Seguridad y Criptografía

Version preliminar del manual V .78

Roxana Bassi rox@arda.com.ar

Colaboradores especiales:

Bruce Tober octobersdad@crecon.demon.co.uk

Este manual esta dedicado a Paul Zimmerman, el autor del PGP.

"They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."
“Aquellos que resignan libertades esenciales para obtener una seguridad temporal, no se merecen ni libertad ni seguridad”
Benjamin Franklin

"Civilization is the progress toward a society of privacy.
The savage's whole existence is public, ruled by the laws of his tribe.
Civilization is the process of setting man free from men."
“Civilización es el progreso hacia una sociedad de privacidad.
La existencia completa de un hombre primitivo es publica,
sujeta a las leyes de su tribu.
Civilización es el proceso de liberar al hombre de los hombres”
Ayn Rand

ÍNDICE

INTRODUCCIÓN..... 7

LA PROTECCIÓN DE TODOS LOS DÍAS 8

LAS PREGUNTAS QUE DEBE HACERSE PARA ELEGIR UNA FORMA DE PROTECCIÓN ADECUADA 8

FORMAS USUALES DE PENETRACIÓN Y SU SOLUCIÓN 9

COMO ELEGIR UNA PASSWORD (CLAVE DE ACCESO)..... 11

COMO ELEGIR UNA PASS PHRASE (FRASE CLAVE) 12

ENCRIPTACIÓN 13

INTRODUCCIÓN Y CONCEPTOS 13

LOS SISTEMAS DE CLAVE PÚBLICA Y CLAVE PRIVADA 13

AUTENTICACIÓN O FIRMA ELECTRÓNICA 14

TÉCNICAS COMBINADAS: ENCRIPTACIÓN Y AUTENTICACIÓN..... 14

TÉCNICAS DE ENCRIPTACIÓN 15

USANDO EL PGP 18

Copyright y derechos de uso 18

Tabla rápida de comandos PGP 19

RIESGOS DEL COMERCIO ELECTRÓNICO 24

MEDIDAS DE SEGURIDAD 24

APÉNDICES..... 25

CONTENIDOS DEL DISKETTE 25

REFERENCIAS: 25

NEWSGROUPS: 25

MAILING LISTS 26

SOFTWARE DE ENCRIPTACION 26

GLOSARIO 27

Introducción

Internet, la red de redes de la Humanidad, nos ha dado una nueva forma de comunicacion global, tal vez tan revolucionaria como lo fueron el telégrafo o el teléfono en su momento.

Pero este nuevo canal de comunicacion también significa nuevas formas de "exposición" al robo de información. El comercio electrónico en Internet está detenido por una simple causa: aun no se logró una forma en que el cliente pueda pagar en forma fácil, segura y autentica.

El mismo método de "packet switching" de Internet, que al romper un mensaje en varias partes que viajan en forma independiente, nos garantiza velocidad de transmisión y capacidad de elección de rutas, también nos esta ofreciendo una grieta por la que nuestros mensajes están expuestos a ojos extraños. Piense que su mail para llegar a destino pasa por 30 o 40 servers distintos...¿que pasaría si en uno solo de ellos el Sysop decidiera guardarse una copia? Sin embargo, no hay necesidad de ponerse paranoico: ¿Acaso no hay mas posibilidad de que al pagar una cena en el restaurante un mozo copie nuestro número de tarjeta de crédito?

No hay una forma cien por ciento segura de proteger nuestra información: una canal de comunicación publico como es la Internet implica que uno puede salir al mundo, pero también que, con la suficiente astucia y conocimientos, alguien del mundo puede penetrar a nuestro sistema. Por algo el Pentágono Norteamericano no posee una conexión on-line a Internet: sus datos hacia el exterior y desde el exterior se transfieren en un CD-ROM, que es exhaustivamente chequeado antes de entrar al sistema.

El de la criptografia es, además, un tema que no escapa a la política mundial: muchos gobiernos (entre ellos el de Argentina) están oponiéndose a el uso de la criptografia cuando el método es tan seguro que ni ellos tienen el medio para descifrarlo

Por eso es importante recordar que ningún algoritmo de encriptación es indescifrable: simplemente es una cuestión de habilidad, tiempo y esfuerzo, que se utilizaran en la medida en que el atacante considere que la información vale la pena.

En este manual cubriremos varios métodos de protección, desde los mas elementales como es la elección de una password adecuada, hasta los mas complejos como son la utilización de algoritmos de encriptación de clave pública.

Sin embargo, ningún método es seguro si uno no fija (y respeta a rajatabla) una política de uso, si no se es estricto en donde se guarda la información clave, de quien tiene acceso a los medios para desencriptación, y que tanto relajamos nuestros cuidados. La Seguridad en Internet depende en gran medida de un método de protección adecuado, es verdad, pero también de un uso responsable y regular de una política de Seguridad.

La protección de todos los días

Todos los días trabajamos generando información valiosa sobre computadoras. Estas están stand-alone (solas) o conectadas a alguna red local, o conectadas a través de Internet con varios millones de personas activas que podrían penetrar nuestros secretos. :)

Algunas de los procedimientos y consejos que comentamos en este manual son aplicables a las tareas de todos los días, y a toda nuestra información, como es la protección anti-virus.

Otros, como el uso de algoritmos de encriptación, valdrá la pena solo cuando nuestros documentos sean importantes

Y otros aún son los mecanismos de autenticación, también llamados firmas electrónicas (Electronic signature): la forma de garantizar que algo escrito por nosotros (y no necesariamente codificado) fue *Realmente* originado por nosotros.

Las preguntas que debe hacerse para elegir una forma de protección adecuada

¿Estoy protegiendo datos **valiosos** o solo quiero autenticar mis documentos? (ya veremos mas adelante en que consiste la "firma" electrónica)

¿Que datos quiero proteger?

¿De que volumen de información se trata?

¿Por cuanto tiempo hay que protegerla?

¿Que tan segura esta la información en su origen (encriptación) y destino (desencriptación)?

¿Cuanta gente tendrá los medios para decodificarla?

¿De quien estoy tratando de proteger la información?

Recuerde siempre

No hay metodos de proteccion infalibles. Si la informacion vale la pena siempre habra alguien dispuesto a encontrar una forma de decodificarla.

Formas usuales de penetración y su solución

Forma	Solución
Una password fácil	Elija una password mas compleja (vea la sección sobre Passwords) No la anote No la comparta con nadie
Una terminal a la que estoy logueado y me voy	Use password en los screen savers Desconéctese de la red cuando se aleje de su terminal, aun al ir a almorzar.
Virus/ Caballos de Troya	Use un buen antivirus. Manténgase actualizado con la ultima versión Defina una política de protección y úsela Proteja los diskettes Haga backup No comparta discos con extraños No ingrese ningún diskette a su computadora sin verificarlo
Acceso Físico	Guarde la información relevante en cintas, diskettes o CD Roms. Nunca en un disco rígido. Mantenga estos medios de almacenamiento en una caja fuerte. Cuando este usándolos no permita que se alejen de su vista Cuando los consulte no lo haga en una computadora de red.

	Nunca se los olvide!!!
Ingreso vía Internet	No conecte computadoras con información confidencial a la Internet (Airwalls) Use un firewall
Remanencia de datos (archivos temporarios, archivos borrados, memoria virtual, programas compresores de disco, etc)	Borre todos los temporarios Sobreescriba los sectores sin uso de su disco Resetee su maquina Destruya físicamente los diskettes Use programas específicos de protección durante la edición
Análisis de trafico	No maneje información confidencial siempre a la misma hora Use siempre la misma maquina para encriptar y desencriptar Apagela luego de usarla

Como elegir una password (clave de acceso)

Que no usar **nunca** como password

- Cualquier palabra o numero fácilmente relacionado con uno mismo (es lo primero que los hackers buscan): nombre, apodo de la primaria, numero de documento, patente del auto, fecha de nacimiento, nombre de su hijo, calle donde vive, etc.
- Cualquier letra repetida varias veces ej. zzzzzzzzzzzzz o 777777
- Cualquier escalera normal ej. . 1234, abcdef , doremifasol
- Cualquier palabra de menos de seis letras
- Palabras usuales como: Clave, MiClave, TopSecret, Secreto, etc.

Además:

- Nunca usar la misma password en varios lugares.(si averiguan una, nada impedirá que accedan al resto de las cosas protegidas con la misma clave)
- No escribirla en ninguna parte en la medida de los posible (nunca en su agenda o billetera)
- No compartirla con nadie.
- No almacenarla en un archivo en su disco rígido.

Que **si** usar como password

- Dos palabras al azar separadas de un signo raro ej. xilofon$rayos-x (elíjalas de un diccionario abriendo paginas al azar)
- Una palabra inventada: aluminatividad
- Una cadena de caracteres al azar: YU6790HGJ

Además:

- Guarde la información relevante en cintas, diskettes o CD Roms. Nunca en un disco rígido.
- Mantenga estos medios de almacenamiento en una caja fuerte.

- Cuando esté usándolos no permita que se alejen de su vista
- Cuando los consulte no lo haga en una computadora de red.
- Nunca se los olvide!!!

Como elegir una pass phrase (frase clave)

Para cierto tipo de algoritmos de encriptación es necesario elegir no una palabra clave sino una frase clave. No utilice una frase común ("de tal palo tal astilla") sino invéntese una propia que le resulte fácil de recordar o utilice el método sugerido:

1. Diríjase a una biblioteca pública
2. camine por un pasillo al azar
3. elija un libro al azar
4. abra una pagina al azar
5. pose su dedo en una linea: Ya tiene su frase Clave!

Y le garantizamos que es casi imposible que alguien la descifre! ;-)

Encriptación

Introducción y conceptos

Supongamos que yo quiera enviarle un mensaje pero no quiera que nadie excepto usted pueda leerlo. Yo podría encriptar o cifrar ese mensaje, es decir, mezclarlo de una forma complicada de modo que solo alguien que sabe cómo yo lo mezcle pueda deshacer los pasos y volver al mensaje original.

Un Criptosistema es un conjunto de reglas que determina como se codifican y decodifican los datos. Existen varios tipos de criptosistemas, que pueden no utilizar claves, utilizar una clave o mas de una. Una clave es un patrón de bits usados para codificar o decodificar un mensaje. La clave suele derivarse de una contraseña (password) o de una frase (pass phrase).

Yo usaría una "key"(clave) criptografica para encriptar el mensaje, y usted usaría la misma clave para descifrarlo o desencriptarlo. Esto es lo que llamamos un sistema criptograficos de llave única (single key), como el DES.

Un sistema tradicional de encriptación como este implica que la clave única debe haber sido intercambiada PRIMERO entre las dos personas que deseen enviarse documentos encriptados. Esto implica enviar antes la clave por un medio seguro: un courier, un sobre. Este es el principal problema: como lograr intercambiar esas llaves con seguridad. No solo eso, sino que personas extrañas no podrían intercambiarse archivos sin antes poder enviarse la llave (imagínese la importancia que esto tiene para el comercio electrónico).

Los Sistemas de clave pública y clave privada

Imagínese que Ud. tiene una caja de seguridad. Encarga a su cerrajero dos tipos de llave para la cerradura: una única llave (la clave privada) que puede abrir la caja, y varias llaves (claves publicas) que pueden cerrarla, pro NO abrirla. Cualquier persona con la llave que cierra (clave publica) puede dejar un mensaje dentro de la caja que solo Ud. podrá abrir. ¿Cual seria el riesgo de entregar a todos una copia de nuestra llave que cierra?

En un sistema de clave pública (también llamados algoritmos D-H) usted tiene dos claves. Una clave, la llamada pública, puede ser distribuida libremente, y cualquier persona que quiera enviarle un mensaje codificado podrá usar su clave pública para la codificación.

La otra clave, la privada, se conserva secreta y se usa sólo para la desencriptación. **De la clave pública no puede deducirse la privada.**

La clave pública puede ser distribuida libremente a través de la red (usualmente se la agrega al final de un mensaje).

Cualquier persona, aun desconocidos, pueden usar su clave pública para enviarle un mensaje cifrado, el cual solo podrá ser descifrado por usted (ni siquiera quien la encriptó originalmente puede revertir el proceso).

Los sistemas de clave publica fueron inventados en 1976 por Whitfield Diffie y Martin Hellman.

Autenticación o firma electrónica

Otra razón para el uso de las claves públicas es la autenticación: poder garantizar que un mensaje proviene efectivamente de una persona en particular, y que no fue alterado en el medio (imagínese el caso de una orden de compra o de un pago electrónico).

La clave privada de quien lo envió puede ser usada para encriptar o firmar un mensaje, de este modo garantizando al autoria del mensaje. Luego, cualquiera puede verificar usando la clave pública de quien lo envió para verificar. De este modo se evita la falsificación de mensajes, o su alteración.

Para generar una "firma" el PGP usa una función llamada Hashing (similar al CRC) que logra una serie de bits resultantes de modo tal que si el mensaje fuera alterado el resultado de aplicar este proceso seria muy distinto. Luego se usa la clave privada para formar la firma.

Técnicas Combinadas: Encriptación y Autenticación

Los dos procesos pueden ser combinados si primero se firma un mensaje con la clave privada, y luego se la encripta con la clave pública de quien la envió. Quien la recibe invierte los pasos: primero desencripta con su propia clave privada y luego verifica la autenticidad con la clave pública del autor.

Como el proceso de encriptación por clave pública es mucho mas lento que por clave única, se utiliza una clave simple generada en el momento para cifrar el mensaje. Esta clave es luego codificada con la clave pública del receptor. Quien recibe le mensaje usa luego su propia clave privada para obtener la clave simple, y desencriptar el mensaje original.

Las claves públicas se guardan en un llavero, incluyendo la identificación de su dueño

Técnicas de Encriptación

rot13

Un algoritmo de sustitución cifrada, no es realmente una forma de proteger información. Usado en los mensajes de chistes verdes de Usenet. Consiste en reemplazar cada letra con la que esta 13 lugares antes en el alfabeto, ej. la “N” por “A”, etc..

Crypt

Una utilidad Unix basada en una versión simplificada de un código de la segunda guerra. Existe software para romper este código, pero solo se usa si la información vale la pena (es bastante trabajoso).

Encriptación incluida en aplicaciones

La mayoría del software de uso masivo (Lotus 123, MS Word, MS Excel, etc) brinda la opción de encriptar los archivos de datos. En general los algoritmos usados son bastante básicos y fáciles de romper. Existen algunos softwares en el mercado que sostienen que pueden romper archivos protegidos por la mayoría de los programas mas usados.

DES

(Data Encription Standards)

Des es un algoritmo originario de los años 70. Fue adaptado por el gobierno norteamericano para proteger información sensible pero no clasificada.

DES fue el primer código de encriptación que se hizo público, así que muchos otros están basados en él . Hace dos décadas que esta disponible, sin embargo hasta ahora nadie ha podido romperlo, aunque se dice que la NSA tiene una forma secreta de descifrarlo a voluntad.

Hay chips DES capaces de encriptar y desencriptar lo suficientemente rápido como para colocarlos en el trafico de una red local.

TRIPLE DES

(Triple Data Encription Standard)

Es un algoritmo que aplica tres veces sucesivas el algoritmo DES. Más seguro que el anterior.

IDEA

(International Data Encryption Algorythm)

Fue desarrollado al final de los años 80 por dos criptografos de excelente reputación: James L. Massey y Xuejia Lai. Esta patentado en muchos países del mundo, y constituye parte de la lógica utilizada en el PGP (descripto mas adelante)

RSA

(Rivest-Shamir-Adleman)

Es un sistema de encriptación de clave pública vendido por RSA Data Security Inc. (vea los sistemas de clave pública, en la sección anterior) Con RSA la clave se genera por la multiplicación de dos números primos muy grandes. La clave secreta es uno de ellos, y la otra clave, la pública, puede obtenerse siempre por divisiones sucesivas. Una clave de 512 bits es el producto de dos numero primos de 265 bits de longitud

RIPEM

(Riodan's Internet Privacy Enhanced Mail)

Es una implementación del standard PEM que usa DES o TRIPLE DES para encriptar y RSA para distribuir la clave.

PGP (Pretty Good Privacy)

Es un software de criptografia de alta seguridad adaptado para los entornos MSDOS, Unix, VAX/VMS, Macintosh, Amiga y Otros. Creado por Phil Zimmerman, uno de lo héroes de Internet, ya que corre riesgo de ir a la cárcel por haber hecho publico un algoritmo de encriptacion secreto.

Es un algoritmo de clave pública, descripto en la sección anterior. Utiliza IDEA para encriptacion y RSA para distribución de la clave

Permite que las personas intercambien mensajes con Privacia, autenticación y conveniencia.

Privacia porque solo aquellos para los cuales estaba destinado un mensaje pueden recibirlo.

Autenticación porque un mensaje publico que sea publicado por una determinada persona puede verificarse que solo haya podido ser escrito por ella (esto es lo que se llama firma electrónica)

Conveniencia porque la Privacia y la autenticación se pueden obtener sin los problemas de manejar claves que en general se tiene con el software común de criptografia. No se requiere un canal seguro para intercambiar claves entre usuarios.

RC2, RC4 y codigos de 40 bits (como los que usa el Netscape)

En general son débiles métodos de protección.

Key Escrow

Un método de encrptacion similar al de clave publica que genera tres claves: una para quien envía, otra para quien recibe y otra para una tercera parte (TTS: Trusted Third Party) que puede ser las Naciones Unidas o un Gobierno.

Lógicamente un sistema donde hay una tercera clave en poder de otra entidad disminuye enormemente la seguridad del método.

Clipper Chip o Capstone

Uno de los productos de criptografia por hardware creados por la NSA, aplicando el concepto de key-escrow. Se basa en un chip que debe comprarse e instalarse en las computadoras que deban encriptar o desencriptar información. La idea es que el gobierno se queda con la tercera clave, y podrá usarla si desea desencriptar un mensaje que intercepto.

El gobierno norteamericano desea lograr que sea ampliamente utilizado, ya que se supone que es crackeable por cualquiera del gobierno. Su algoritmo es secreto, y por lo tanto se desconoce su seguridad.

Se supone el mejor algoritmo de criptografia, pero solo puede ser usado dentro de USA con una licencia del gobierno.

Si el Cliper Chip y sus codigos son aceptados como estándares, el gobierno norteamericano probablemente prohiba todo otro método de encrptacion.

One time pads

El único método garantizadamente seguro, usado ampliamente por los espías. Se basa en generar dos claves al azar con gran cantidad de bits. Luego, se envía un mensaje generado por el mensaje original operado con la clave de bits mediante una operación XOR (or excluyente). Solo poseyendo una clave igual de bits e puede decodificar le mensaje original. Es el método usado, por ejemplo, en la linea de comunicacion entre Washington y Moscú.

Usando el PGP

Como instalar el PGP

Copie el archivo a un directorio deseado (ej. PGP) y luego descompactelo con el PKUNZIP utilizando el parámetro -d.

Elija un lugar para su “llavero”(keyring). Usualmente será un diskette.

[variables[

Cree su propio juego de claves pública y privada

Tipee PGP -kg

El PGP le solicitara su nombre de usuario., Usualmente completaremos este campo con nuestro nombre seguido de nuestra dirección de e-mail (se estila poner la dirección de e-mail entre <>)

ej. Roxana Bassi <rox@arda.sicoar.com>

Luego el sistema nos pedirá nuestra frase clave (pass phrase) la cual deberemos memorizar. (vea: estrategias para elegir una pass phrase)

Tabla rápida de comandos PGP

Para encriptar un archivo con la clave pública de su receptor

pgp -e textfile her_userid

To sign a plaintext file with your secret key:

pgp -s textfile [-u your_userid]

To sign a plaintext ASCII text file with your secret key, producing a signed plaintext message suitable for sending via E-mail:

pgp -sta textfile [-u your_userid]

To sign a plaintext file with your secret key, and then encrypt it with the recipient's public key:

pgp -es textfile her_userid [-u your_userid]

To encrypt a plaintext file with just conventional cryptography, type:

pgp -c textfile

To decrypt an encrypted file, or to check the signature integrity of a signed file:

pgp ciphertextfile [-o plaintextfile]

To encrypt a message for any number of multiple recipients:

pgp -e textfile userid1 userid2 userid3

--- Key management commands:

To generate your own unique public/secret key pair:

pgp -kg

To add a public or secret key file's contents to your public or
secret key ring:

pgp -ka keyfile [keyring]

To extract (copy) a key from your public or secret key ring:

pgp -kx userid keyfile [keyring]
or: pgp -kxa userid keyfile [keyring]

To view the contents of your public key ring:

pgp -kv[v] [userid] [keyring]

To view the "fingerprint" of a public key, to help verify it over
the telephone with its owner:

pgp -kvc [userid] [keyring]

To view the contents and check the certifying signatures of your
public key ring:

pgp -kc [userid] [keyring]

To edit the userid or pass phrase for your secret key:

pgp -ke userid [keyring]

To edit the trust parameters for a public key:

pgp -ke userid [keyring]

To remove a key or just a userid from your public key ring:

pgp -kr userid [keyring]

To sign and certify someone else's public key on your public key ring:

pgp -ks her_userid [-u your_userid] [keyring]

To remove selected signatures from a userid on a keyring:

pgp -krs userid [keyring]

To permanently revoke your own key, issuing a key compromise certificate:

pgp -kd your_userid

To disable or reenable a public key on your own public key ring:

pgp -kd userid

--- Esoteric commands:

To decrypt a message and leave the signature on it intact:

    pgp -d ciphertextfile

To create a signature certificate that is detached from the document:

    pgp -sb textfile [-u your_userid]

To detach a signature certificate from a signed message:

    pgp -b ciphertextfile

--- Command options that can be used in combination with other
command options (sometimes even spelling interesting words!):

To produce a ciphertext file in ASCII radix-64 format, just add the
-a option when encrypting or signing a message or extracting a key:

    pgp -sea textfile her_userid

or: pgp -kxa userid keyfile [keyring]

To wipe out the plaintext file after producing the ciphertext file,
just add the -w (wipe) option when encrypting or signing a message:

    pgp -sew message.txt her_userid

To specify that a plaintext file contains ASCII text, not binary, and

should be converted to recipient's local text line conventions, add the -t (text) option to other options:

```
pgp -seat message.txt her_userid
```

To view the decrypted plaintext output on your screen (like the Unix-style "more" command), without writing it to a file, use the -m (more) option while decrypting:

```
pgp -m ciphertextfile
```

To specify that the recipient's decrypted plaintext will be shown ONLY on her screen and cannot be saved to disk, add the -m option:

```
pgp -steam message.txt her_userid
```

To recover the original plaintext filename while decrypting, add the -p option:

```
pgp -p ciphertextfile
```

To use a Unix-style filter mode, reading from standard input and writing to standard output, add the -f option:

```
pgp -feast her_userid <inputfile >outputfile
```

Riesgos del comercio electrónico

Medidas de seguridad

Apéndices

Contenidos del Diskette

PGP versión 2.61 versión del MIT

PGP versión 2.61 documentación

Documentación en español

PGP FAQ

Referencias:

Newsgroups:

alt.privacy	
alt.privacy.clipper	Clipper, Capstone, Skipjack, Key Escrow
alt.security	Seguridad en general
alt.security.index	Índice de alt.security
alt.security.pgp	donde se debate el uso del Pgp.
alt.security.ripem	discusión de RIPEM
alt.society.civil-liberty	Libertades civiles, incluyendo privacidad
comp.compression	Debate sobre algoritmos de compresión
comp.risks	Criptografia
comp.society.privacy	Privacia en general
comp.security.announce	Anuncio de fallas de seguridad

misc.legal.computing Patentes, derechos y leyes de computación.

sci.crypt Un newsgoup sobre la ciencia de la criptografia.

talk.politics.crypto Un news sobre legislación y criptografia

Mailing Lists

Cypherpunks mailing list

Dedicada a la discusión de las defensas tecnológicas para la privacidad en el ambiente digital.

Envíe un e-mail a cypherpunks-request@toad.com para agregarse a la lista. El volumen es de 30 a 40 mensajes diarios.

Software de encriptacion

SecureEdit: (macinstosh) ripem.msu.edu /pub/crypt

primary FTP distribution site (net-dist.mit.edu).

Mike Johnson (mpj@csn.org) for a list of Internet FTP sites and BBS phone numbers.

rsa.com

ripem.msu.edu: para obtener el Ripem.

Glosario

Autenticación: el proceso de verificación de un mensaje que nos garantiza que esta completo y no ha sido alterado.

Criptososistema: Conjunto de reglas que determina como se codifican y decodifican los datos.

Clave: es un patrón de bits usados para codificar o decodificar un mensaje. La clave suele derivarse de una contraseña (password) o de una frase (pass phrase).

Cracker: Especialista en romper codificaciones o descubrir passwords. Usualmente peligrosos.

D-H Algorithm: otro nombre para los sistemas de encriptacion de clave publica.

DSS (Digital Signature Standard): Estándar para la firma electrónica, basado en el Secure Hash Standard.

Hacker: Pirata informatico. Persona que se divierte al resolver claves o resolver passwords.

Hashing: Un algoritmo que convierte generar una serie de bits a partir de un archivo, de modo que esta serie de bits esta relacionada con el documento. Son avanzadas funciones de criptografia, destinadas a evitar la posibilidad de alterar fácilmente un documento.

Secure Hash Standard (SHS): Función de hashing que genera una verificación de 160 bits que actúa de firma electrónica de acuerdo al DSS.

Sistema de clave simétrica o única: un sistema donde se usa la misma clave para encriptar y desencriptar.

NSA (National Security Agency): el sector del gobierno norteamericano responsable de mantener secretos a los comunicados clasificados del gobierno.

PEM (Privacy Enhanced Mail): el standard de Internet para enviar mensajes encriptados y/o autenticados.