http://glo.org.mx/~patux/

Introduccion a la Criptografia

Geronimo Orozco Martinez
Jose Luis Nuñez Becerra

Indice

Indice

- Firmas digitales
  - Funcionamiento
- Certificados digitales
- Critptografia Recapitulacion
- Protocolos que utilizan criptografia
- Aplicaciones que utilizan criptografia
- Organizaciones y Regulacion
- Metodos de evaluacion y selección de algoritmos modernos.
- Organizaciones estandar
- Organizaciones criptograficas
- Esfuerzos abiertos
- Implicaciones legales

Historia

- La criptografía es tan antigua como la escritura misma.
- Los egipcios usaron metodos criptográficos (escritura jeroglífica).
- A quien se le atribuye el primer método de encriptado es al Gral. Julio César.
- El libro más antiguo de criptografía data del siglo XIV.
- En el siglo XV destaca Leon Battista Alberti, considerado por muchos el padre de la ciptografía.
- En 1470 Leon Battista publica “Tratado de cifras” y en 1530 publica “Poligrafía”.

Historia

- En el siglo XVI destaca Girolamo Cardano.
- En el siglo XIX se utilizó mucho el método de “transposición”.
- La primer patente data de 1919 obre del holandes Alexander Koch y del alemán Arthur Sherbius.
- Arthur Sherbius inventó la “ENIGMA”.
- El mayor desarrollo de la criptografía se dió en el periodo de entreguerras.
- En 1975 Diffie y Hellman establecen bases teóricas de los algoritmos de llave pública.

Finalidad.

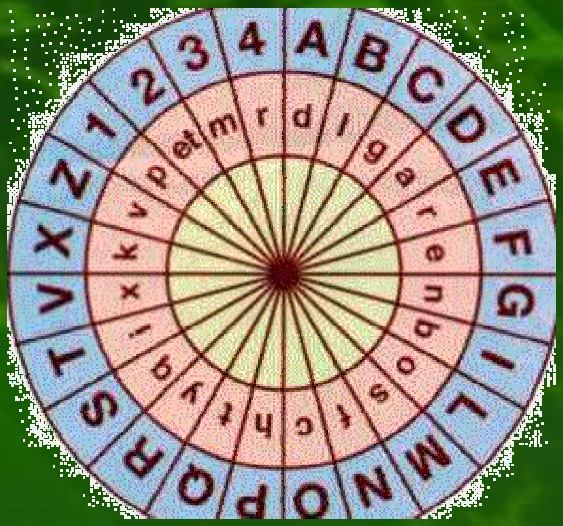
- Garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc).
- Asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser.
- Impedir que el contenido del mensaje enviado (criptograma) sea modificado en su tránsito.

Criptología.

Se conforma de matemáticos e investigadores que dedican sus valiosas neuronas para inventar nuevos algoritmos.

Abarca dos grandes areas:

- **Criptoanálisis.**
- **Criptografía.**



Criptoanálisis.

Defínción:

- **Se encarga de encontrar sistemas para descifrar la información que se transmiten a travéz de un medio.**

- **Es el conjunto de técnicas que intenta encontrar la clave utilizada entre dos comunicaciones.**

Criptografía.

Definición:

- **Proviene de las palabras "*criptos*" (oculto, secreto) y "*grafos*" (escritura).**

- **La criptografía es la ciencia de aplicar matemáticas complejas para aumentar la seguiridad de las transacciones electronicas (PKI).**

- **Se encarga de la seguridad en el envio de los datos (cifrado de información).**

Criptografía clásica.

Métodos criptográficos básicos.

- **SUSTITUCIÓN.**
  Consiste básicamente en sustituir los caracteres del mensaje inicial por otros; los nuevos caracteres pueden ser de cualquier tipo: letras, simbolos, digitos, etc....
  (Algoritmo de César, ROT13, ROT47, Vigénere)

- **ORDEN ALEATORIO.**
  (Transposición).

Criptografía clásica.

- ***Algoritmo de César.***

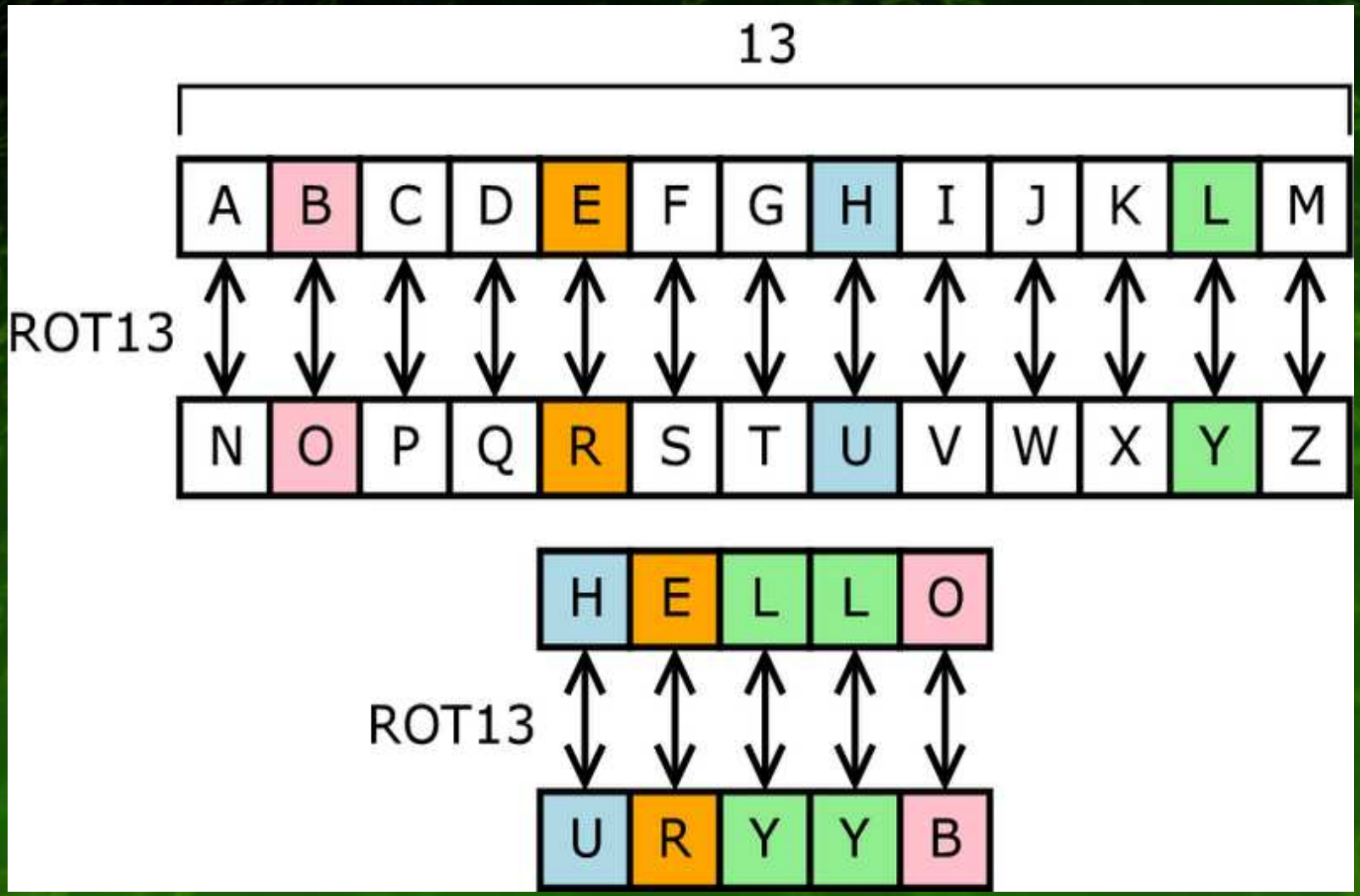
  El algoritmo de César, llamado así por que es el que empleaba Julio César, para enviar mensajes secretos, es uno de los algoritmos más simples que hay.

  Por ejemplo:

  A la letra 'A' le corresponde la 'D', a la letra 'B' la 'E' y así sucesivamente.....

Criptografía clásica.

- ***Algoritmo "ROT13".***



Criptografía clásica.

- ***Algoritmo "ROT47".***

Presenta tres variantes:

- **A diferencia del algoritmo ROT13, el algoritmo ROT47 toma el caracter que esta '47' caracteres antes del caracter original.**
- **El algoritmo ROT47 toma en cuenta todos los caracteres imprimibles.**
- **Hace distinciones entre mayúsculas y minúsculas.**

Criptografía clásica.

- ***<u>Sustitución por clave</u> (Vigénere,"Blaise de Vigénere").***

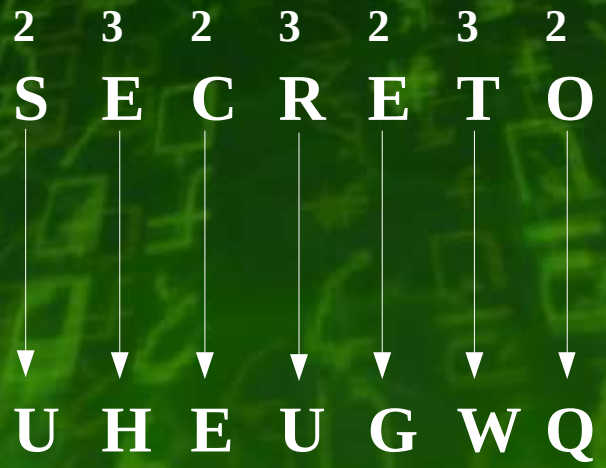
Una vez establecida la correspondencia entre alfabetos, la asignación de caracteres se realiza teniendo en cuenta la posición del carácter en el mensaje y el digito que le corresponde según la clave.

.....?????

EJEMPLO:

Dado el texto “SECRETO” con clave “23”, cifrar utilizando el método de sustitución por clave.

RESULTADO:



asi está mejor !!!

Criptografía clásica.

- ***Transposición.***

  Este tipo de mecanismos de cifrado no sustituye unos símbolos por otros, sino que cambia su orden dentro del texto.

  Consiste en colocar el texto en una tabla de 'n' columnas, y dar como texto cifrado los símbolos de una columna -ordenados de arriba a abajo- concatenados con la otra.

  La clave 'k' se compondría del número 'n' junto con el orden en el que se deben leer las columnas.

....?????

Criptografía clásica.

Por ejemplo:

Cifrar el texto “El perro de San Roque no tiene rabo“, con n = 5 y la permutación {3,2,5,1,4} como clave.

Posición

Leer

1	2	3	4	5
e	l		p	e
r	r	o		d
e		s	a	n
	r	o	q	u
e		n	o	
t	i	e	n	e
	r	a	b	o

Resultado:

“ osonealr r irednu eoere et p aqonb“

Seguridad en la obscuridad

- **Marzo 1997**: Counterpane Systmes y UC Berkeley colaboraron para desifrar el *Cellular Message Algorithm* (CMEA).
- **Noviembre 1999:** Programadores noruegos del grupo *Masters of Reverse Engineering* (MoRE) desifraron con éxito el *Content Scramblig System* (CSS) que se uso para cifrar los DVD.
- **Noviembre 2000:** Adi Shamir, desifro una de las series de algoritmos A5 usadas para proteger conversaciones por telefonos celulares digitales en mas de 200 millones de telefonos digitales GSM.

Todos estos algoritmos se desarrollaron en secreto y no soportaron la revision abierta de los criptoanalistas.

Criptografía Simetrica

- Método criptográfico que usa una misma clave para cifrar y para descifrar mensajes.
- Numero aleatorio de la longitud correcta.
- Toman el texto claro como entrada y usando la *clave simetrica* sacan una versión, cifrada del texto. (texto cifrado).

Criptografía Simetrica Algoritmos

Cifrado por maquinas de substitucion polialfabetico

- Enigma
- Purple
- SIGABA
- TypeX

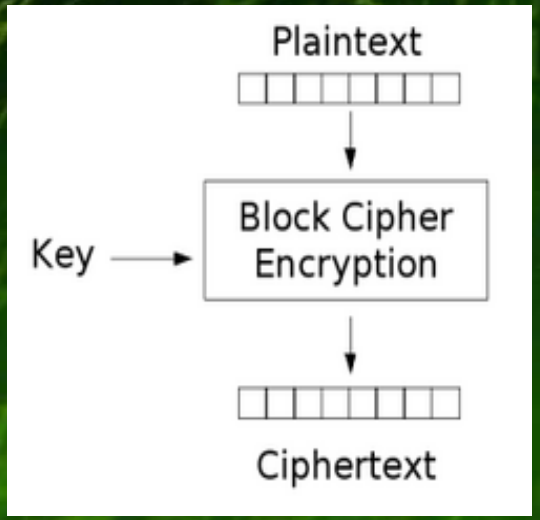
Criptografía Simetrica Algoritmos

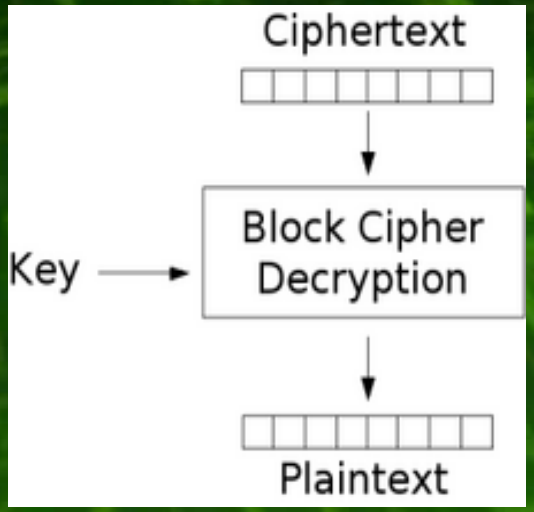
Cifrado de flujo (Stream Cipher)

- RC4
- A5/1, A5/2
- Chameleon
- FISH
- Helix
- ISAAC
- Panama
- Pike
- SEAL
- SOBER
- SOBER-128
- WAKE

Criptografía Simetrica Algoritmos

Cifrado de bloque (Block Cipher)





Criptografía Simetrica Algoritmos

Cifrado de bloque (Block Cipher)

- 3-Way
- AES
- Blowfish
- Camellia
- CAST-128
- CAST-256
- CMEA
- DEAL
- DES
- DEX-X
- FEAL
- GDES
- GOST
- IDEA
- Iraqui Block cipher
- KASUMI
- Khafre
- KHAZAD
- Khufu
- LOKI89/91
- Lucifer
- MAGENTA
- MARS
- MISTY1
- MMB
- RC2
- Red Pike
- S-1
- SAFER
- Serpent
- SHARK
- Skipjack
- Square
- TEA
- Tripe DES
- Twofish
- RC5
- RC6
- XTEA

Criptografía Simetrica

Como trabaja ?

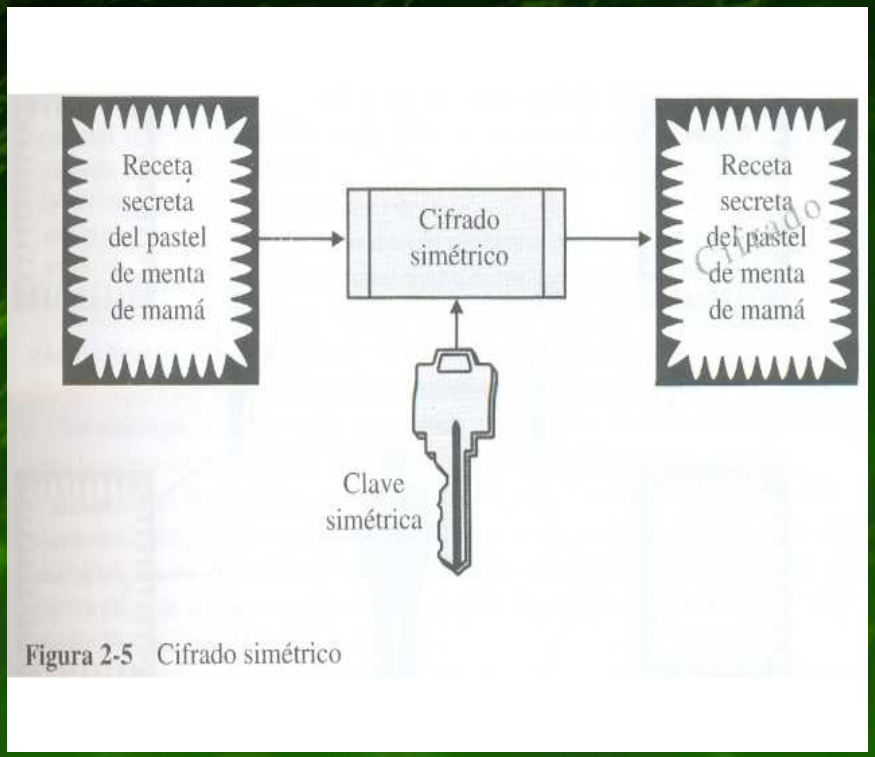


Figura 2-5 Cifrado simétrico

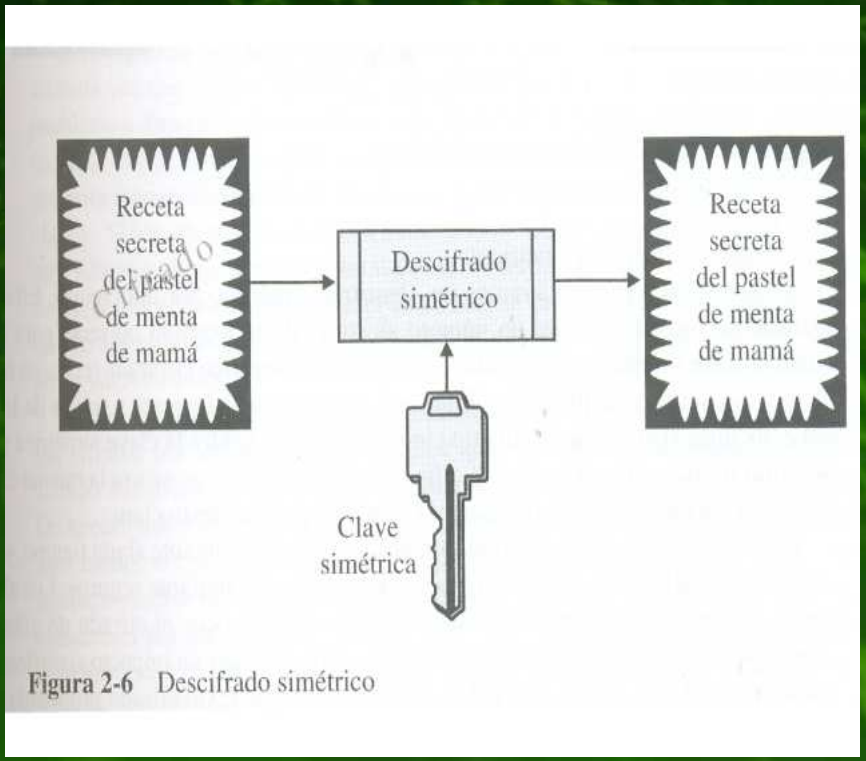


Figura 2-6 Descifrado simétrico

Criptografía Simetrica

DES usa una clave de 56 bits

2^56 claves posibles.
72,057,594,037,927,936

3DES,Blowfish e IDEA usan claves de 128bits.

2^128 claves posibles.
340,282,366,920,938,463,463,374,607,431,768,211,456

Criptografía Simetrica Ejemplo:

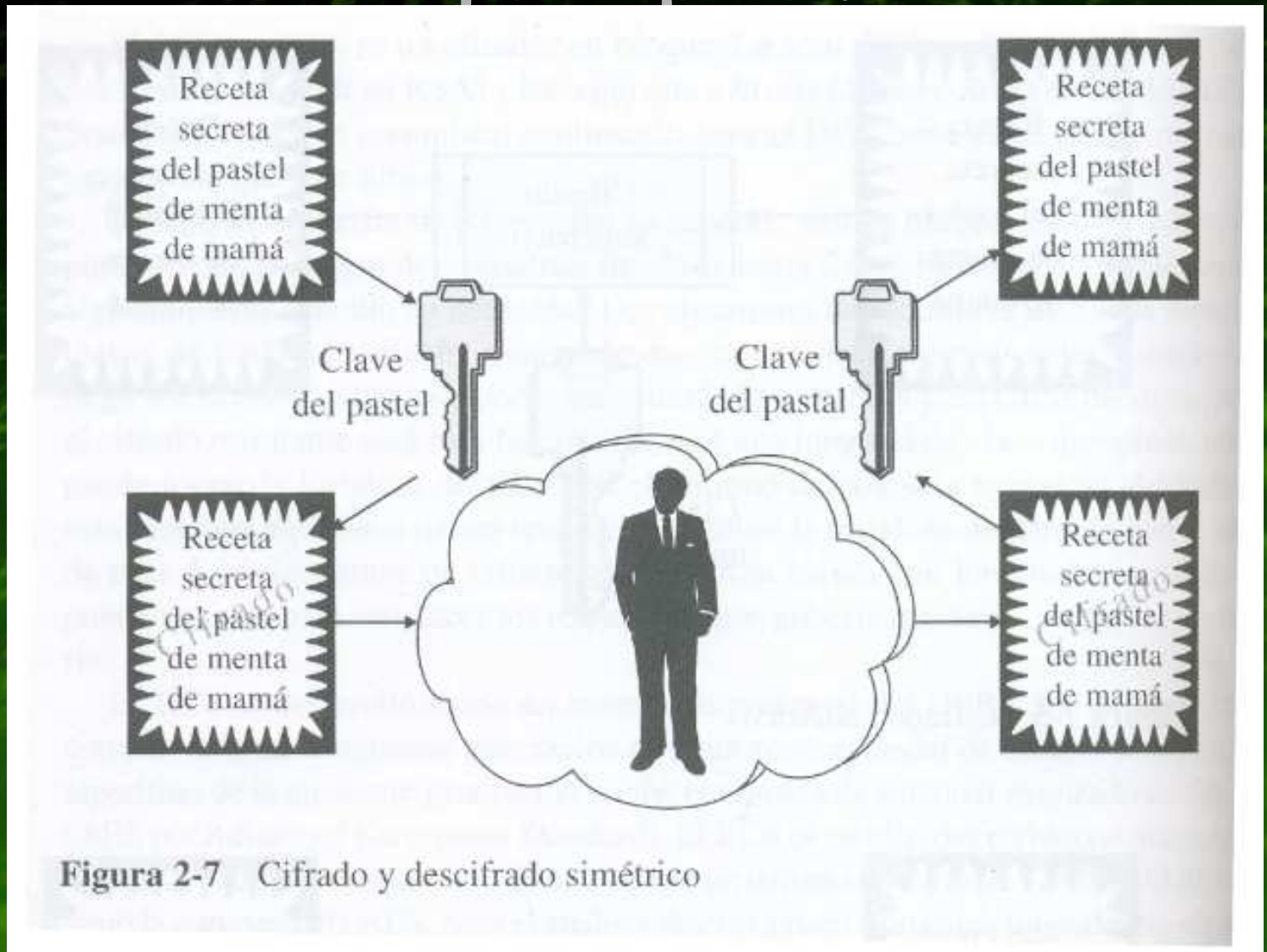


Figura 2-7 Cifrado y descifrado simétrico

Criptografía Simetrica

INCONVENIENTES

- El intercambio de claves

- Para que **n** numero de personas se comuniquen necesitan: **n(n-1)/2** claves para comunicarse entre si, y estas no se vuelven a utilizar una vez usadas.

  Ej: 100 personas= 4450 claves cada una

Criptografía Simetrica

Recapitulacion

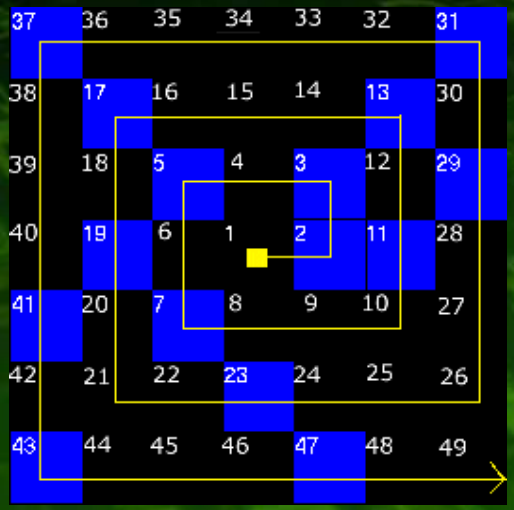
- Se utiliza la misma clave para cifrar y descifrar.
- El cifrado simetrico es rapido.
- El cifrado simetrico es seguro.
- El texto cifrado que resulta de un cifrado es compacto.
- Dado que la clave simétrica debe llegar al receptor, el cifrado simétrico esta sujeto a la intercepción.
- El número de claves en la criptografía simétrica es, aproximadamente, el cuadrado del número de participantes y, por tanto, no tiene una buena escalabilidad en poblaciones muy numerosas.
- La criptografía simétrica requiere una administración compleja de claves.
- La criptografía simetrica no se ajusta a las firmas digitales o a la aceptación.

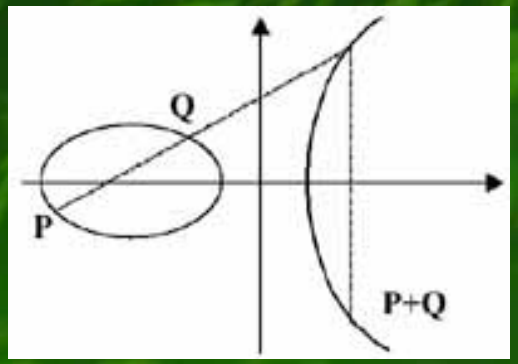
Criptografía Asimetrica

- Método criptográfico que usa un par de claves para el envío de mensajes. Una publica y otra privada.
- El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.
- Se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos.
- Se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

Criptografía Asimetrica Algoritmos

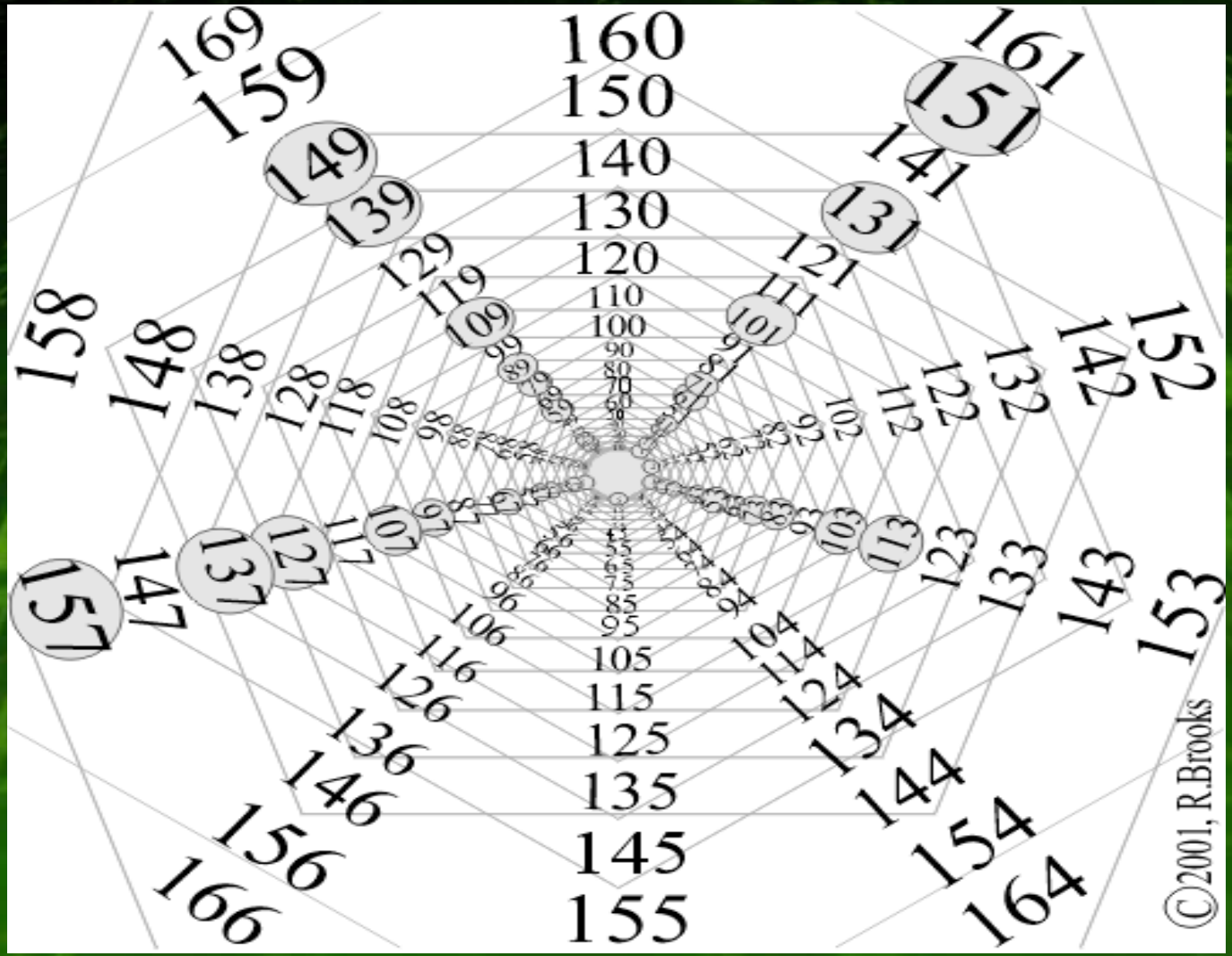
- Diffie- Hellan
- RSA
- DSA *(Digital Signature Algotithm)*
- ElGamal
- Criptografía de curva elíptica (*ECC*)





Criptografía Asimetrica

Distribucion de los numeros primos



Criptografía Asimetrica Algoritmos

- Costo equivalencia en tamaño de claves

Clave Simetrica	Clave ECC	Clave RSA	Tiempo para descifrarlo	Maquinas	Memoria
56	112	420	Menos de 5 minutos	10000	Trivial
80	160	760	600 meses	4300	4GB
96	192	1020	3 millones de años	114	170GB
128	256	1620	10E16 años	0.16	120TB

* http://www.nullify.org/docs/bulletin13/bulletin13.html

Criptografía Asimetrica
Como funciona?

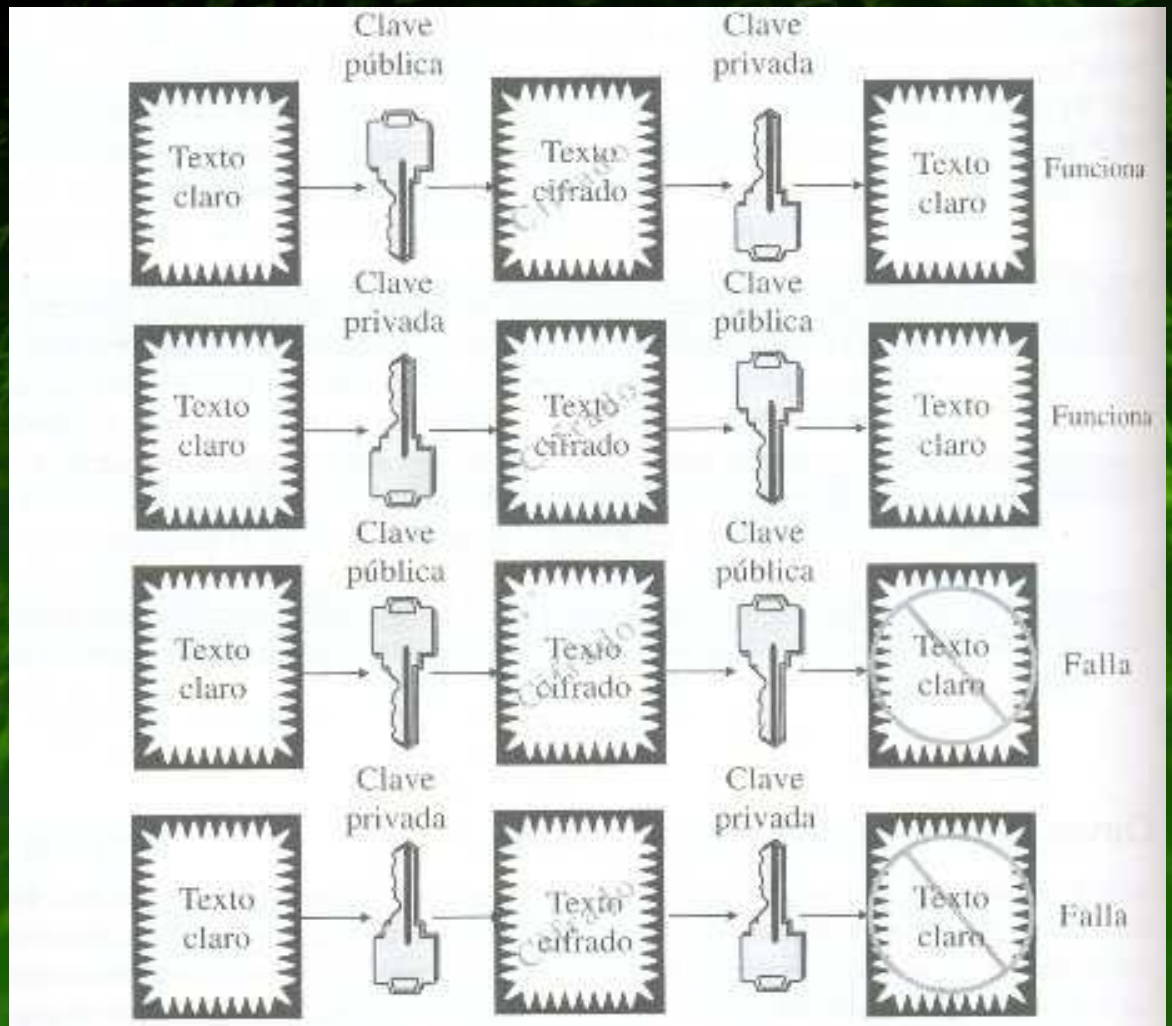


Figura 2-8 Claves públicas y privadas

Criptografía Asimetrica Ejemplo:

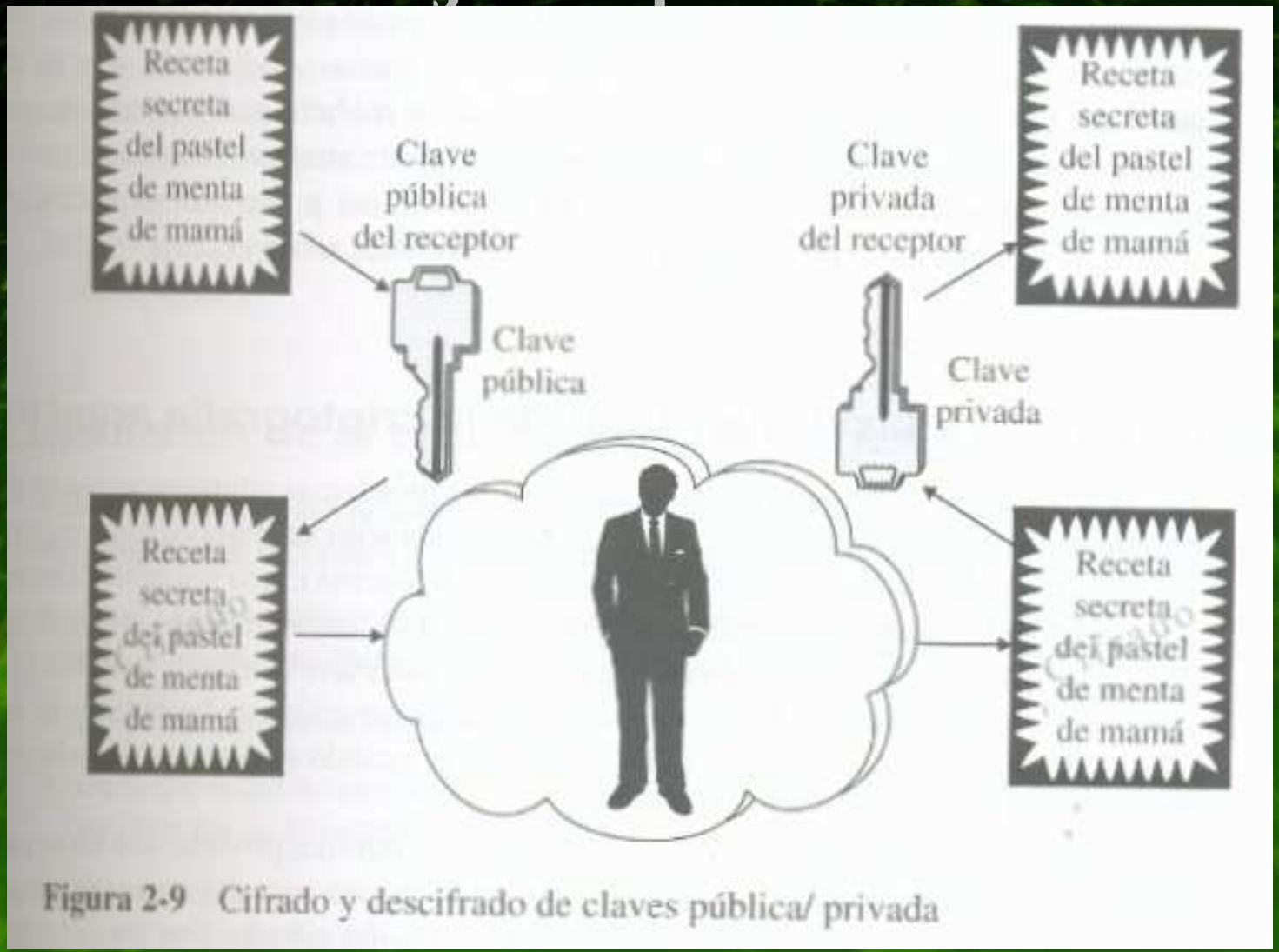


Figura 2-9 Cifrado y descifrado de claves pública/ privada

Criptografía Asimetrica

INCONVENIENTES

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje cifrado ocupa mas espacio que el original.
- El sistema de criptografía de curva elíptica representa una alternativa menos costosa para este tipo de problemas.

Criptografía Asimetrica

Recapitulacion

- Lo que esta cifrado con una clave (publica o privada) solo se puede descifrar con la otra clave (privada o publica).
- El cifrado asimetrico es seguro.
- No sufre por la interceptacion de claves.
- No tiene los problemas complejos de distribucion de claves.
- No exige una relacion previa entre las partes para hacer el intercambio de claves.
- Soporta firmas digitales y aceptacion.
- Es relativamente lento.
- Expande el texto cifrado.

Criptografía Asimetrica

La Solucion ideal

- Debe ser segura.
- El cifrado debe ser rapido.
- El texto cifrado debe ser compacto.
- La solucion debe servir en escalas de grandes poblaciones.
- La solucion no debe ser vulnerable a la interceptacion de claves.
- La solucion no debe requerir una relacion previa entre las partes.
- La solucion debe soportar firmas digitales y aceptacion.

Criptografía Hibrida

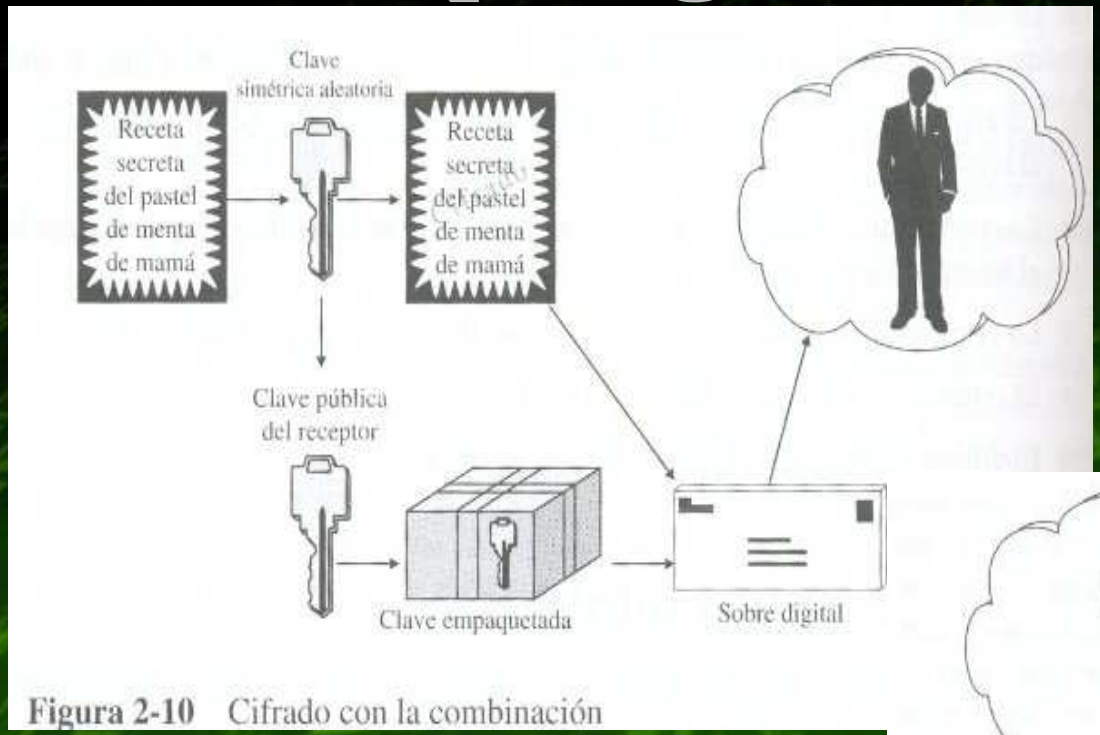


Figura 2-10 Cifrado con la combinación

PGP y GnuPG
Utilizan criptografia hibrida

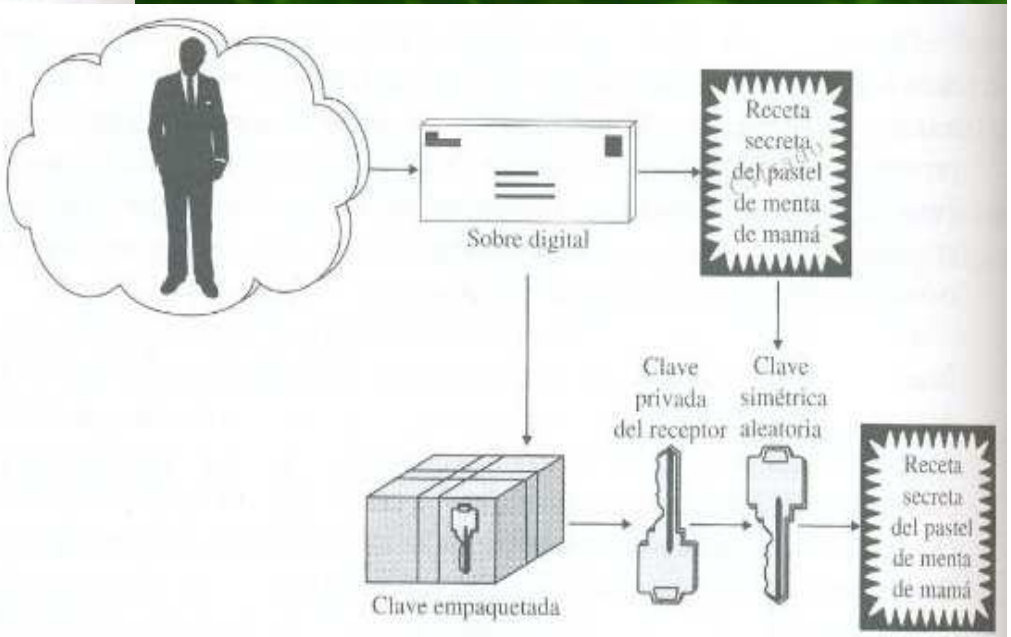


Figura 2-11 Descifrado con la combinación

Firmas digitales

- La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido.

- Método criptográfico que asegura la integridad de los mismos así como la identidad del remitente

Hashes

- Función múltiple que asigna a su entrada un valor dentro de un conjunto finito, eneralmente un subconjunto de los números naturales.

- Son usadas en múltiples aplicaciones, como los arrays asociativos, la firma digital, etc.

- Ejemplo: **f(x) = x mod 37**

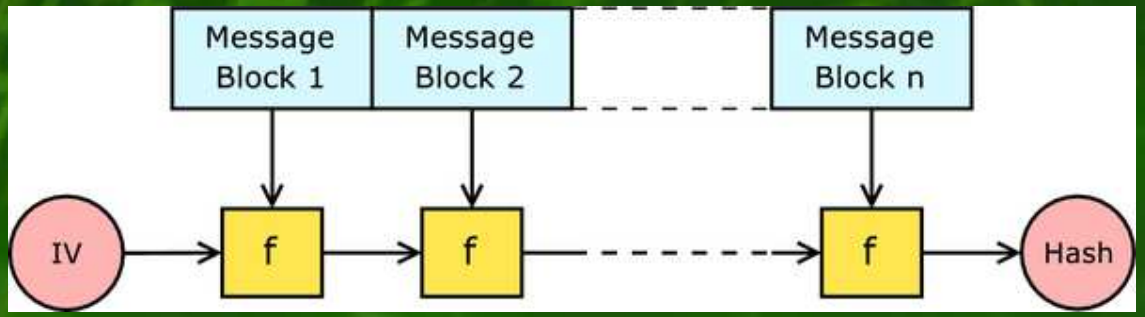
Hashes criptograficos

- Es una funcion hash con ciertas propiedades adicionales de seguridad y hacerlo usable para ser usado como primitiva en aplicaciones con informacion segura.
  - Autentificacion
  - Verificar Integridad del mensaje
- Un algoritmo hash toma un gran bloque de datos y lo comprime en una huella digital (*fingerprint)* o reseña(*digest)* de los datos originales.

Hashes criptograficos

Propiedades

- No se puede poner a funcionar el hash hacia atrás y recuperar algo del texto claro inicial.
- La reseña resultante no dira nada sobre el texto claro inicial.
- No es factible crear/descubrir texto claro que verifique un valor especifico.



Hashes criptograficos

- **HAVAL**
- **MD2** (*Message Digest Algorithm*)
- **MD4**
- **MD5**
- **N-Hash**
- **RIPEMD-160**
- **SHA-0 SHA-1** *(Secure Hash Algorithm)*
- **Snefru**
- **Tiguer**
- **Whirlpool**

Firmas digitales funcionamiento

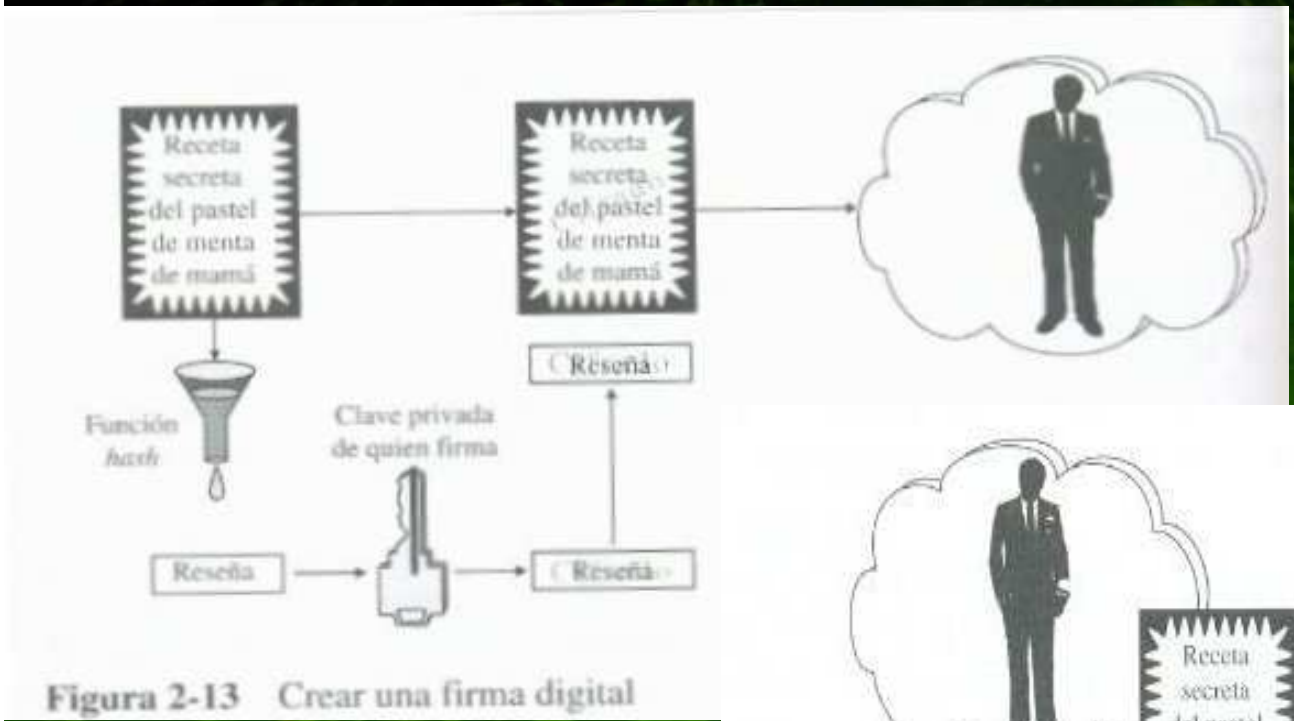


Figura 2-13 Crear una firma digital

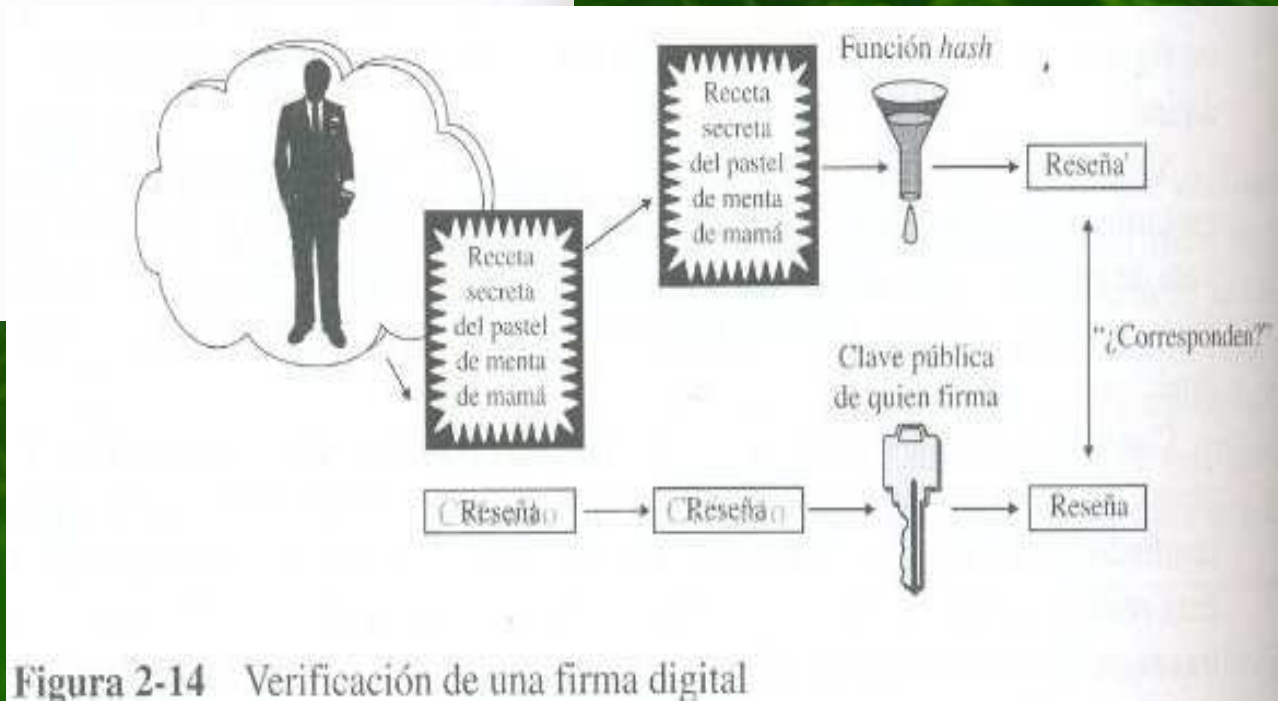


Figura 2-14 Verificación de una firma digital

Certificados digitales

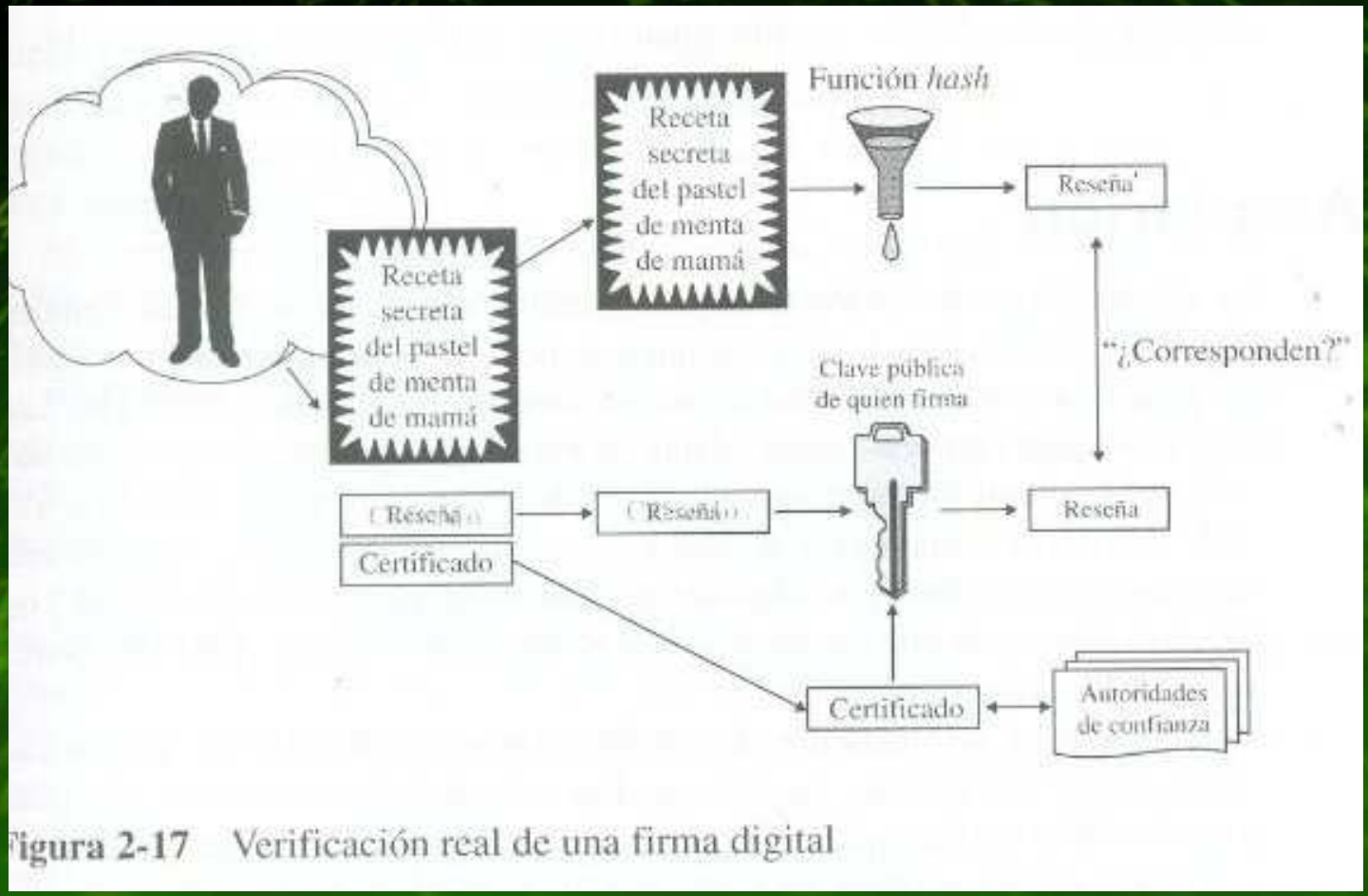


Figura 2-17 Verificación real de una firma digital

Criptografia

Recapitulacion

- Las mejores aplicaciones de criptografia combinan algoritmos simetricos y asimetricos.
- Con la combinacion, las claves simetricas suelen ser efimeras, Las claves simetricas se utilizan para el cifrado en bloques.
- Las claves asimetricas se usan para envolver las claves simetricas y protegerlas durante su trancito, lo mismo que para cifrar verificaciones *(hashes)* de datos para crear firmas digitales.
- Las claves publicas estan protegidas del engaño al codificarlas en un certificado digital, junto con la identidad del propietario.
- Las autoridades de confianza firman certificados digitales. La mayor parte del SW contiene listas previamente cargadas de dichas autoridades.
- Las firmas digitales deben incluir una marca de hora precisa y confiable si van a resitir el rechazo.

Criptografia
Protocolos

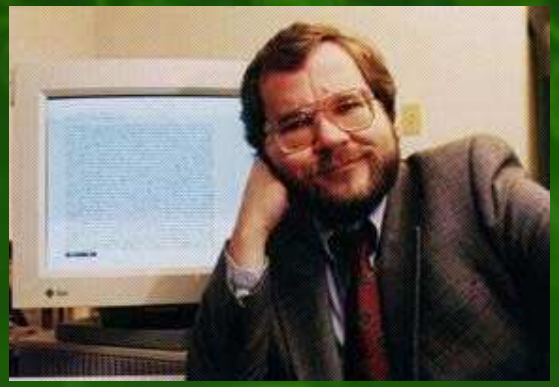
Protocolos que utilizan criptografia

- **TLS** *(Transport Layer Security)*
- **SSL** (Secure Sockets Layer)
- **SET** *(Secure electronic transaction)*
- **OpenPGP**
- **DSS** *(Digital Satellite System)*
- **SSH**

Criptografia
Aplicaciones

Aplicaciones de la criptografia

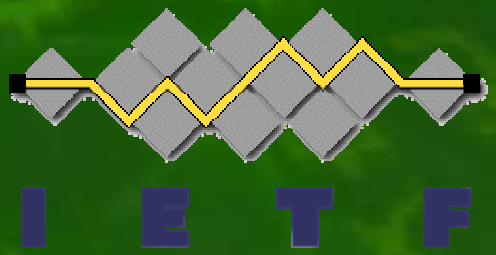
- **SOFTWARE:**
  - **PGP** *(Prety Good Privacy) Phil Zimmerman*
  - **GnuPG** *(GNU Privacy Guard) Free Software Foundation*
- **VOTO ELECTRONICO**
- **PAGO ELECTRONICO**
  - Transacciones seguras
  - Monedero electronico.



Criptografia

Metodos de evaluacion y selección de algoritmos modernos.

- **Organizaciones Estandar:**
  - **The Federal Information Processing Standards Publication program**
    - A cargo del **NIST** *(National Institute of Standards and Technology: USA)*
  - **ANSI** *(American National Standards Institute)*
  - **ISO** *(International Organization for Standardization)*
  - **IEEE** *(Institute of Electrical and Electronics Engineers)*
  - **IETF** *(Internet Engineering Task Force)*



Criptografia

Metodos de evaluacion y selección de algoritmos modernos.

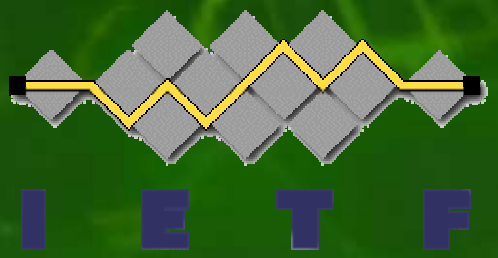
- **Organizaciones Criptograficas:**
  - **NSA** *(National Security Agency) USA*
  - **GCHQ** *(Government Communications Headquarters) UK government*
  - **Communications Security Establishment** *(CSE) — Canadian intelligence agency.*

Criptografia

Metodos de evaluacion y selección de algoritmos modernos.

- **Esfuerzos Abiertos:**
  - **DES** *(Data Encryption Standard) (NIST)*
  - **AES** *(Data Encryption Standard) (NIST)*
  - ***NESSIE*** *(New European Schemes for Signatures, Integrity, and Encryption) (European Union)*
  - ***CRYPTREC*** *(Cryptography Research and Evaluation Committee) (Japanese Government)*
  - **IETF** *(Internet Engineering Task Force)*
  - ***CrypTool project*** *(eLearning Program for Cryptography and cryptanalysis)*

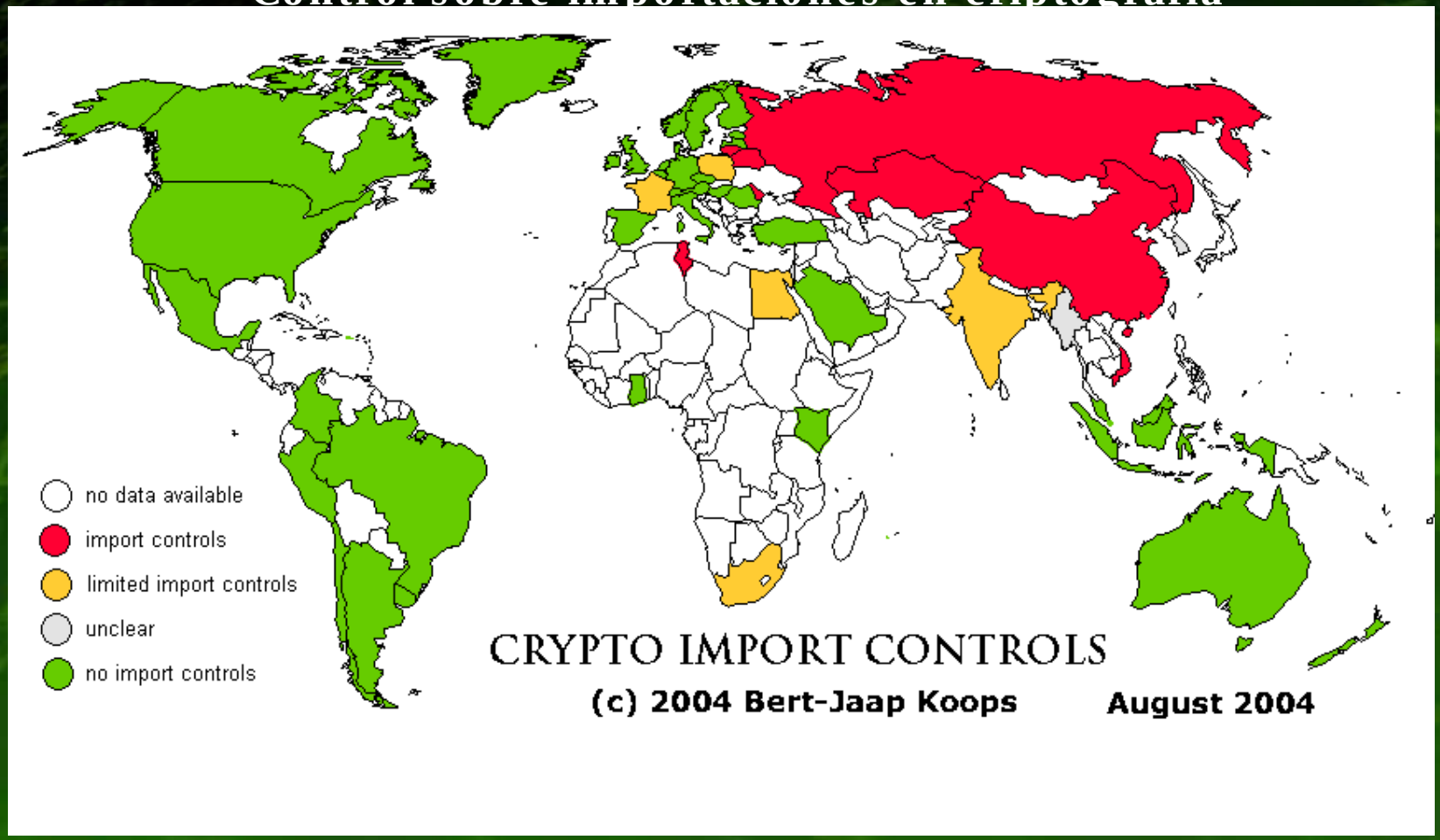
NIST NESSIE



CrypTool

Criptografia
Implicaciones legales

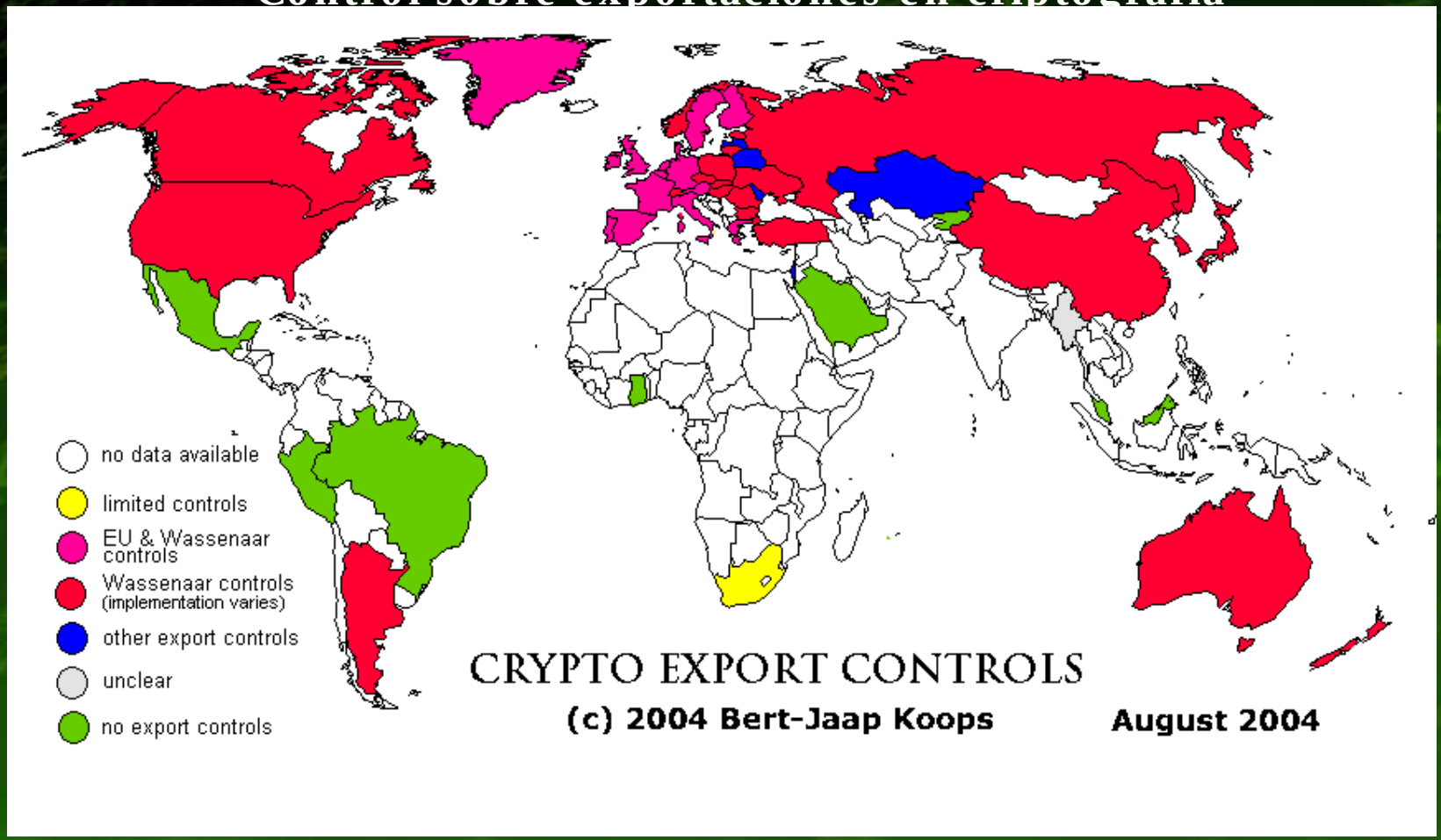
Control sobre importaciones en criptografia



* http://rechten.uvt.nl/koops/cryptolaw/cls-sum.htm

Criptografia
Implicaciones legales

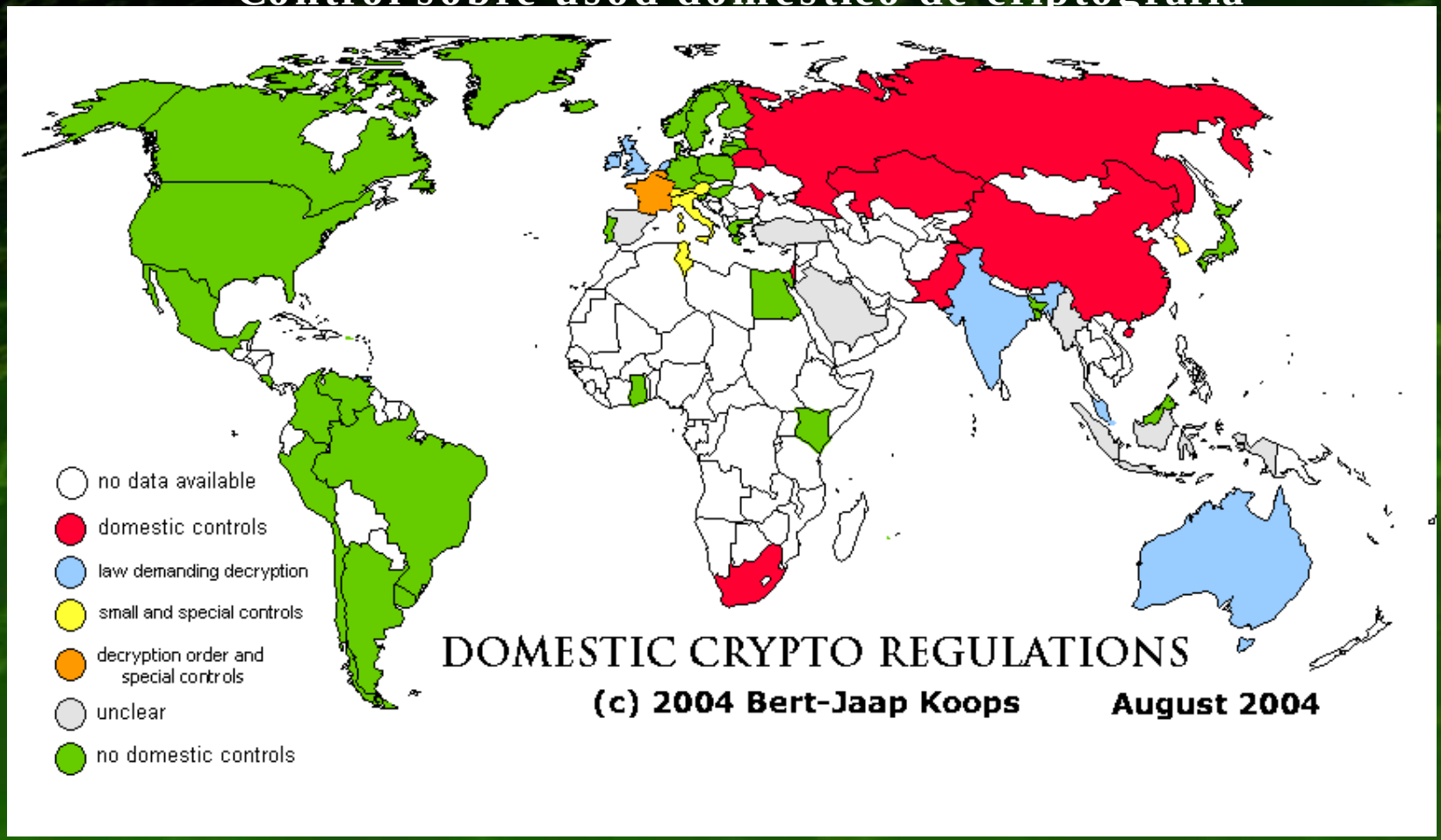
Control sobre exportaciones en criptografia



* http://rechten.uvt.nl/koops/cryptolaw/cls-sum.htm

Criptografia
Implicaciones legales

Control sobre usod domestico de criptografia



* http://rechten.uvt.nl/koops/cryptolaw/cls-sum.htm

Criptografia
RERFERENCIAS

- **Cifrado Simetrico, Asimetrico e Hibrido:** PKI Infraestructura de claves publicas (Andrew Nash, William Duane, Celia Joseph y Derek Brink) Osborne Mc. Graw-Hill
- **Comunicaciones y Redes de Computadoras:** (William Stallings) Prentice Hall.
- **Historia:** http://leo.worldonline.es/jlquijad/histo.htm
- **Histora y conceptos generales:** http://www.ciberia.ya.com/rvalle2001/criptografia2.htm
- **Codigo root13 root47 y vigenere:** http://www.udlap.mx/~is111936/oto02/programas/
- **Descripcion criptografia, algoritmos....**
  - **Enciclopedia libre:**
    - http://en.wikipedia.org
    - http://es.wikipedia.org
    - http://en.wikipedia.org/wiki/Topics_in_cryptography
  - **Numeros primos y propiedades:**
    - http://fdonea.tripod.com/primes.htm
    - http://www.hermetic.ch/pns/pns.htm
    - http://www.mersenne.org/
    - -- Codigo en C para sacar el numero primo mas grande
    - http://fabrice.bellard.free.fr/mersenne.html

Criptografia
REFERENCIAS

- **Boletin RSA sobre el tamaño de llames:** http://www.nullify.org/docs/bulletin13/bulletin13.html (Robert D. Silverman)
- -- Codigo en C de: AES,RC4,3DES,MD5,SHA1,SHA2
  - http://www.cr0.net:8040/code/crypto/
- A Javascript SHA-1 calculator showing intermediate values in the calculation
  - http://www.cs.eku.edu/faculty/styer/460/Encrypt/JS-SHA1.html
- **Algoritmo RSA**
  - http://daniellerch.com/papers/html/algoritmo_rsa.html
- **Preguntas frecuentes sobre criptografia: http://www.mindspring.com/~schlafly/crypto/faq.htm**
- **GnuPG:** http://www.gnupg.org/
- **PGP Corportation:** http://www.pgp.com/
- **PGP International:** http://www.pgpi.org/
- **OpenPGP Alliance:** http://www.openpgp.org/
- **Protocolo SSH:** http://www.ietf.org/html.charters/secsh-charter.html
- **OpenSSL:** http://www.openssl.org/
- **OpenSSH:** http://www.openssh.org/

Criptografia
REFERENCIAS

- **Cripto Law Survey:** http://rechten.uvt.nl/koops/cryptolaw/index.htm (© Bert-Jaap Koops)
- **ORGANIZACIONES:**
  - **National Institute of Standards and Technology: http://www.nist.gov/**
  - **Federal Information Processing Standard:** http://www.itl.nist.gov/fipspubs
  - **American National Standards Institute:** http://www.ansi.org/
  - **International Organization for Standardization:** http://www.iso.org/
  - **Institute of Electrical and Electronics Engineers:** http://www.ieee.org/
  - **Internet Engineering Task Force:** http://www.ietf.org/ietf_chairs_year.html
  - **National Security Agency:** http://www.nsa.gov/
  - **Government Communications Headquarters:** http://www.gchq.gov.uk/
  - **Communications Security Establishment:** http://www.cse-cst.gc.ca/
  - **NESSIE:** http://www.cryptonessie.org/
  - **Cryptography Research and Evaluation Committee:** http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html
  - **CryptTool:** http://www.cryptool.org/

Criptografia
PREGUNTAS?