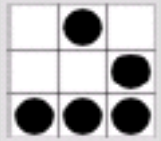
GnuPG para dummies

Marzo-2018
ParanaConf

Otro capítulo de:
"Como luchar contra su Malvado Administrador"...

Jorge “**Vampii**” Franco



Podrías pensar lo peor...

”Sí, soy un criminal. Mi crimen es la curiosidad, juzgar a la gente por lo que dice y piense, no por su aspecto. Mi crimen es superarte, algo por lo que nunca me vas a perdonar.”

Extraído del Manifiesto Hacker,
The Mentor, 1986

Cuando el fuego crezca quiero estar alli...

El Hombre semi-libre es uno que cree que es libre. El Hombre realmente libre es uno que sabe completamente lo que puede hacer en su prisión y lo hace. El verdadero truco de la vida no es el estar informado, sino vivir el misterio...

Mejor abrir los ojos para saber lo que te gustaria hacer

Don't panic!

"Es un hecho importante y conocido que las cosas no siempre son lo que parecen."

Douglas Adams – La Guía del Autoestopista Galáctico.

Criptología
Definición

Proviene de las palabras “***criptos***” (oculto, secreto) y “***logos***” (ciencia).

La ***criptología*** es la ciencia de aplicar matemáticas complejas para cifrar mensajes.

Abarca dos grandes áreas:

Criptoanálisis

Criptografía

Criptoanálisis
Definición

Es el conjunto de técnicas que intenta descifrar la clave utilizada entre dos comunicaciones.

Tiene como objetivo encontrar sistemas (algoritmos) para descifrar la información que se transmite a travéz de un medio.

Criptografía
Definición

Proviene de las palabras “***criptos***” (oculto, secreto) y “***grafos***” (escritura).

La ***criptografía*** es la ciencia de aplicar matemáticas complejas para aumentar la seguridad de las transacciones.

Se encarga de la seguridad en el envío de los datos (cifrado de información)

Criptografía

A Jeroglificos I

(Métodos criptográficos)

Primer método de encriptado = Julio Cesar

Siglo XIV libro más antiguo conocido

León Battista (S. XV) Tratado de cifras y Poligrafía

esto No tiene Sentido peterete

Finalidad

Garantizar el secreto en la comunicación

Autenticidad y no-repudio, el remitente “es quien dice ser”

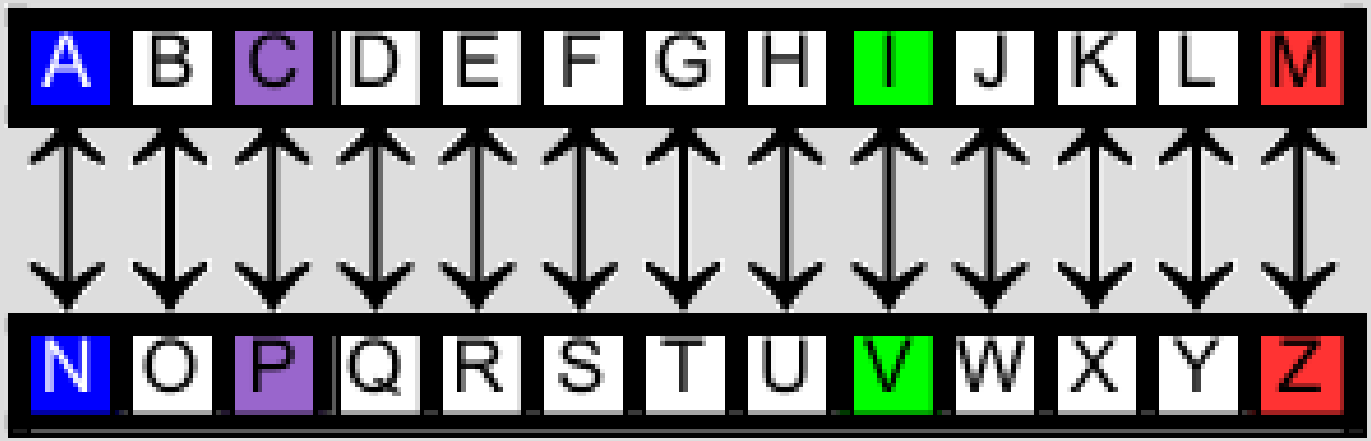
Impedir la modificación del mensaje en tránsito

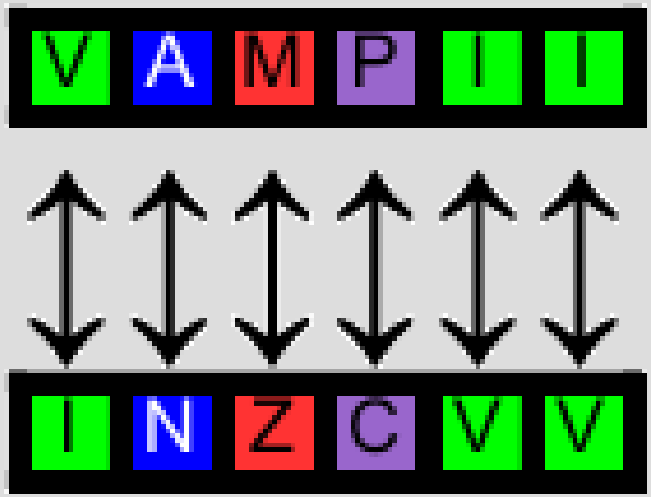
Privacidad...

En lo más profundo y fundamental de la mente y del Universo, hay una razón para ello.

Douglas Adams – La Vida, el Universo y Todo lo Demás.

Cifrado ROT13





Criptografía Asimétrica

Método criptográfico que usa un par de claves para el envío de mensajes. Una pública y otra privada.
El remitente usa la clave pública del destino para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destino 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 Asimétrica
Algoritmos

Diffie-Hellman

RSA RSA

DSA (Digital Signature Algorithm)

ElGamal ElGamal

Criptografía de curva elíptica (ECC)

Criptografía Asimétrica

Lo que está cifrado con una clave (pública o privada) sólo se puede descifrar con la otra clave (privada o pública).

El cifrado asimétrico es seguro.

No sufre por la interceptación de claves.

No tiene los problemas complejos de distribución de claves.

No exige una relación previa entre las partes para hacer el intercambio de claves.

Soporta firmas digitales y aceptación.

Es relativamente lento.

Expande el texto cifrado.

Criptografía Asimétrica

Debe ser segura.
El cifrado debe ser rapido.
El texto cifrado debe ser compacto.
La solución debe servir en escalas de grandes poblaciones.
La solución no debe ser vulnerable a la interceptación de claves.
La solución no debe requerir una relación previa entre las partes.
La solución debe soportar firmas digitales y aceptación.

Criptografía Cuántica

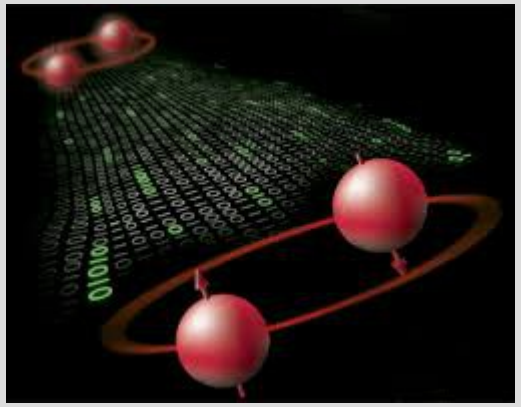
Principio de incertidumbre de Heisenberg.

Canal cuántico como medio de transmisión (Fibra óptica).

Canal tradicional público como medio de intercambio.

Teorema de no-clonación.

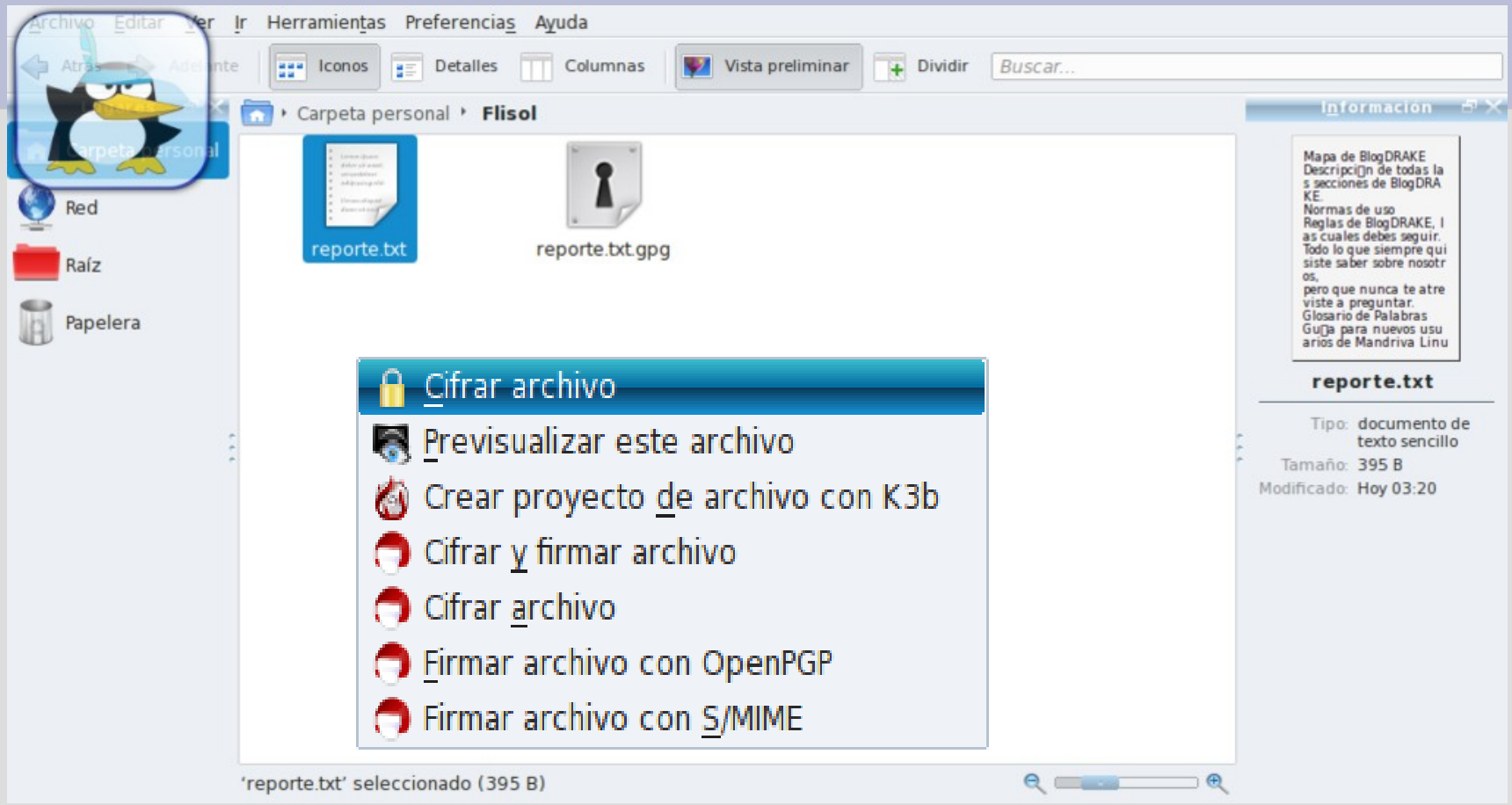
Amenazas sobre BITCOIN y otros.



Reflexíon:

La computadora no es una máquina inteligente para gente estúpida, si no una máquina estúpida que sólo funciona en manos de gente inteligente.

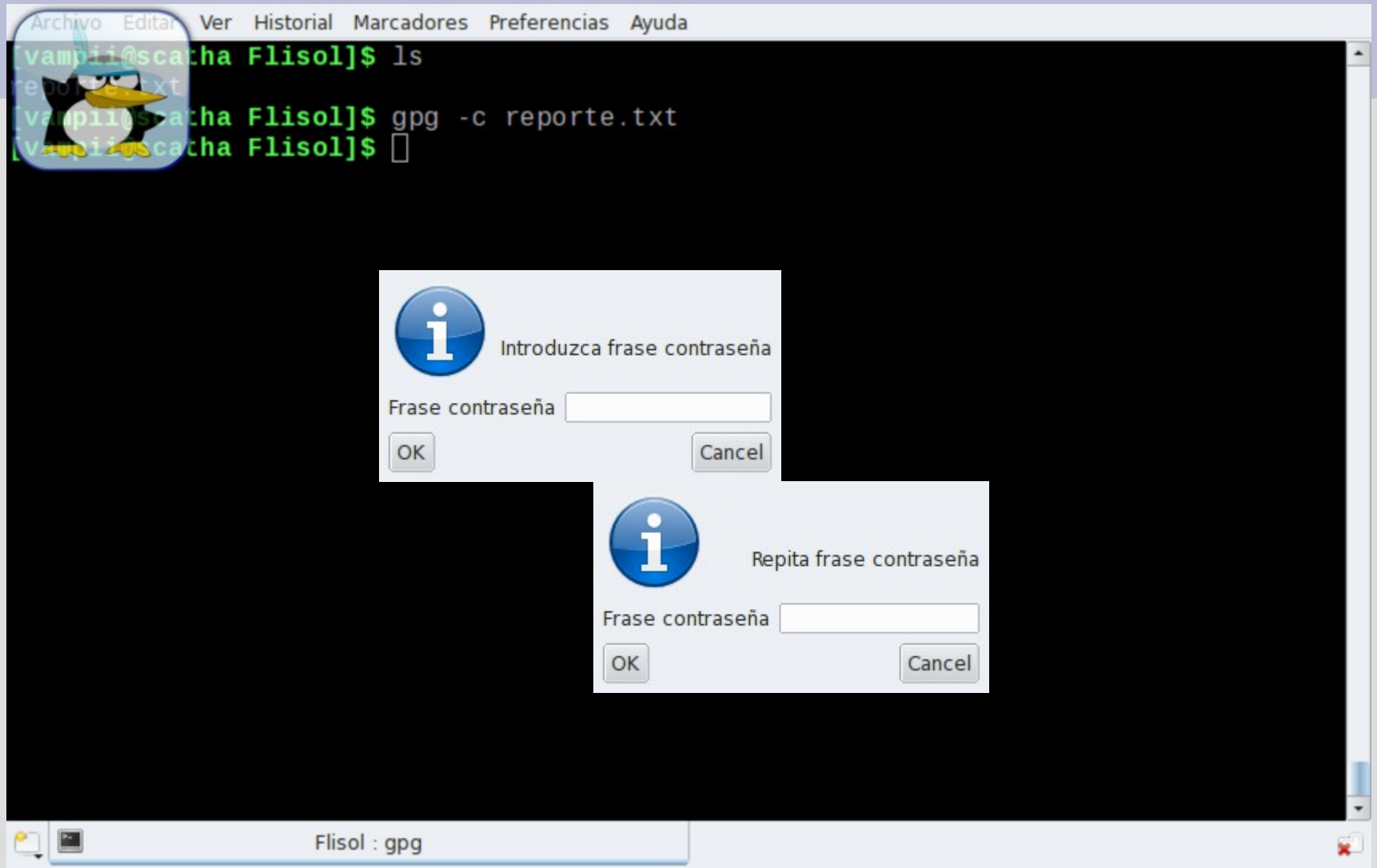
Modo simple...


Archivo Editar Ver Ir Herramientas Preferencias Ayuda
Atrás Adelante
Iconos
Detalles
Columnas
Vista preliminar
Dividir
Buscar...
Carpeta personal
Flisol
Información
Red
Raíz
Papelera
reporte.txt
reporte.txt.gpg
Mapa de BlogDRAKE
Descripción de todas las secciones de BlogDRAKE.
Normas de uso
Reglas de BlogDRAKE, las cuales debes seguir.
Todo lo que siempre quisiste saber sobre nosotros,
pero que nunca te atreviste a preguntar.
Glosario de Palabras
Guía para nuevos usuarios de Mandriva Linux
reporte.txt
Tipo: documento de texto sencillo
Tamaño: 395 B
Modificado: Hoy 03:20
Cifrar archivo
Previsualizar este archivo
Crear proyecto de archivo con K3b
Cifrar y firmar archivo
Cifrar archivo
Firmar archivo con OpenPGP
Firmar archivo con S/MIME
'reporte.txt' seleccionado (395 B)

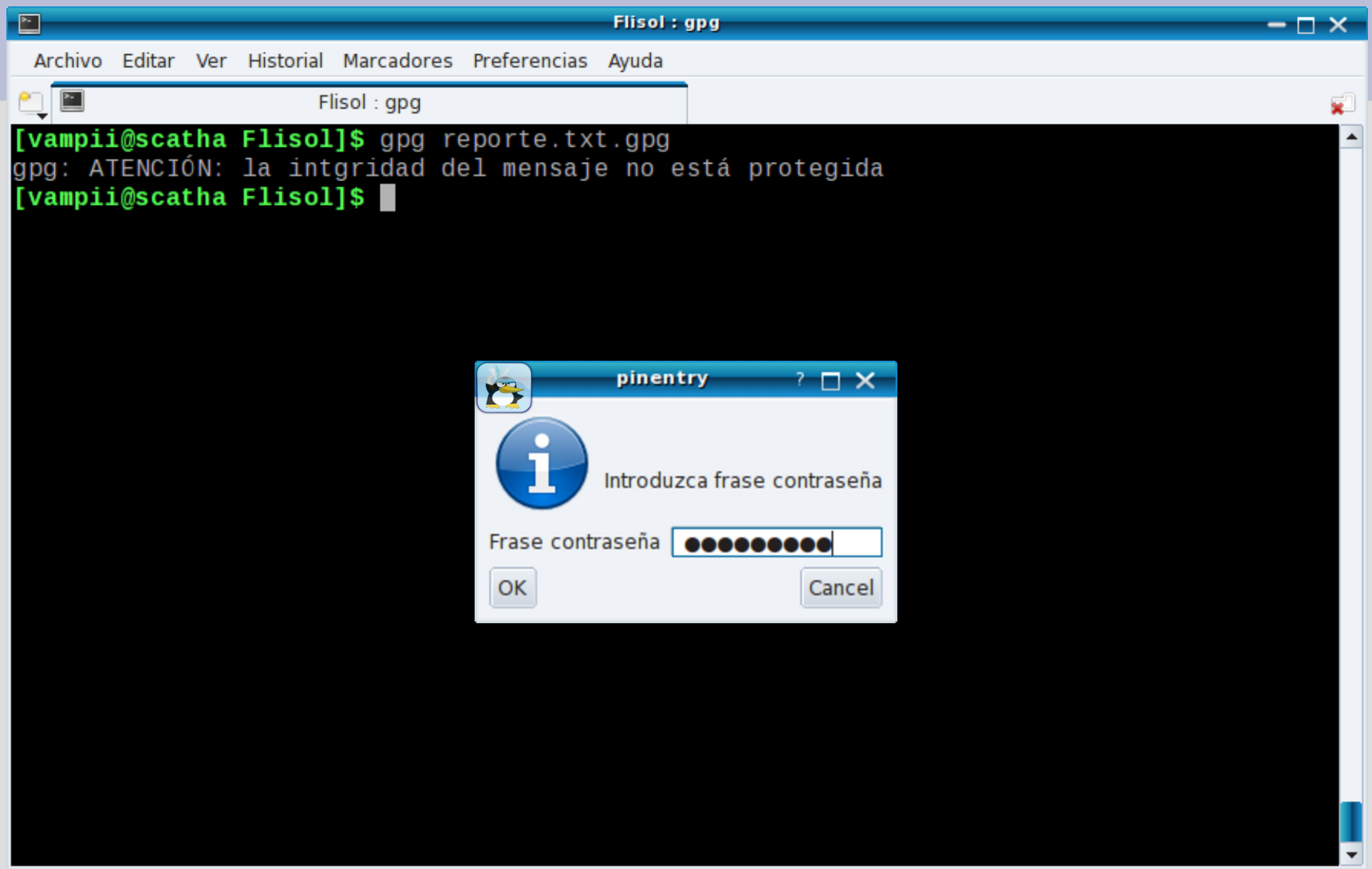
Me tocó crecer viendo a mi alrededor Paranoia y Dolor...

¿Qué consuelo encontraríamos en saber que los sufrimientos de millones de hombres han permitido la revelación de una situación límite de la condición humana, si más allá de dicha situación límite sólo estuviera la nada?

Modo Universal...



Modo Universal...



¿Cuánto tiempo guardás un secreto?

“Parasiempre” es mucho tiempo…

Del Manual de GnuPG...

-c Cifra con una cifra simetrica usando una frase de paso. La cifra simetrica usada por omision es CAST5, pero se puede elegir con la opcion **--cipher-algo**. Esta opcion se puede combinar con **--sign** (para firmar y cifrar simetricamente el mensaje), **--encript** (para que el mensaje pueda ser descifrado via una clave secreta o frase de paso), o ambos **--sign** y **--encript** (para firmar y que pueda ser descifrado via una clave secreta o frase de paso).

Ver --for-your-eyes-only

No hay un dónde, allí. A los niños se les enseñaba eso para explicar el ciberespacio.

William Gibson - Mona Lisa Acelerada – 1992

De cómo partiendo de la nada, se llegó a las cimas más altas de la Miseria

```
sh Configure
make
make test
make install
```

Un mundo mágico de Magos, Unicornios y Gente Amable...

Quien sabe lo que es correcto también hará lo correcto.

No me mires así, Dios me ha hecho para caer...

(O ¡Ups, todo hace CRACKKKK!!!...)

Si hay algo que nos salva en este mundo...

Es la incapacidad de la mente humana para correlacionar todos sus contenidos. Vivimos en una isla de ignorancia en medio de los mares negros del infinito, y no estamos hechos para viajar lejos...

H. P. Lovecraft

Paranoia: Arte de trabajar en Sistemas, no es una ciencia exacta.

Referencias

Internet y La Vida, reuniones 2600 y otras no menos luminosas y esclarecedoras en antros de poca monta y cabarets muy famosos...

Documentación de GNU/Linux en español y “no tan en español”

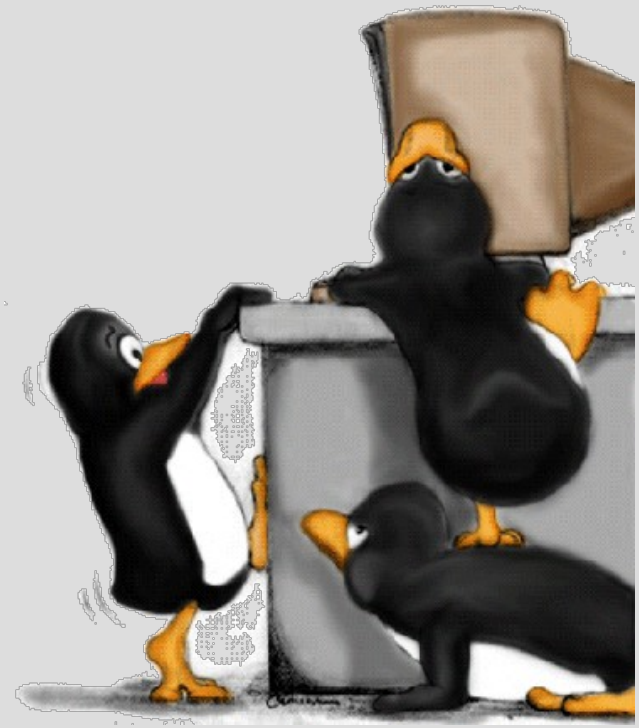
GnuPG:	http://www.gnupg.org/
PGP Corportation:	http://www.pgp.com/
PGP International:	http://www.pgpi.org/
OpenPGP Alliance:	http://www.openpgp.org/

Acerca de este documento:
Este documento fue escrito utilizando joe y mcedit. Los gráficos fueron realizados utilizando LibreOffice y Gimp.

Referencias

OpenSSL: http://www.openssl.org/
OpenSSH: http://www.openssh.org/
NESSIE: http://www.cryptonessie.org/

http://fdonea.tripod.com/primes.htm
http://www.hermetic.ch/pns/pns.htm
http://www.mersenne.org/



Referencias

American National Standards Institute: http://www.ansi.org/
Communications Security Establishment: http://www.cse-cst.gc.ca/
Cryptography Research and Evaluation Committee:
http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html
CryptTool: http://www.cryptool.org/
Federal Information Processing Standard: http://www.itl.nist.gov/fipspubs
Government Communications Headquarters: http://www.gchq.gov.uk/
Institute of Electrical and Electronics Engineers: http://www.ieee.org/
International Organization for Standardization: http://www.iso.org/
Internet Engineering Task Force: http://www.ietf.org/ietf_chairs_year.html
National Institute of Standards and Technology: http://www.nist.gov/
National Security Agency: http://www.nsa.gov/

http://daniellerch.com/papers/html/algoritmo_rsa.html

Protocolo SSH: http://www.ietf.org/html.charters/secsh-charter.html

Bibliografía:

El escarabajo de oro, de Edgar Alan Poe

Departament of Defense Trusted Computer System Evaluation Criteria, National Computer Security Center (El Libro Naranja).

Cifrado Simetrico, Asimetrico e Hibrido: PKI Infraestructura de claves publicas, de Andrew Nash, William Duane, Celia Joseph y Derek Brink, Osborne Mc. Graw-Hill

Comunicaciones y Redes de Computadoras, de William Stallings, Prentice Hall.

Cálculo y Geometria Analítica, de Roland E. Larson y Robert P. Hostetler, Mc. Graw-Hill

"La Mandragore et le mythe de la 'naissance miraculeuse'", Zalmoxix III, de Mircea Eliade. París-Bucarest, 1943, pags. 1-52.

Agradecimientos

A Liliux y sus asadetes con aventuras...

Y principalmente a ustedes por estar aca...

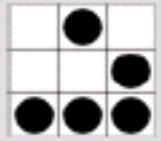
¿Preguntas?

En las sabiamente inmortales palabras de Pepe Le Pew:

“El que espera y no desespera se lleva la mejor pera.”

Demás está decir que si te sentís muy generoso, también "acepto donaciones"...

[@Vampii]



vampii en centrux.org