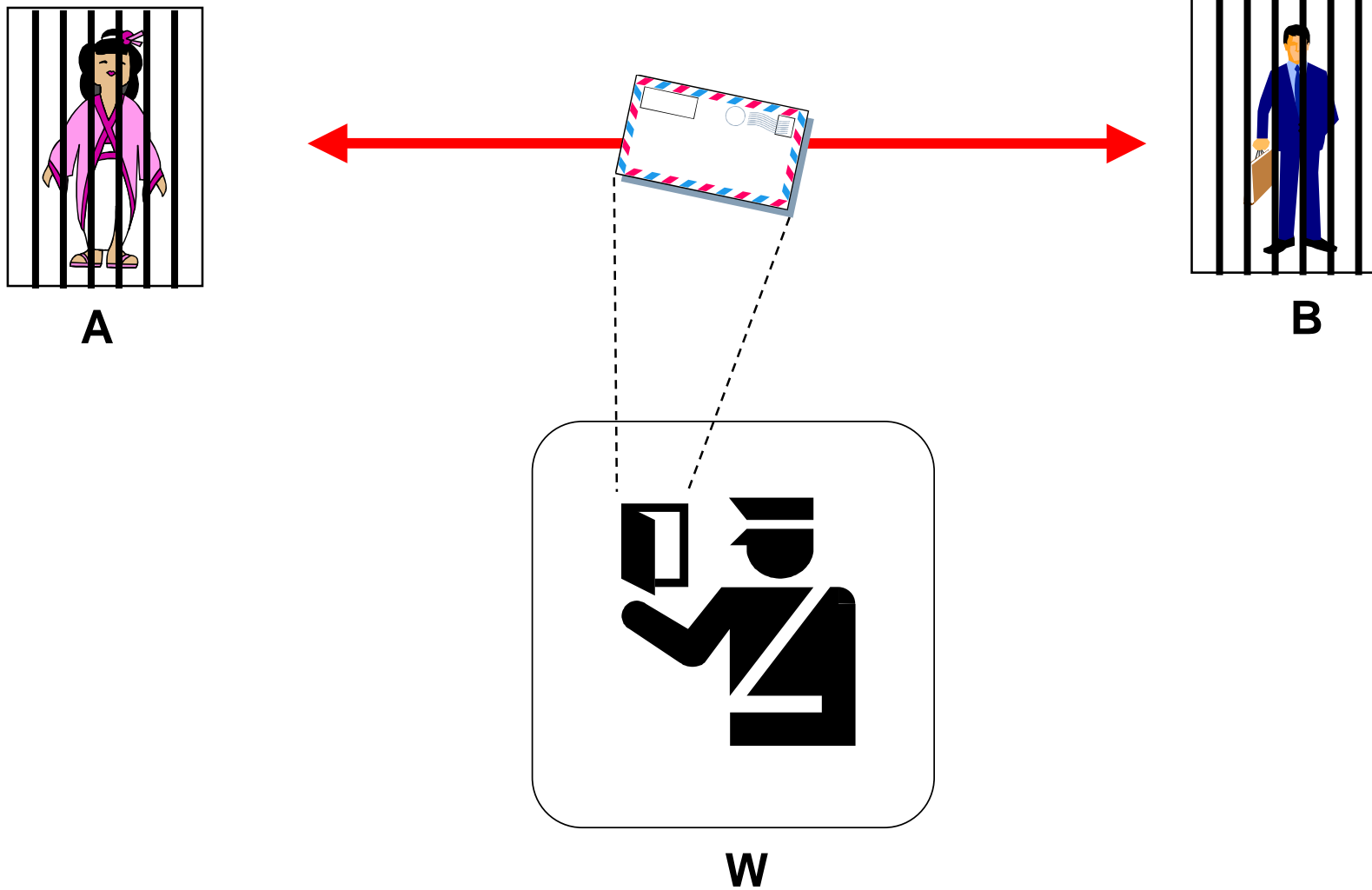
¿Y que hago ahora?

- Programar las rutinas de encriptación/decriptación uno mismo
- Usar librerías/bibliotecas con rutinas de encriptación decriptación
 - <http://www.eskimo.com/~weidai/cryptlib.html>
 - <http://www.cryptix.org/>
 - <http://www.cs.auckland.ac.nz/~pgut001/cryptlib/>
- Utilizar estándares aplicaciones disponibles en internet.
 - S/MIME
 - PEM
 - PGP

PGP

- Software acceso libre (<http://www.pgpi.org>).
 - Versión actual: 8.0
- Desarrollado por Phil Zimmermann en 1994.
- Protección de e-mail y de archivos de datos.
 - Encriptación de archivos
 - Encriptación de correo electrónico
 - Manejo de llaves
 - Borrado seguro (secure wipe)
 - Firmas digitales.
 - VPNs

El concepto de canal oculto



Esteganografia

- Area similar a la de criptología.
- Viene del griego stegos (ocultar).
- Conjunto de técnicas que nos permiten ocultar o camuflar cualquier tipo de datos, dentro de información considerada como válida.
- La información puede esconderse de cualquier forma
 - diferentes métodos se han ido desarrollando



Algunos ejemplos históricos

- Herodoto:
 - 440 ac: Aristagoras de Milet usa esclavos calvos para la revuelta contra los persas
 - Demeratus envía mensaje (tablones cubiertos de cera) a Esparta para avisar de que Xerxes (rey de Persa) tenía intenciones de invadir Grecia.
- Tintas invisibles
 - naturales: jugo limón, leche, orina, sal de amoníaco
 - química: alumbre y vinagre, traspasar cáscara huevo duro
- Chinos: texto escrito sobre seda china
- Siglo XVII: Schola Steganographica, Gaspar Schott partituras música
- Segunda Guerra mundial:
 - "Null Cipher"
 - Microfilmes
 - prisioneros usan i, j, t, y f para ocultar mensaje en código morse

Un primer ejemplo de Null Cipher

Tomando la primera letra de cada palabra

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

Hidden Information !

Newt is upset because he thinks he is President.

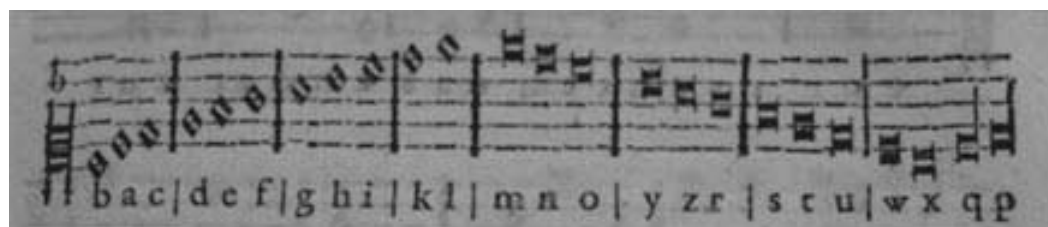
Un segundo ejemplo Null Cipher

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Apparentleutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Pershing sails from NYr June i

Ejemplo esteganografia en partituras



Métodos modernos

- Códigos de programas
- Archivos de música y de películas
- Campos no usados de paquetes de redes
- Espacio no utilizado del disco: slack space
- Imágenes

En códigos

```
/* hello.c */  
main( )  
{  
    printf("Bonjour\n");  
}
```

```
[raynal]$ gcc -o hello hello.c
```

```
[raynal]$ gdb -q hello
```

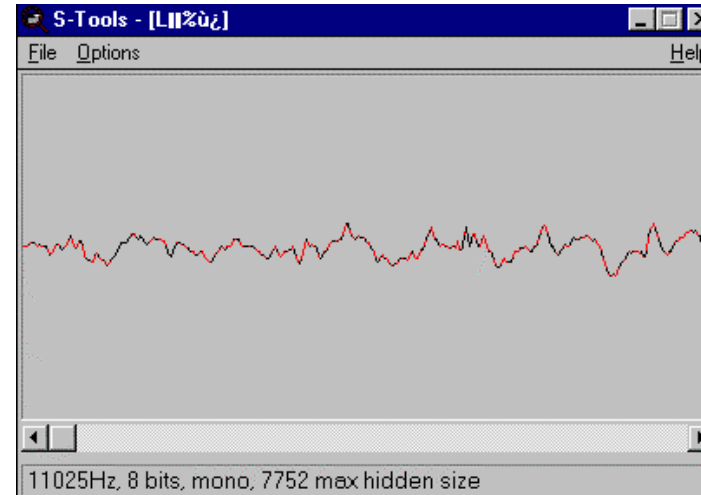
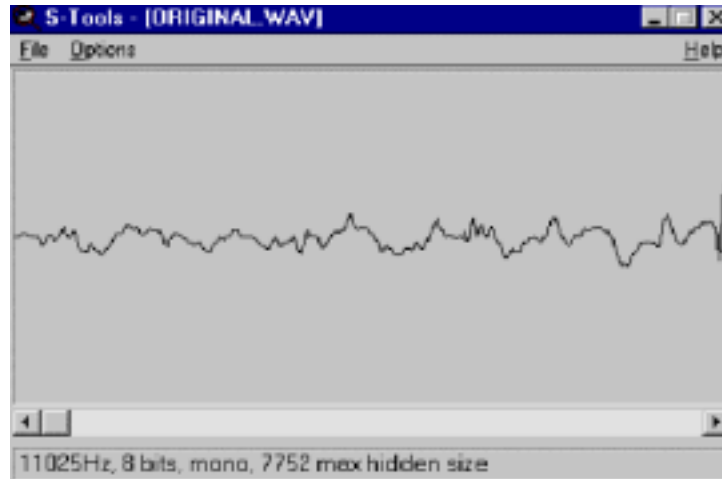
```
(gdb) disass main
```

Dump of assembler code for function main:

```
0x80483c8 <main>:      push %ebp  
0x80483c9 <main+1>:    mov %esp,%ebp  
0x80483cb <main+3>:    push $0x8048430  
0x80483d0 <main+8>:    call 0x8048308 <printf>  
0x80483d5 <main+13>:   add $0x4,%esp  
0x80483d8 <main+16>:   leave  
0x80483d9 <main+17>:   ret  
0x80483da <main+18>:   nop  
0x80483db <main+19>:   nop  
0x80483dc <main+20>:   nop  
0x80483dd <main+21>:   nop  
0x80483de <main+22>:   nop  
0x80483df <main+23>:   nop
```

End of assembler dump.

Esteganografía en música



Información: 132 134 137 141 121 101 74 38

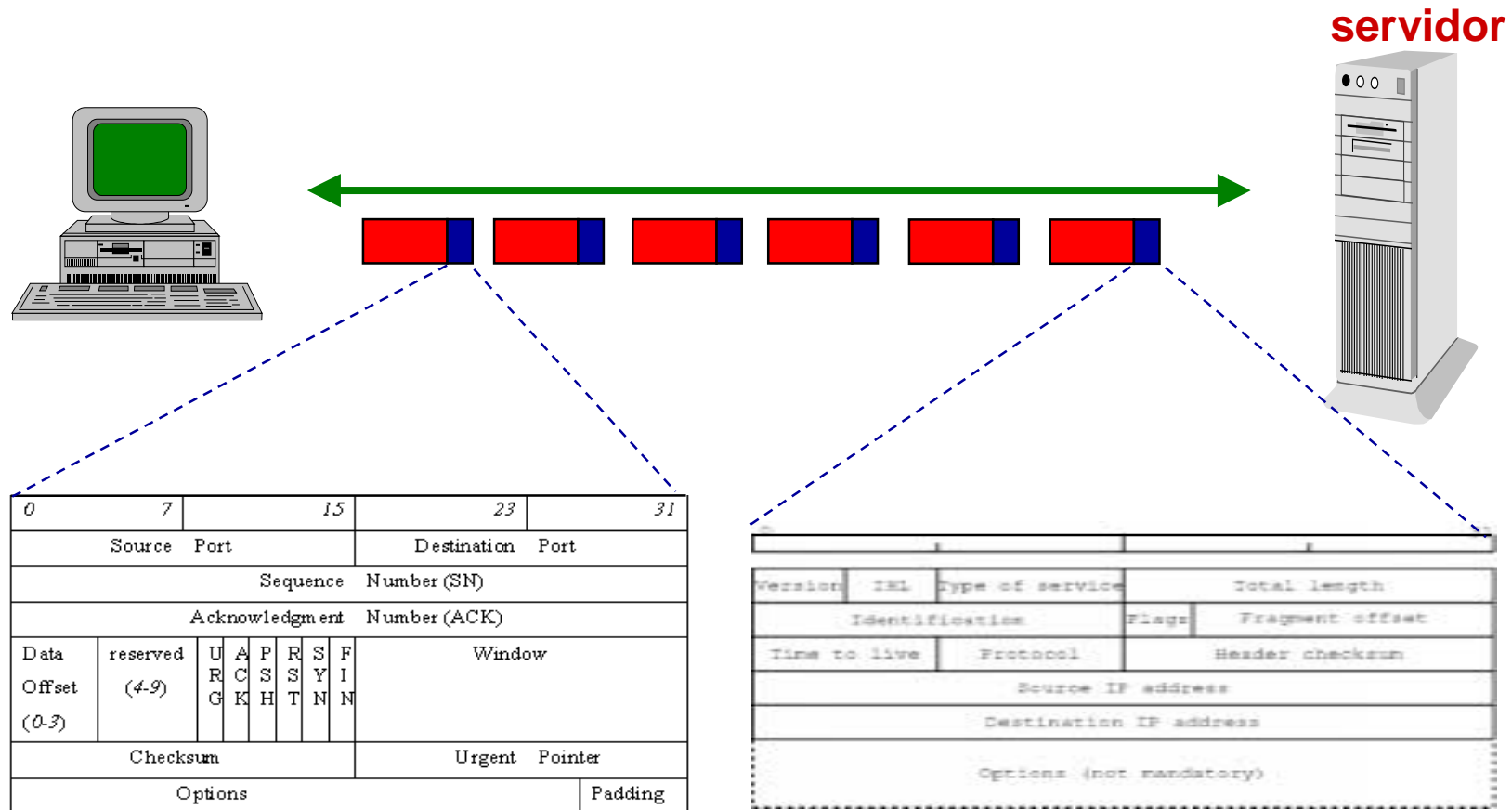
**Binario: 10000100 10000110 10001001 10001101 01111001 01100101
01001010 00100110**

Información a esconder: 11010101 (213)

Resultado: 133 135 136 141 120 101 74 39

**Binario: 10000101 10000111 10001000 10001101 01111000 01100101
01001010 0010011**

Paquetes redes



Esteganografía en paquetes redes

Encabezado IP

0				31	
Version	IHL	Type of service	Total length		
Identification			Flags	Fragment offset	
Time to live		Protocol	Header checksum		
		Source IP address			
		Destination IP address			
		Options (not mandatory)			

Opción 1:
IP Identification Field

Encabezado TCP

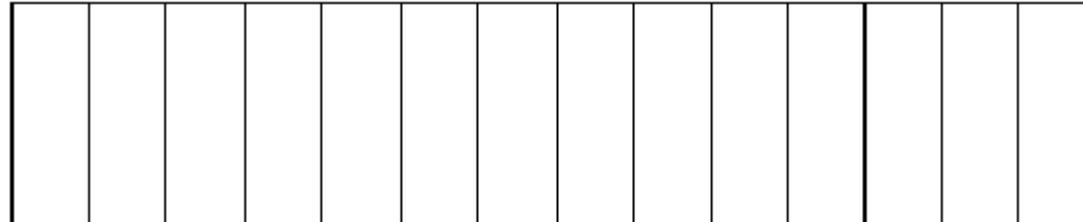
0	7	15	23	31
Source Port			Destination Port	
Sequence Number (SN)				
Acknowledgment Number (ACK)				
Data Offset (0-3)	reserved (4-9)	URG	ACK	PSH
		RST	SYN	FIN
Checksum			Window	
Options				Padding

Opción 2:
Initial Sequence Number Field

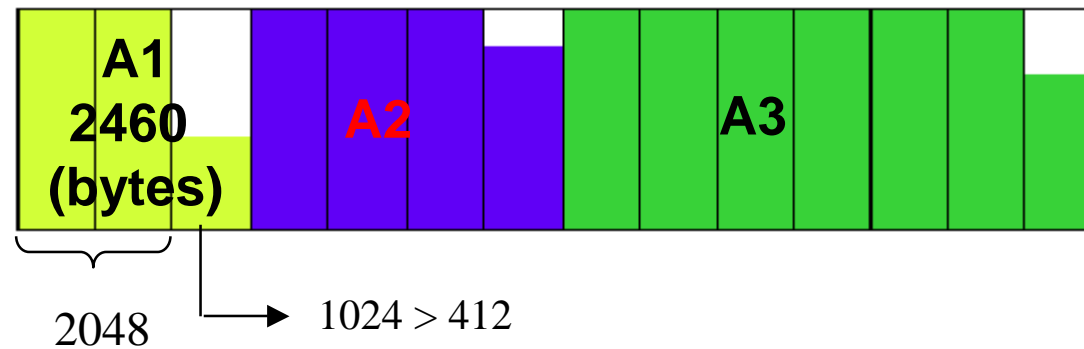
Opción 3:
The TCP Acknowledge Sequence Number Field "Bounce"

El slack space

14 clusters libres
c/cluster = 1024 bytes



Tres archivos:
A1, A2 y A3

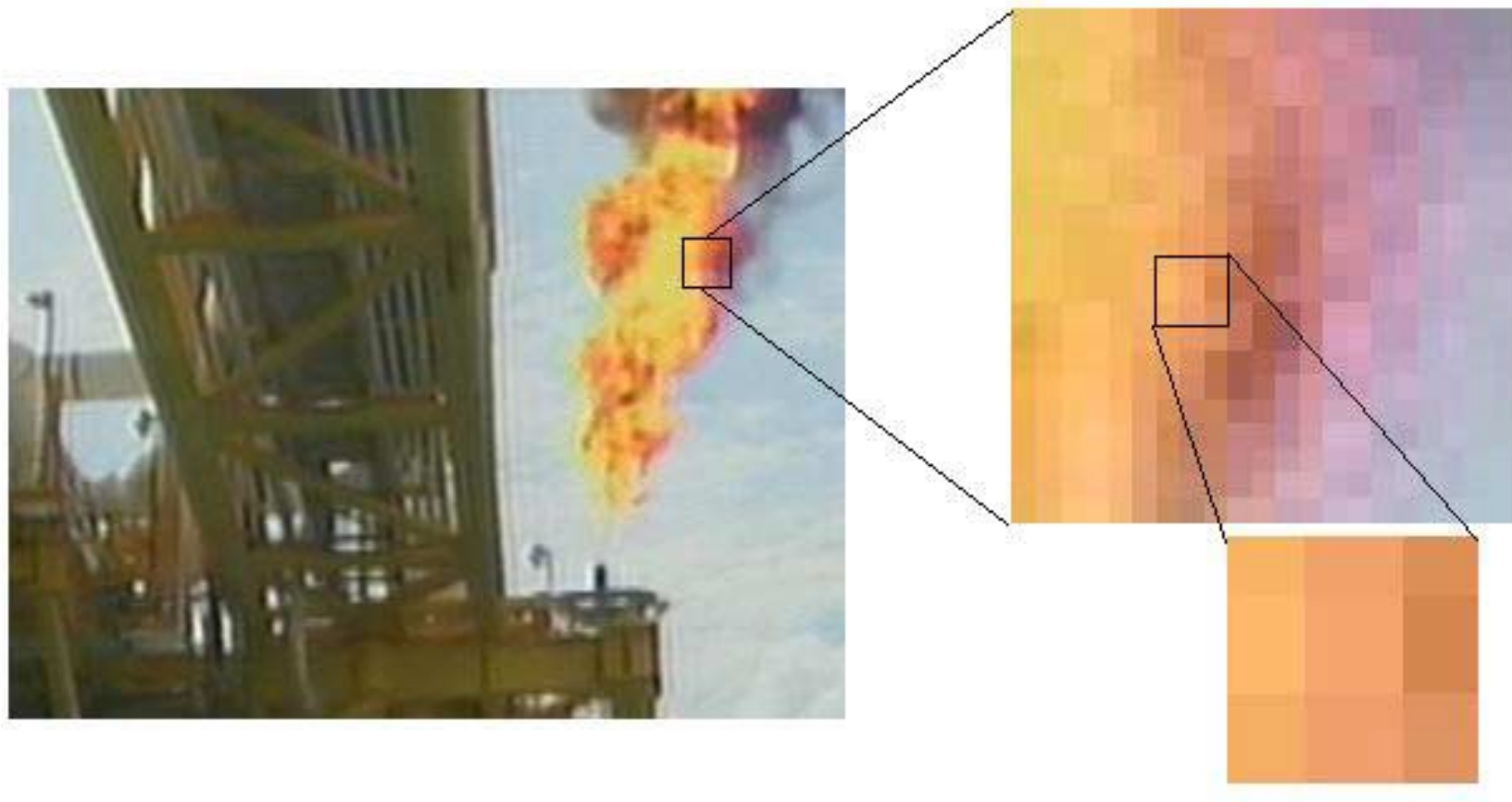


Cluster = 512bytes



Imágenes

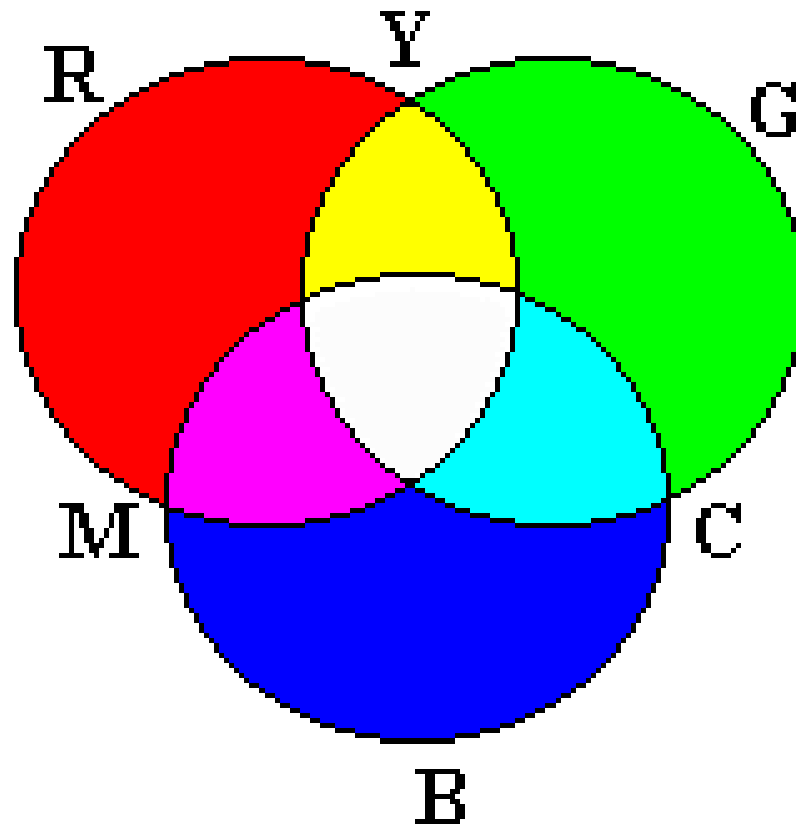
- Una imagen es una matriz de $M \times N$ Píxeles.
- Un Pixel es la unidad mínima de dibujo



Modelo de Color RGB

- Emplea síntesis aditiva, es decir, suma colores para obtener nuevos colores.
- El color de inicio es el negro y la suma de todos los colores da blanco.
- Posee tres canales de color: Rojo (R), Verde (G), Azul (B)

Colores primarios y secundarios



Representación de Colores

- Los colores se representan con 24 bits. 8 para cada componente RGB.
- Cada componente tiene 8 bits, es decir, 256 posibles niveles de color
- A esto se le conoce como color verdadero

1 0 0 0 1 1 0 0

Azul

1 0 0 0 1 1 0 0

Verde

1 0 0 0 1 1 0 0

Rojo

¿Podemos Tomar un Bit Prestado?



Segundo Bit Más Significativo



Tercer Bit



Cuarto Bit



Quinto Bit

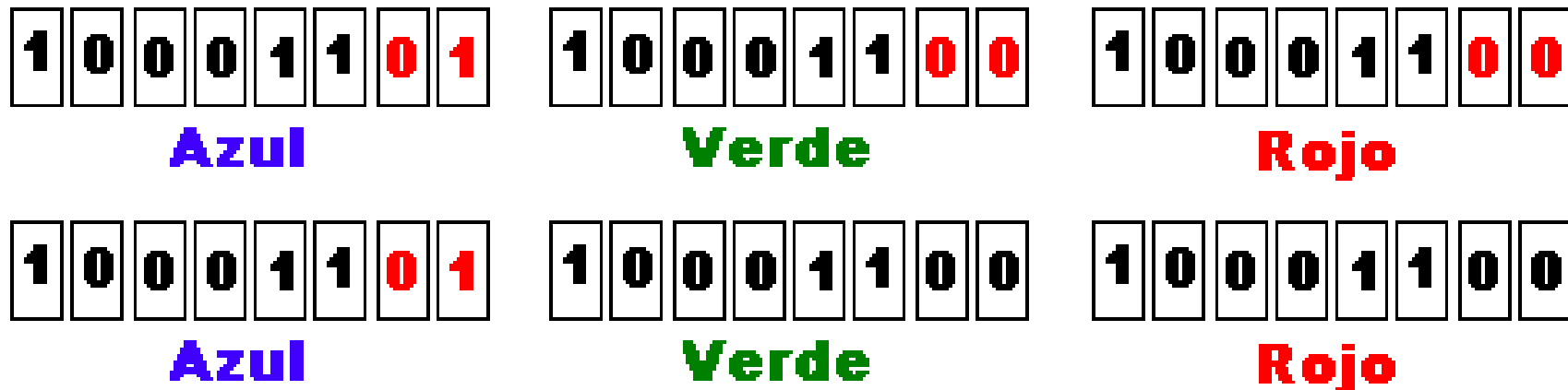


Sexto Bit



¿Cómo Metemos una “A” en una Imagen?

- Simple imagenes de 24 bits
- Almacenadas internamient como tripletas RGB
- Se esparcen los bits en el archivo
- Por ejemplo: insertar caracter A = (01 00 00 01)



¿Qué Información Podemos Meter en una Imagen?

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

Características Información Oculta

- La información oculta es muy sensible al encontrarse en los bits menos significativos
- La pueden destruir:
 - La aplicación de cualquier filtro
 - Cambios en brillo o contraste
 - Un cambio de tamaño en la imagen
 - Cualquier trazo o cambio en la imagen
 - Recortar la imagen

Esteganografia vs Watermarking

- Misma características esteganografía
- Robustez en contra de posibles ataques
 - esteganografia esta relacionada con la detección de un mensaje oculto, mientras que watermarking involucra el borrado/duplicación de un pirata
- Watermarking no siempre necesita estar oculto
 - alguno sistemas usan marcas agua digitales visibles
- La información ocultada por un sistema de marca de agua, siempre se asocia al objeto digital a ser protegido.
- Comunicaciones esteganograficas son del tipo punto a punto, mientras que watermarking son del tipo punto-multipunto.

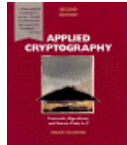
Stegoanálisis

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

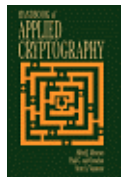
Herramientas

- Steganos Security Suite 5 (shareware)
- Invisinle Secrets V4.0 (shareware)
- SecurEngine 2.0 (freeware)
- Camera/Shy (freeware)
- Camaleon (freeware)
- CyptArkan (shareware)
- Stego-Lame freeware
- Stegdetect (XSteg) freeware
- MP3Stego (freeware)
- S-Tools4
- S-Tools3 <http://www.jjtc.com/stegoarchive/stego/software.html>

Referencias Criptografia



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



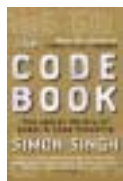
Handbook of applied Cryptography, A Menezes P van Oorschot and Vanston, CRC Press, 1996
(<http://www.cacr.math.uwaterloo.ca/hac>)



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

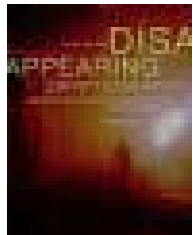


Cryptography and Network Security, Principles and Practice, William Stallings, Ed. Prentice Hall, 2da. edición, 1999



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

Referencias Esteganografia



- Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser, F. A.P. Petitcolas, F. Petticolas Ed. Artech House, 2000
- Disappearing Cryptography, Second Edition - Information Hiding, Steganography and Watermarking, Peter Wayner, Ed. Morgan Kaufmann; 2da. edición, 2002
- Digital Watermarking: Principles & Practice, Ingemar Cox, Jeffrey Bloom, Matthew Miller, Ed. Morgan Kaufmann; 1a. edición, 2001
- Páginas
 - <http://www.cl.cam.ac.uk/~fapp2/steganography/index.html>
 - <http://fravia.anticrack.de/stego.htm>

LOS DELITOS CIBERNÉTICOS Y LA COMPUTACIÓN FORENSE

Criptología y Esteganografía

Roberto Gómez Cárdenas

rogomez@itesm.mx

<http://campus.cem.itesm.mx/ac/rogomez>