Seguridad Informatica para todos

PGP
GNUPG
Encriptar mensajes
Desencriptar mensajes
Firmar mensajes
Verificar mensajes firmados
Algunos Comandos
Anillo de confianza

Seguridad Informatica para todos

Lic. Carlos Alberto Rico

Ing. Felipe Evans

G.I.D.I.

Grupo de Ingeniería en Desarrollos Informaticos

Facultad de Ingeniería

U.N.M.d.P.

2009

Seguridad Informatica para todos

Criptología

Pretty Good Privacy

Privacidad bastante buena:

Zimmermann 1991.

Standard de Internet.

pgp -h

Seguridad Informatica para todos

GNU-PG

GnuPG es una aplicación que sirve para Encriptar y/o Firmar mensajes, documentos

GnuPG usa un sistema de claves públicas.

Cada Usuario tiene una clave privada y una clave pública.

El programa se puede obtener de la siguiente url http://www.gnupg.org

Seguridad Informatica para todos

GNU-PG

¿Para que ?

Encriptar mensajes

Desencriptar mensajes

Firmar mensajes

Verificar mensajes firmados

Anillo de confianza

Seguridad Informatica para todos

GNU-PG

Encriptar mensajes

Encripta quien envia.

Utiliza Clave Pública del destinatario.

gpg --armor --recipient ClaveID –encrypt mensaje

Seguridad Informatica para todos

GNU-PG

Desencriptar mensajes

Desencriptar quien recibe.

Utiliza su propia Clave Privada.

gpg --decrypt archivo

Seguridad Informatica para todos

GNU-PG

Firmar mensajes

Firma quien Envía

Utiliza su propia Clave Privada.

gpg --clearsign a.txt y genera: a.txt.asc

O

gpg --sign a.txt y genera: a.txt.gpg (encriptado)

Si Aplica --sign para desencriptar Usar --decryp

Seguridad Informatica para todos

GNU-PG

Verificar mensajes firmados

Verifica quien recibe

Utiliza la Clave Pública del que envió.

gpg --verify a.txt.asc

Seguridad Informatica para todos

GNU-PG

Anillo de confianza

Base del Escribano Virtual.

1) Escribano y usuario1 Intercambian sus Claves Publicas y las verifican con sus huellas.

2) Escribano Firma con su Clave Privada la Publica de Usuario1.

3) Usuario2 Recibe la Clave Publica de Usuario1 Firmada por Escribano.

Se basa en la confianza del Usuario2 sobre el Escribano.

Seguridad Informatica para todos

GNU-PG

Algunos Comandos

Crear Claves: gpg --gen-key.

Ver Publicas: gpg --list-keys

Ver Privadas: gpg --list-secret-keys

Borrar Priv.: gpg --delete-secret-key ClaveID. Archivo: secring.gpg

Borrar Públ.: gpg --delete-key ClaveID. Archivo: pubring.gpg

Ver Huella: pgp --fingerprint ClaveID (Como el MD5)

Exportar Publica: gpg --armor --output Archivo.asc --export ClaveID

Exportar Privada: gpg --armor --output Archivo.asc --export-secret-key ClaveID

Seguridad Informatica para todos

GNU-PG

Algunos comandos

Importar Ambas: gpg --import ClaveID

Encriptar un mensaje : gpg --armor --recipient ClaveID --encrypt mensaje

Desencriptar mensaje : gpg --decrypt archivo.asc

Firmar mensaje: gpg --clearsign archivo --> archivo.asc

gpg --sing archivo --> archivo.gpg

gpg --decrypt archivo.gpg (para desencriptar la fierma)

Verificar Firmas: gpg --verify mensaje

Seguridad Informatica para todos

GNU-PG

Algunos comandos

Buscar En servidores: gpg --keyserver NombreServer --search-keys ClaveID.

Inportar desde Serv : gpg --keyserver NombreServer --recv-keys ClaveID.

exportar a un serv. : gpg --keyserver NombreServer --send-keys ClaveID

Acceder a la Shell: gpg --edit-key ClaveID

Revocar una Clave: gpg --output archivo.asc --gen-revoke.

Seguridad Informatica para todos

Firma Digital en la Argentina.

Autoridad Certificante de la Oficina Nacional de Tecnologías Información.

Autoridad Certificante
Oficina Nacional de Tecnologías de la Información (ONTI)
Subsecretaría de la Gestión Pública
Jefatura de Gabinete de Ministros
Abril, 2002

Sitio : http://ca.pki.gov.ar/

Seguridad Informatica para todos

Gracias por su Atención.