Criptografía

Dr. Hugo D. Scolnik

Prof. Titular Dpto. Computación
FCEN -UBA

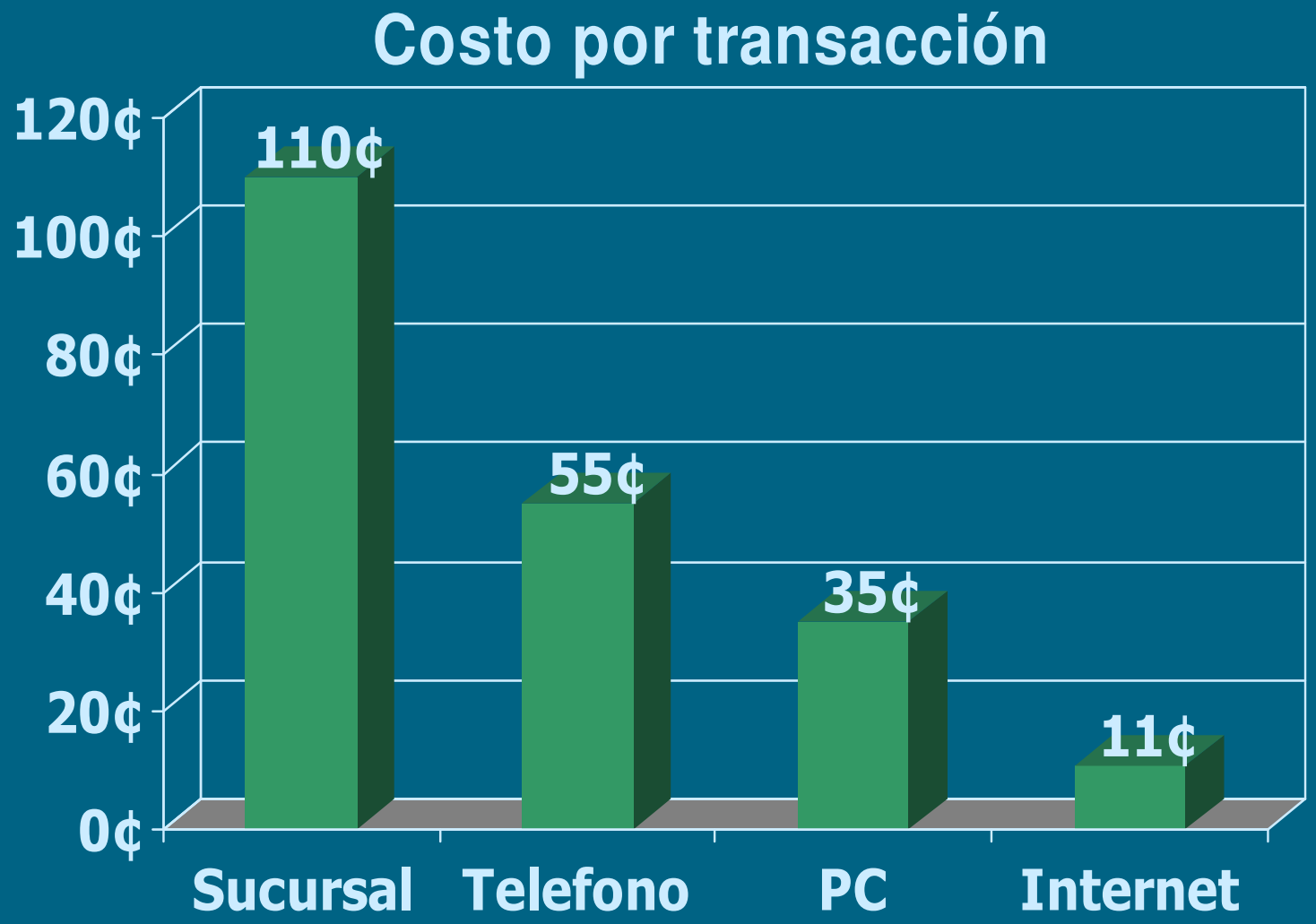
ELEMENTOS BÁSICOS DE CRIPTOGRAFÍA

- Criptografía: es el arte de transformar mensajes de modo tal que sean ilegibles para todos aquellos a los que no se les confiere el modo de acceder a los mismos.
- Criptoanálisis: es el estudio de las técnicas para quebrar mensajes criptografiados.

OBJETIVOS DE LA CRIPTOGRAFÍA

- CONFIDENCIALIDAD
- INTEGRIDAD
- CERTIFICACIÓN DE ORIGEN
- NO REPUDIO

Internet Banking



Source: Frans Hesp ABN-AMRO 11/01

Y cada vez hay más aplicaciones:

CONFIDENCIALIDAD

ATAQUE DE FUERZA BRUTA

Consiste en probar en forma sistemáticamente todas las combinaciones posibles de las claves, hasta descubrir la que fue usada en una encripción

Seguridad de un sistema criptográfico

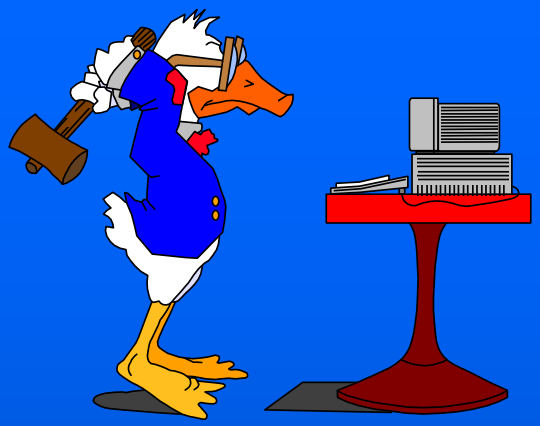
debe depender únicamente del desconocimiento de las claves y no del algoritmo (este es generalmente conocido)


SEÑOR... DESCUBRIERON EL CÓDIGO DEL GENOMA HUMANO
¡¡MALDITOS HACKERS!! VOY A TENER QUE CAMBIAR LA CONTRASEÑA
Daniel PAZ

Punto 2.

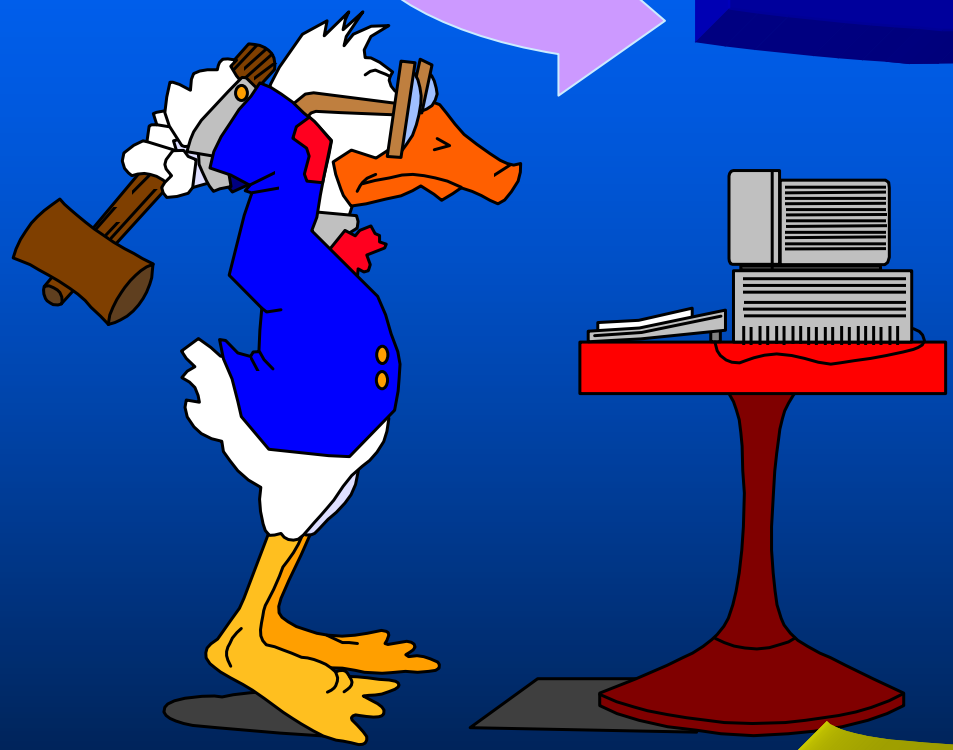
Inalterabilidad de los mensajes. El concepto de hashing.

INTEGRIDAD



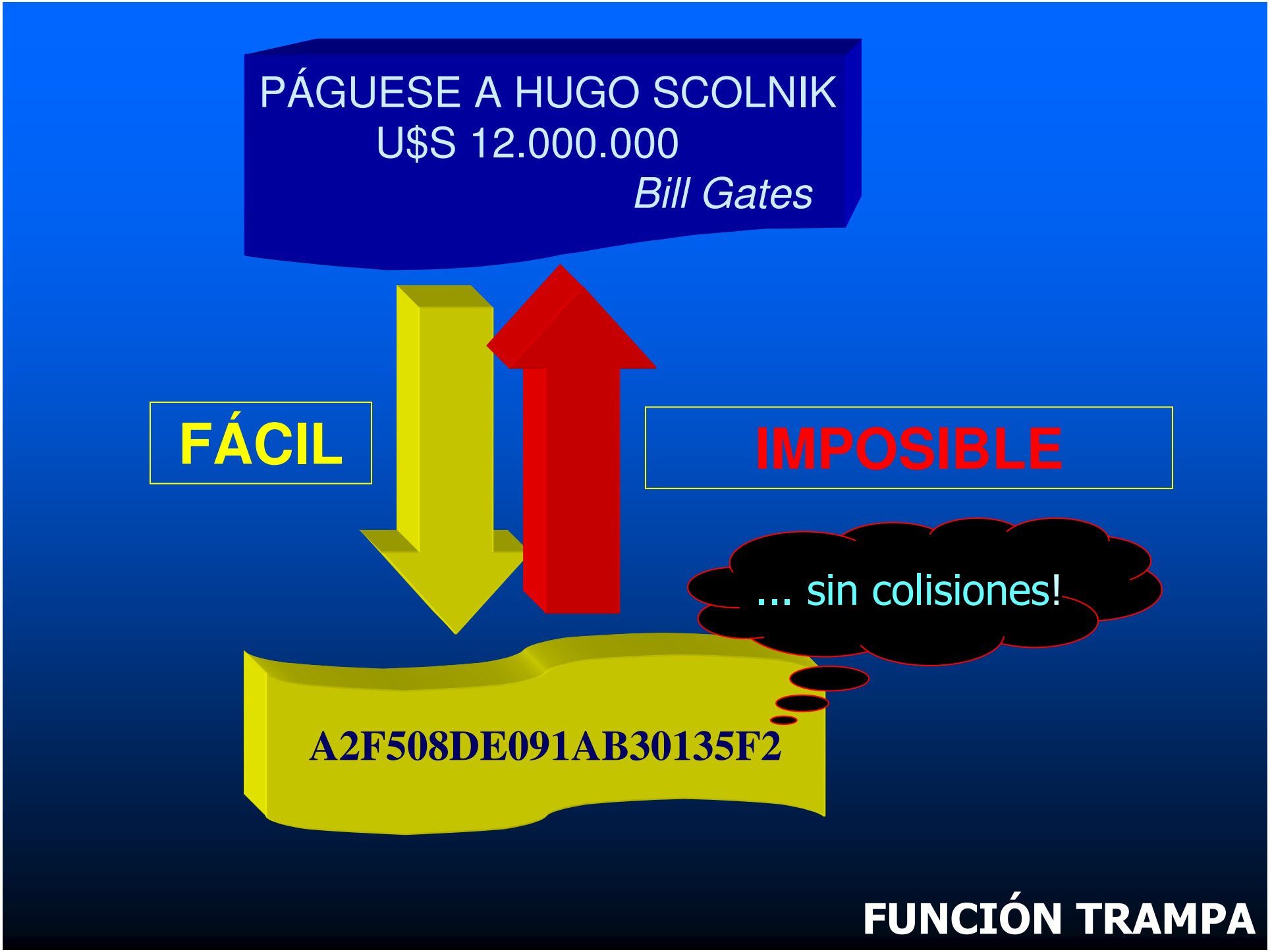
Hash: dado un mensaje de n bits una función de hashing aplicada al mismo da como resultado otro "mensaje" de longitud que constituye un "resumen" del mismo. **La idea es que aunque obviamente hay otros mensajes que producen el mismo hash, es extremadamente difícil encontrarlos y aún más difícil que tengan un significado**. Por lo tanto si se transmite un mensaje (encriptado o no) por una vía y su correspondiente hashing por otro (o firmado digitalmente), se puede verificar si el mismo ha sido alterado.

PÁGUESE A HUGO SCOLNIK
U$S 12.000.000
Bill Gates



A2F508DE091AB30135F2

HASHING


PÁGUESE A HUGO SCOLNIK
U$S 12.000.000
Bill Gates
FÁCIL
IMPOSIBLE
... sin colisiones!
A2F508DE091AB30135F2
FUNCIÓN TRAMPA

"Secure" hashes

- **SNEFRU** (128/256 bits); El SNEFRU de 2 pasos se puede quebrar, usando una PC, en 3 minutos [birthday: dado M, hallar M' cuyo H(M')=H(M)], o en 1 hora (hallar un mensaje M dado un hash h)
- **N-HASH**
- **MD2** (Message Digest-2, Ron Rivest, 128 bits, mas lento, menos seguro que MD4, usado en PEM)
- **MD4** (Message Digest-4, Ron Rivest, 128 bits, muy usado)
- **MD5** (Message Digest-5, Ron Rivest, 128 bits, MD4 con mejoras, muy usado, usado en PEM, SSL)
- **SHA/SHA-1** (secure hash algorithm, 160 bits, usado en DSS, SSL)
- **RIPEMD 128 / RIPEMD 160**
- **OTROS**

Punto 3.

Métodos simétricos, DES, 3DES, IDEA, AES, Cryptoflash, confiabilidad, longitud de claves, el problema de la distribución de las claves.

La máquina ENIGMA

http://homepages.tesco.net/~andycarlson/enigma/enigma_j.html

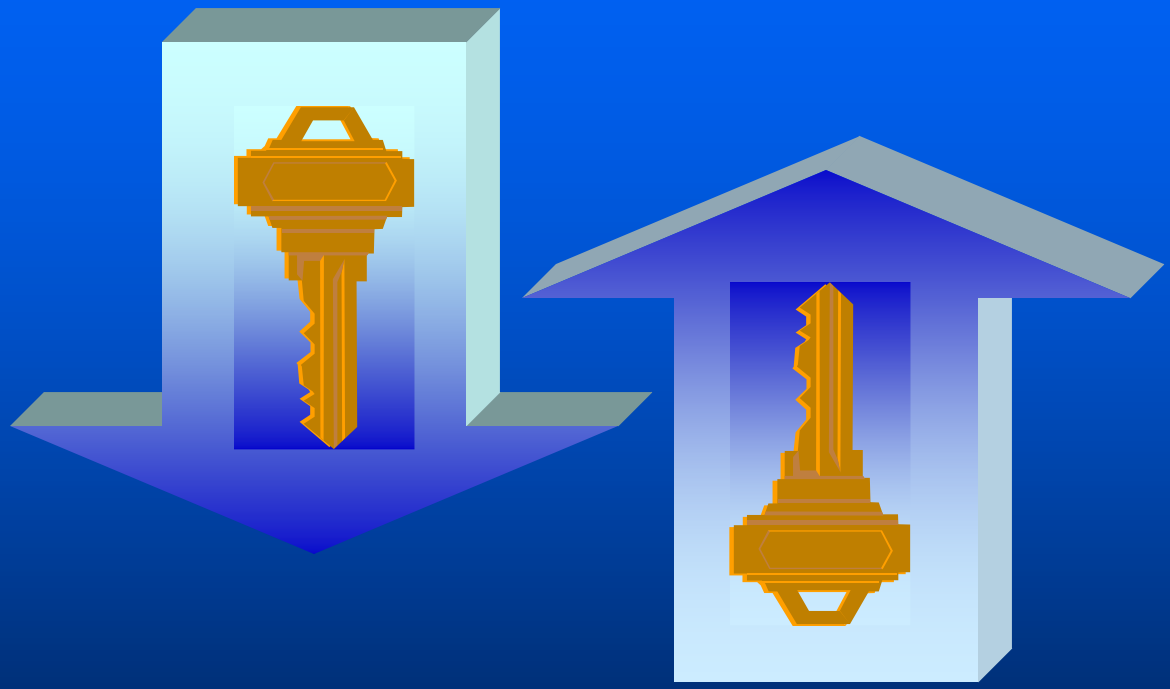
http://users.telenet.be/d.rijmenants/en/enigmasim.htm

CLAVE

(ÚNICA)

MÉTODOS DE ENCRIPCIÓN SIMÉTRICOS

ESTAMOS HABLANDO DE CRIPTOGRAFÍA



#@Y6&(*-+jW3!’G&%;{I8=U

ENCRIPCIÓN SIMÉTRICA

Interceptamos este mensaje en Internet

Ä¨a åŸ□‘‹>îEÏ□Ñ□ê□Õ¬Ë□□Á{□_È-¶üì—A[ñiÁ,Û–¥¢wê□PCæ□à×□”âÏéñK□

¹ŒB’Ý5□ÿh□ƒ!Zƒ13□□ÊZ¾□úP,àæ;□P□¹á2Ê□À□Jâ□(

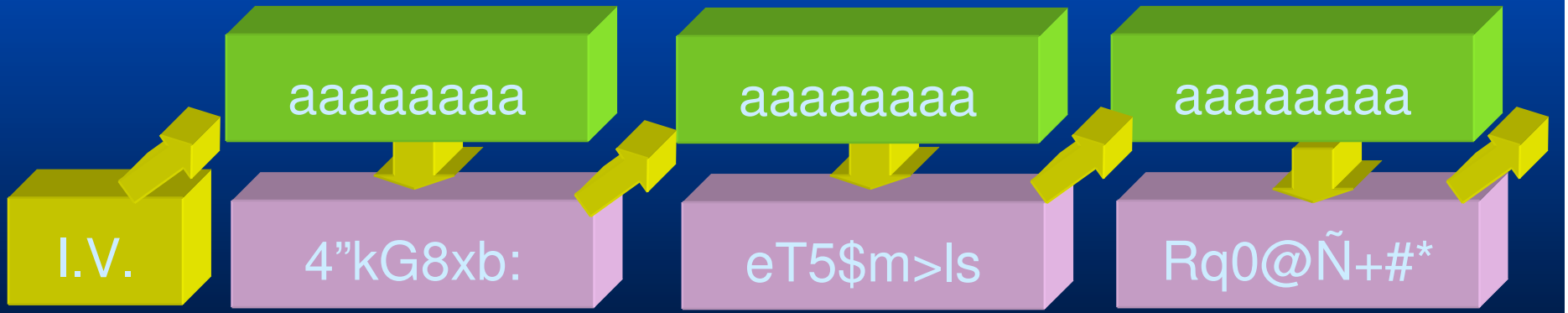
#_-Âþlë□…õ^³>2Ü¦□àÜ[O8.n

Algoritmos simétricos

- DES (block, clave de 56 bits)
- 3DES (block, clave de 112/168 bits)
- RC2 (block, Ron Rivest, reemplazo para DES, clave de tamaño variable)
- RC6 (block, Ron Rivest, clave arbitraria)
- IDEA (block, international data encryption algorithm. clave de 128 bits)
- NCT (block, non-linear curves traveller, clave arbitraria)
- RIJNDAEL (block, clave 128/256-bits)
- CRYPTOFLASH (Stream, clave de 1024-bits)

MODO ECB (sin feedback)

MODO CBC (con feedback)



CLAVE	4 Bytes	6 Bytes	8 Bytes
Minúsculas (26)	.5 sec	5 min	2.4 dias
minúsc + dígitos (36)	1.7 sec	36 min	33 dias
Caracteres alfanuméricos (62)	15 sec	16 horas	6.9 años
Caracteres ASCII (128)	4.5 min	51 dias	2300 años
Bytes (256)	1.2 horas	8.9 años	580000 años

Exploración a razón de 1.000.000 pruebas/segundo

(y el poder computacional se duplica cada 18 meses)

RELATIVE BENCHMARK OF Cryptoflash ® AND THE SYMMETRIC ALGORITHM SELECTED BY THE NIST (10/02/2000) AS THE PROPOSED AES (Advanced Encryption Standard)

ON A STANDARD PENTIUM USING TEXTS WITH LENGTHS > 2^{15} bytes

Rijndael	**20** CPU Cycles/byte	Max key length: 256-bits	--difficult scalability with performance slowdown -the inverse takes more code & time
Cryptoflash	**7** CPU cycles/byte ***285% faster***	Max key length: 1024-bits	- CPU Fully scalable (8/16/32/64-bits) with same performance - inverse and direct take the same code & time

Bibliography:

[1] Wolfram,S., "Cryptography with Cellular Automata", CRYPTO'85
[2] Meier,W. et al., "Analysis of Pseudo Random Sequences Generated by Cellular Automata", EUROCRYPT'91
[3] Hecht, J.P., ,"Generación de caos determinístico y atractores extraños usando AC", FOUBA, Mar 2000
[4]. Schneier et al, "Performance Comparison of the AES Submissions – Vers 1.4b – Jan 15, (1999)
http://www.counterpane.com/aes-performance.html
[5] http://csrc.nist.gov/encryption/aes/round2/AESAlgs/Rijndael/Rijndael.pdf

Punto 5.

Métodos asimétricos, transmisión de claves. El método de Diffie-Hellman. Sobres digitales, RSA. El concepto de firma digital, claves privadas y públicas. Seguridad de los protocolos.

Como distribuir las claves secretas

La idea es disponer de un conjunto numerado de claves y transmitir códigos ininteligibles para un espía que permiten arribar mediante operaciones matemáticas al mismo número. Este valor en común entre los usuarios habilitados será utilizado luego como llave de un algoritmo simétrico.

Ejemplo:

Sea $p = 23, a = 5, x = 6, y = 10$. Ahora el usuario 1 calcula:

$$f(x) = a^x \bmod(p) = 5^6 \bmod(23) =$$

$$15625 \bmod(23) = 8$$

y se lo envía al usuario 2.

El usuario 2 calcula

$$f(y) = a^y \bmod(p) = 5^{10} \bmod(23) =$$

$$9765625 \bmod(23) = 9$$

y se lo envía al usuario 1.

El usuario 2 recibió el número 8 y procede a calcular:

$$K = f(x)^{y} \bmod(p) = 8^{10} \bmod(23) = 3$$

El usuario 1 recibió el número 9 y calcula:

$$K = f(y)^{x} \bmod(p) = 9^{6} \bmod(23) = 3$$

Por lo tanto ambos llegaron a la MISMA clave.

Qué consigue un espía ? Intercepta los números y aunque conozca el primo elegido y la base (o sea) , no sabe cuales fueron los números .Para encontrar la clave común tendría que resolver el llamado problema del logaritmo discreto, por ejemplo:

$$5^x \bmod(23) = 8$$

Cuando los números involucrados son muy grandes, y están bien elegidos, este problema es computacionalmente irresoluble en un tiempo razonable.

Ejemplo:

$$p = 1000475149\ ,\ a = 876543098\ ,$$

$$x = 1234567890987654 3\ ,$$

$$y = 654375426738848$$

Los resultados son:

$$f(x) = 993617947\ \ ,\ f(y) = 839026926$$

y la clave común a la que ambos arriban es:

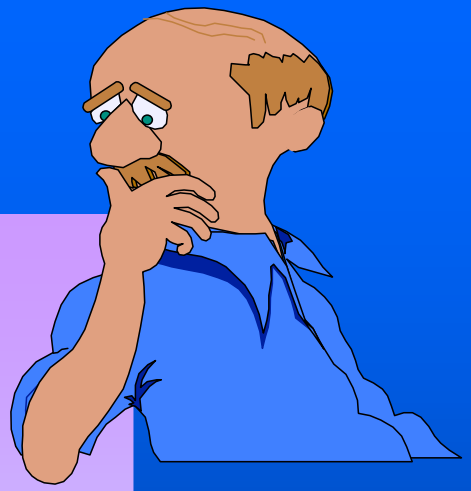
$$K = 708448295$$

Obviamente puede usarse esta clave en un algoritmo simétrico o puede ser una referencia a un conjunto de claves numeradas,

El espía (si llegó a conocer los números p, a) tendría que resolver la ecuación:

$$876543098^{x} \bmod(1000475149) = 993617947$$

En la práctica se usan números mucho mayores, lo que solo es factible con un software o hardware muy bien implementado.



Criptografía de clave pública

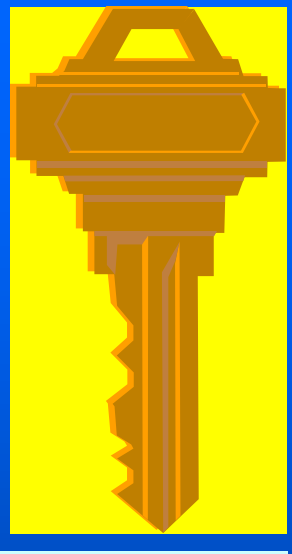
- prácticamente inquebrable si se implementa adecuadamente
- Deducir una clave a partir de la otra es computacionalmente irrealizable, aún disponiendo de recursos extremos

  (se presume que se requieren 60.000.000 de años de una batería coordinada de 1.000.000 de computadoras que operen a razón de 1.000.000 de multiplicaciones y divisiones por segundo con números de 309 dígitos decimales para deducir una sola clave privada RSA 1024-bits a partir de la pública, usando el algoritmo más eficiente conocido - SNFST)
- 100 veces más lentos que los simétricos
- claves mucho mas largas que los simétricos

MÉTODOS DE ENCRIPCIÓN ASIMÉTRICOS

(de clave pública)

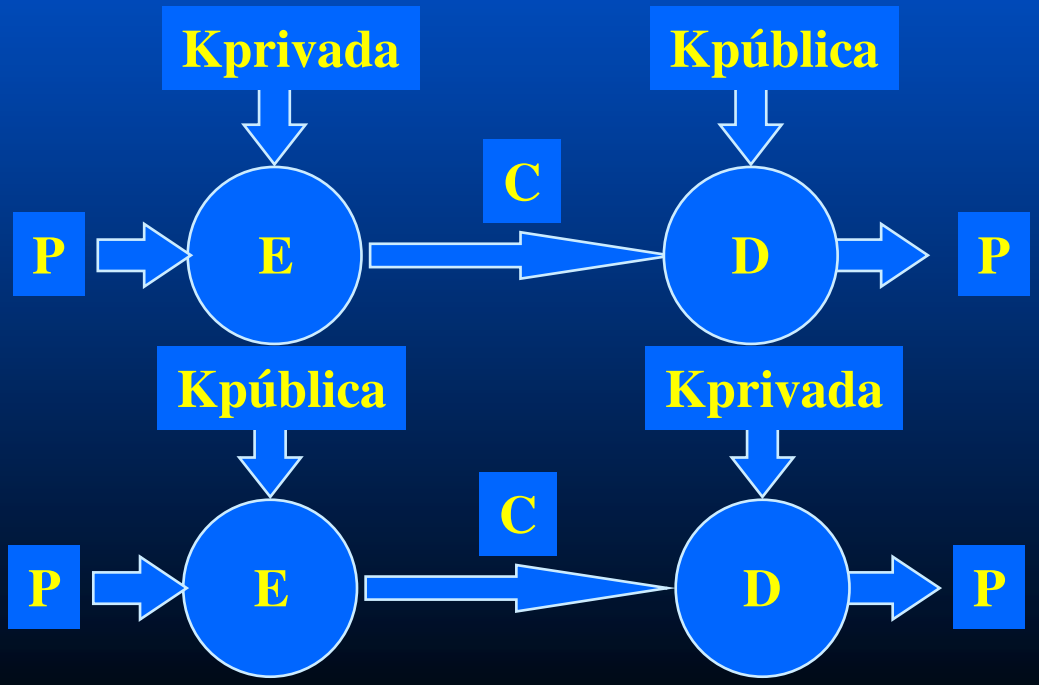
CLAVE
(PÚBLICA)



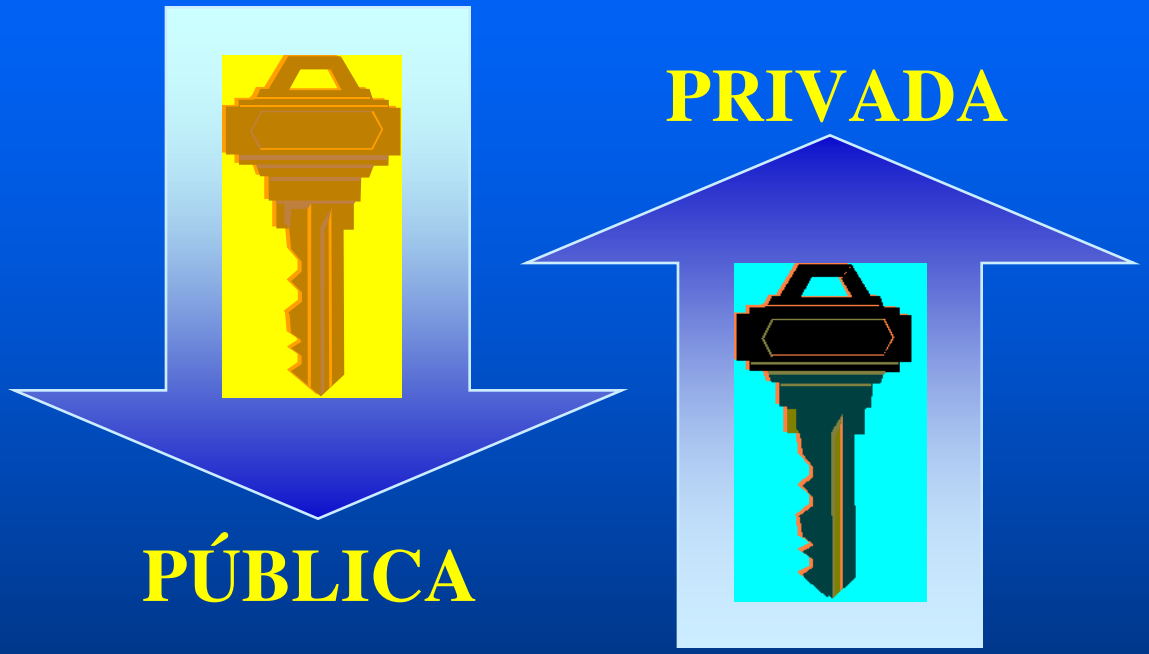
CLAVE
(PRIVADA)

Criptografía Asimétrica (Sistemas de Clave Pública)

- Mediante un programa, el usuario genera un PAR de claves. Una es la pública, la otra es la privada **(secreta).**
- **Si se encripta con una, se desencripta con la otra.**



ESTAMOS HABLANDO DE CRIPTOGRAFÍA

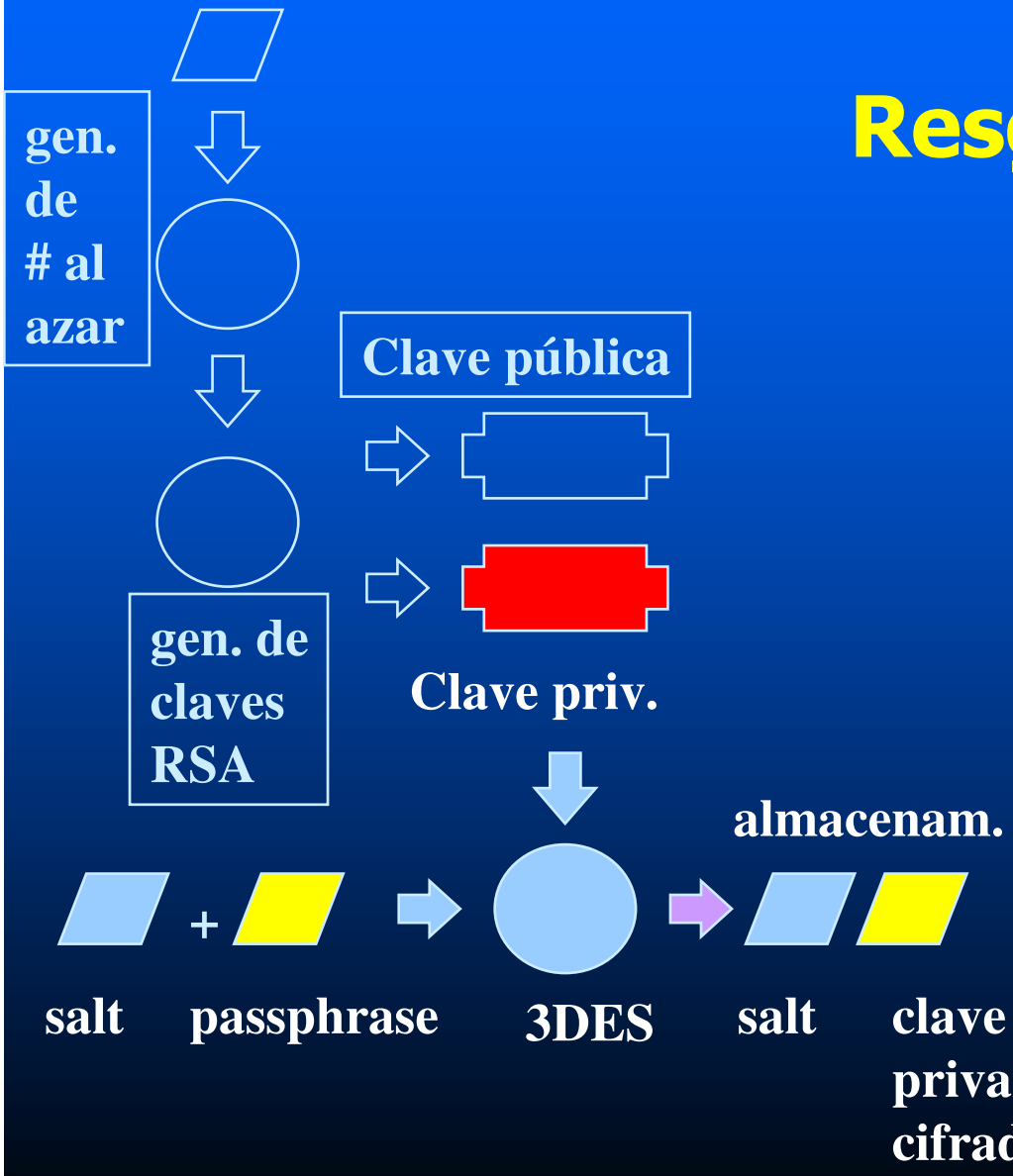


K*#5Al[#@Y6&(*-8!-U

]fQ1^+jW3!’G&%;{I8=

ENCRIPCIÓN ASIMÉTRICA

Resguardo de clave privada



EL USUARIO ES EL ÚNICO RESPONSABLE DEL USO (o abuso) DE SU CLAVE PRIVADA.

③CÓMO PROTEGERSE ?

- IDENTIFICACIÓN BIOMÉTRICA (huella digital)

- ALMACENAMIENTO PORTATIL (smartcards, eToken)

Desafíos actuales

Por ejemplo el premio para factorizar RSA 704

74037563479561712828046796097429573142593188889231
28908493623263897276503402826627689199641962511784
39958943305021275853701189680982867331732731089309
00552505116877063299072396380786710086096962537934
650563796359

es de 30.000 U$S y para RSA 2048 es de 200.000 U$S

Ver:

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


INTEGRIDAD
CERTIFICACIÓN
Y NO REPUDIO
FIRMA DIGITAL

PÁGUESE A HUGO SCOLNIK
U$S 12.000.000
Bill Gates

HASHING

A2F508DE091AB30135F2

CLAVE
(PRIVADA)

FD
#3Ds@*j0{28z!^}Tc)%4+<6

GENERACIÓN DE FIRMA DIGITAL

PÁGUESE A HUGO SCOLNIK
U$S 12.000.000
Bill Gates

FD
#3Ds@*j0{28z!^}Tc)%4+<6

CLAVE
(PÚBLICA)

RECALCULAR HASHING

A2F508DE091AB30135F2

A2F508DE091AB30135F2

SON IGUALES ?

VERIFICACIÓN DE FIRMA DIGITAL

Punto 7.

Modelos de e-commerce seguro.

Criptografía – E-COMMERCE

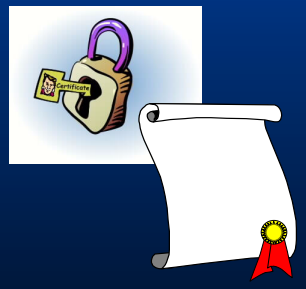
③E-COMMERCE: ***transacciones en Internet***

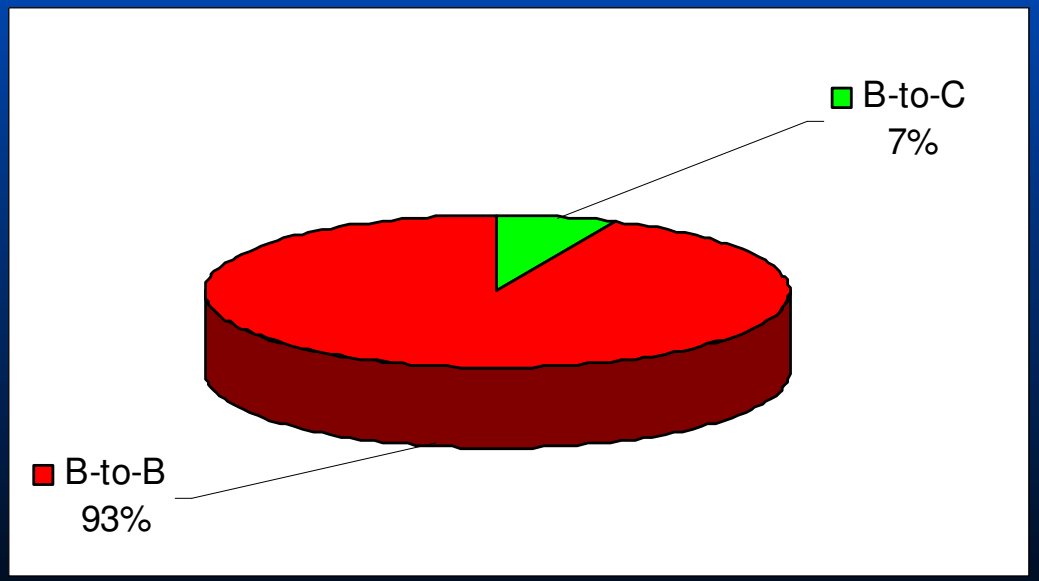
③basado en la confianza y la seguridad mutuas

③*REVENUES MUNDIALES E-COMMERCE AÑO 2000*

③BUSINESS-TO-BUSINESS: 125.000 Millones U$S

③BUSINESS-TO-CONSUMER: 9.000 Millones U$S





INTERNET

- es abierta
- es universal
- es económica
- es insegura

e-Commerce

- requiere confidencialidad
- requiere autentificación
- requiere control de integridad
- requiere simplicidad
- es el futuro

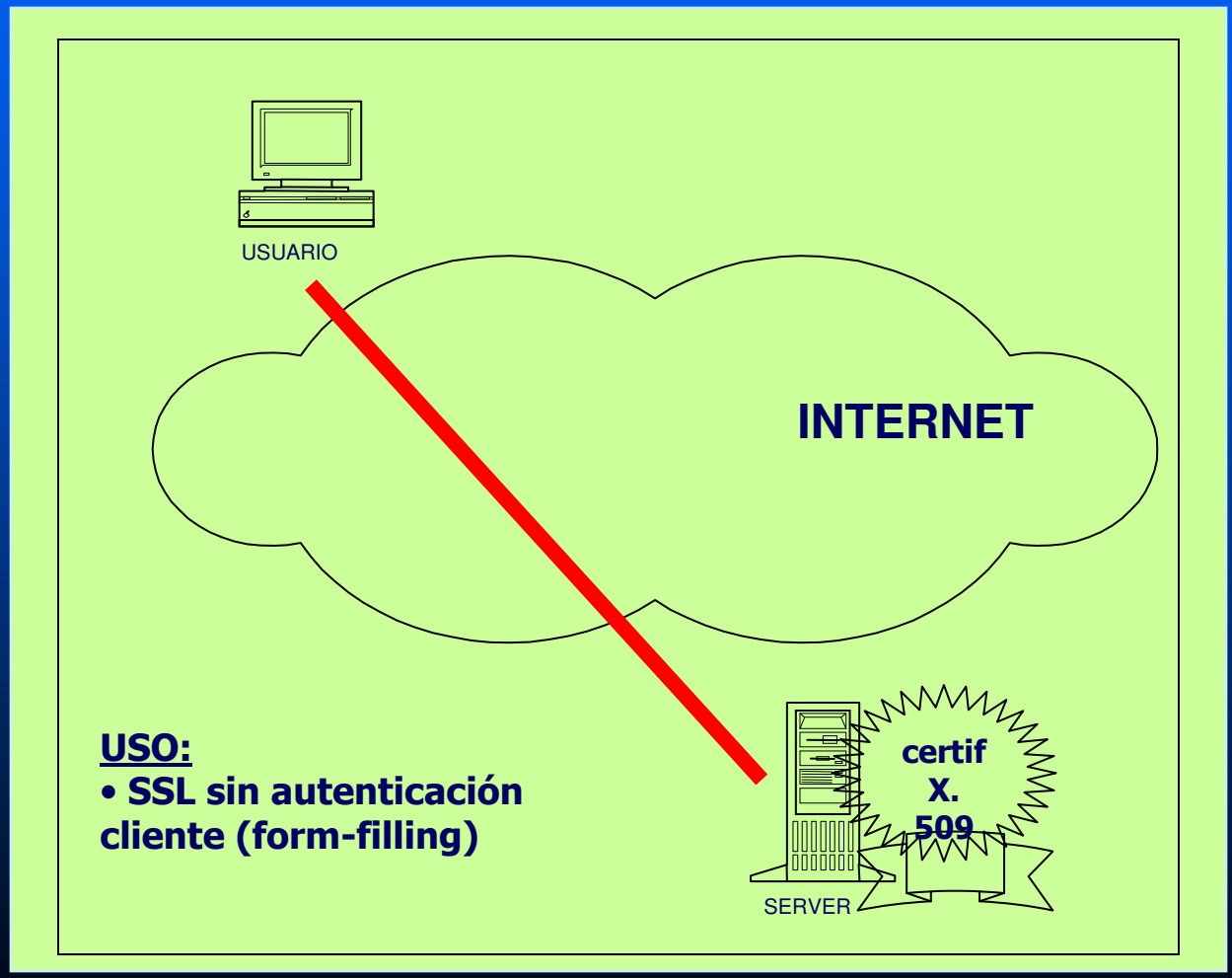
pero la realidad actual muestra el divorcio entre ambos....

www.interbank.com.pe
London Fire Brigade(londonfirebrigade.gov.uk)
Epson, China (www.epson.com.cn)
Poder Judicial de Costa Rica (www.poder-judicial.
Ministerio de Ciencia y Tecnología, de España (w
National Archives of Canada (www.archives.ca)
RISX Security (risx.mine.nu)
Black and Decker Corporation (www.bdk.com)
Headquarters Allied Land Forces Central Europe (LANDCENT) (www.landcent.nato.int)
Renault Italia (www.renault.it)
Banca Manzano (www.bancamanzano.it)
Banca Aimi (www.bancaimi.it)
Banca Popolare di Ravenna (www.bpr.it)
Technical Info, Jet Propulsion Labs (NASA) (techinfo.jpl.nasa.gov)
US Army Corps of Engineers, Portland District Home (cadd.nwp.usace.army.mil)
Computer Modeling and Simulation Department, Naval Surface Warfare Center
Secretaria de Comercio y Fomento Industrial (www.secofi-siem.gob.mx)
La Comisión Nacional Bancaria y de Valores (www.cnbv.gob.mx)
Microsoft Informatica Ltda (www.microsoft.com.br)
Organization of the Petroleum Exporting Countries (www.opec.org)
Lotería Nacional Sociedad del Estado (www.loteria-nacional.gov.ar)
Tower Argentina (ns2.tower.com.ar)

Fuente: http://www.attrition.org/mirror/attrition/index.html

LA SOLUCIÓN B2C ES....

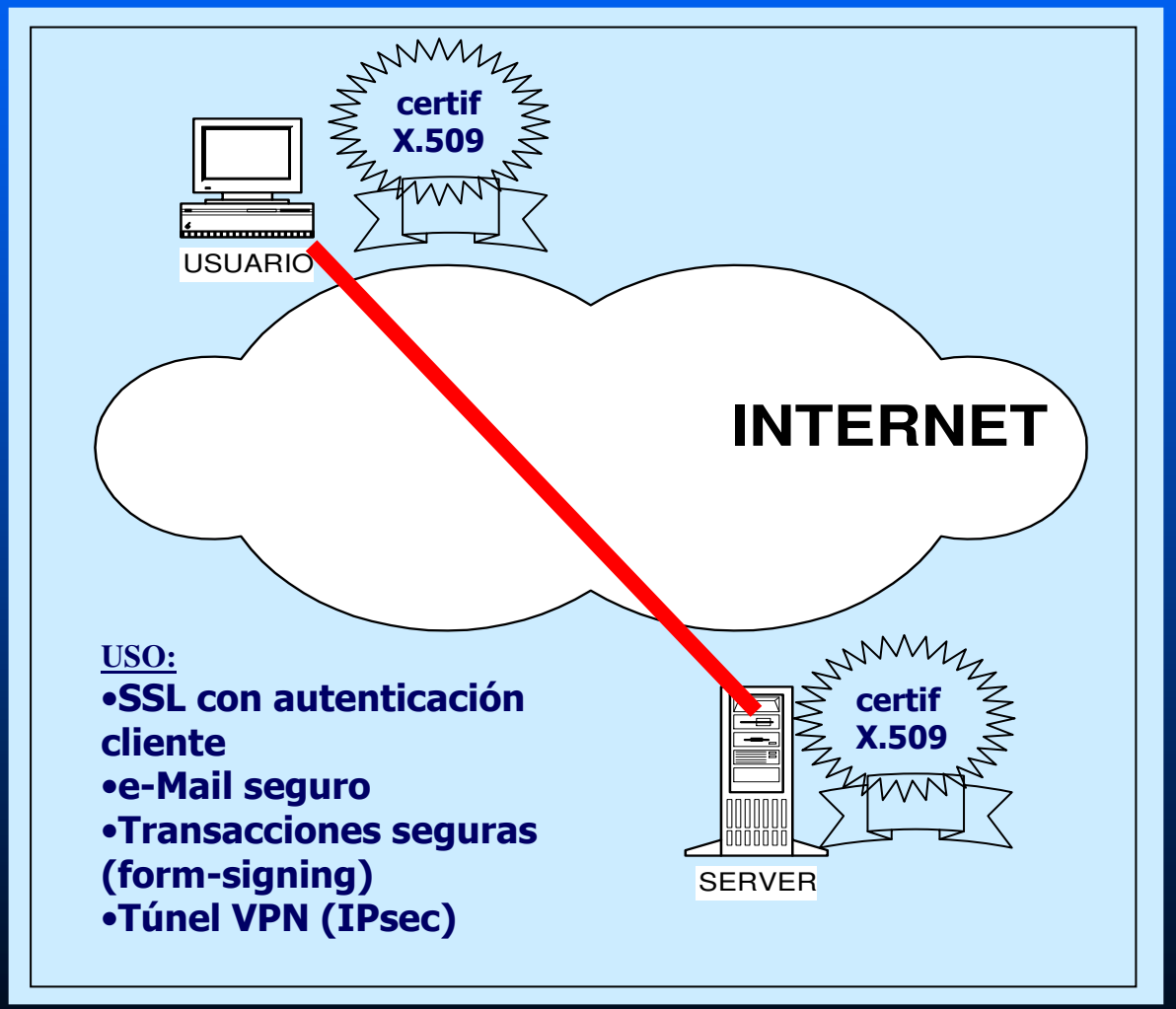
Autenticación del Servidor con Certificado Digital



PKI

Y LA SOLUCIÓN INTEGRAL ES...

Autenticación del Servidor y del Cliente con Certificados Digital

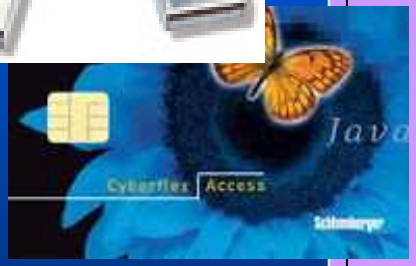


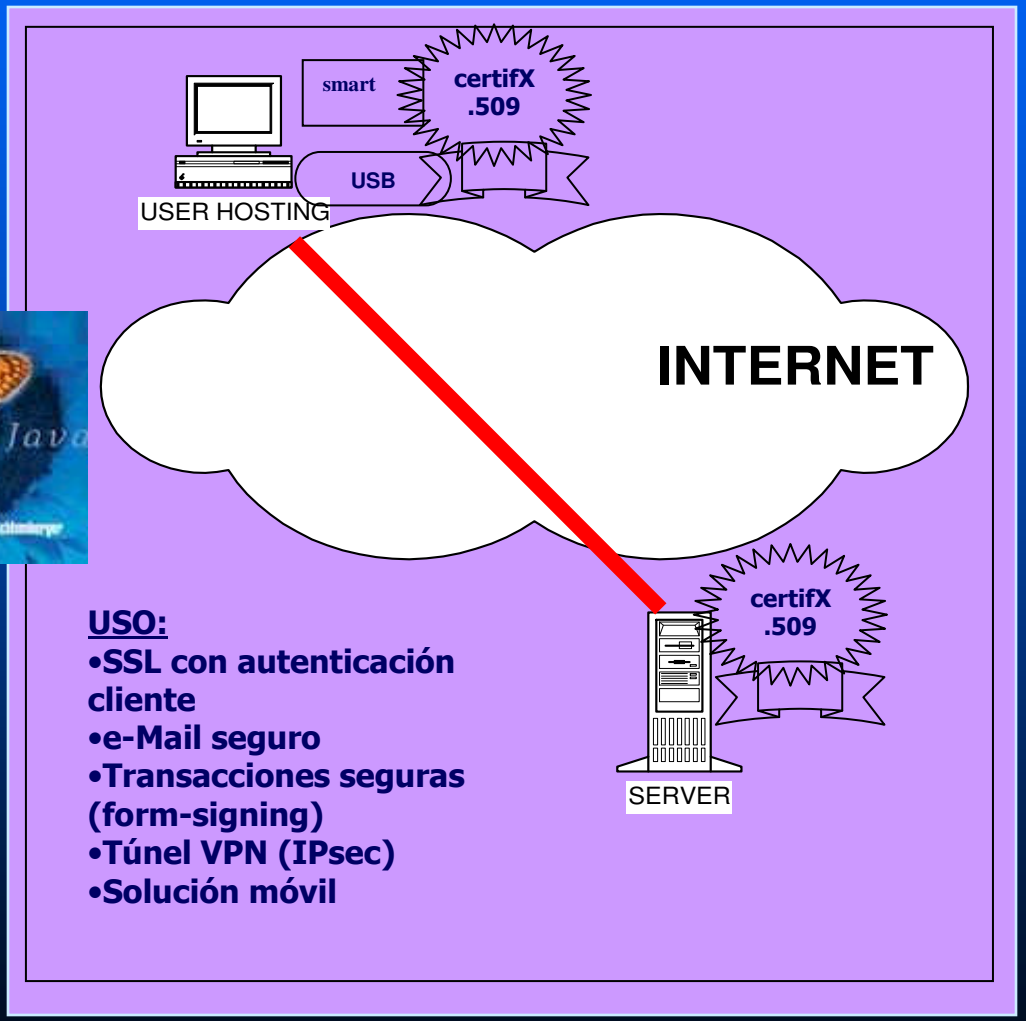
USO:

- **SSL con autenticación cliente**
- **e-Mail seguro**
- **Transacciones seguras (form-signing)**
- **Túnel VPN (IPsec)**

PKI

Y SE POTENCIA CON ALMACENAMIENTO PORTÁTIL Y CAPA BIOMÉTRICA...



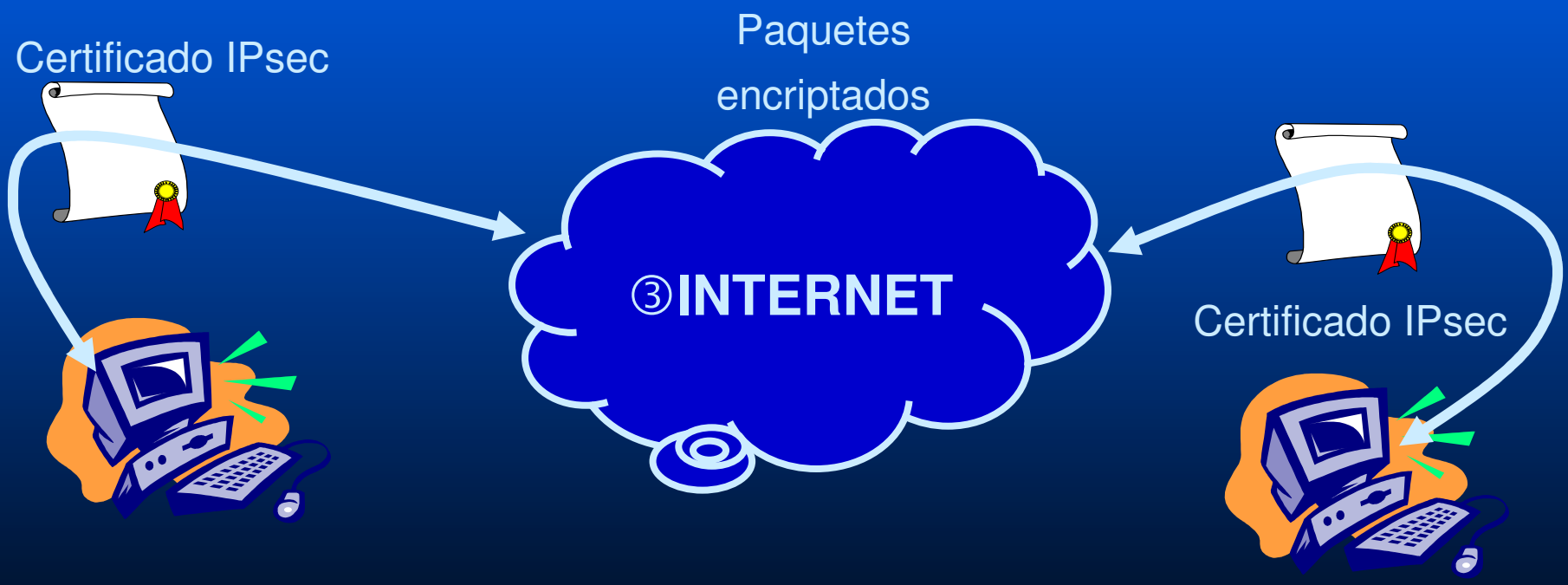


USO:

- **SSL con autenticación cliente**
- **e-Mail seguro**
- **Transacciones seguras (form-signing)**
- **Túnel VPN (IPsec)**
- **Solución móvil**

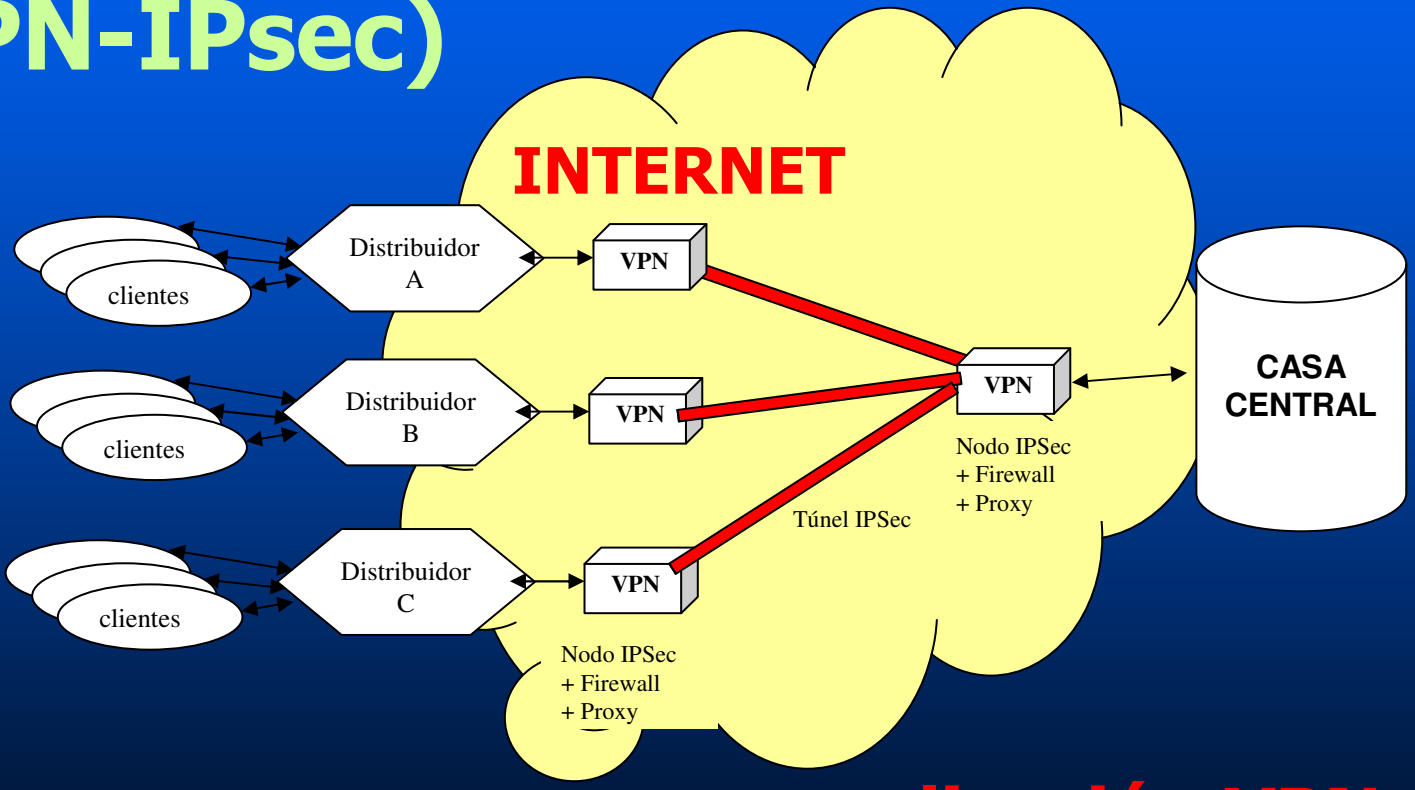
PKI

VPN (virtual private network)



RED PRIVADA VIRTUAL (VPN-IPsec)

Los nodos deben tener:
+Firewall (Packet Filtering)
+Proxy Server



aplicación VPN al e-Commerce (B2B)

Y aquí terminamos

E-MAIL

hugo@dc.uba.ar