UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Envio de contraseñas

Breve procedimiento para en envio de contraseñas planas.
Como buena practica todas las password deben estar encriptadas.
Si se va a mandar una password de cuenta, se debe tratar de enviar una password de uso unico, que cuando el usuario se loguee lo obligue a cambiarla.
En el caso de que esto no se puedea realizar, como minimo deberia mandarse la password cifrada.

Cifrado Asimetrico

Consiste en el encriptado de un archivo que contiene la password en texto plano, usando un juego de llaves publico-privada con GPG.
Flujo:

1. Remitente crea pass segura
2. Destinatario de la password debe crear juego de llaves
3. Destinatario debe enviar/publicar **llave publica**
4. Remitente encripta password con la pubkey
5. Remitente envia archivo encriptado con pubkey.
6. Destinatario desencripta password

Linux

Creacion juego de llaves

Hay varias formas de crear el juego de llaves pero se opta por el mas intuitivo que es el modo interactivo.

```
gpg --full-generate-key
```

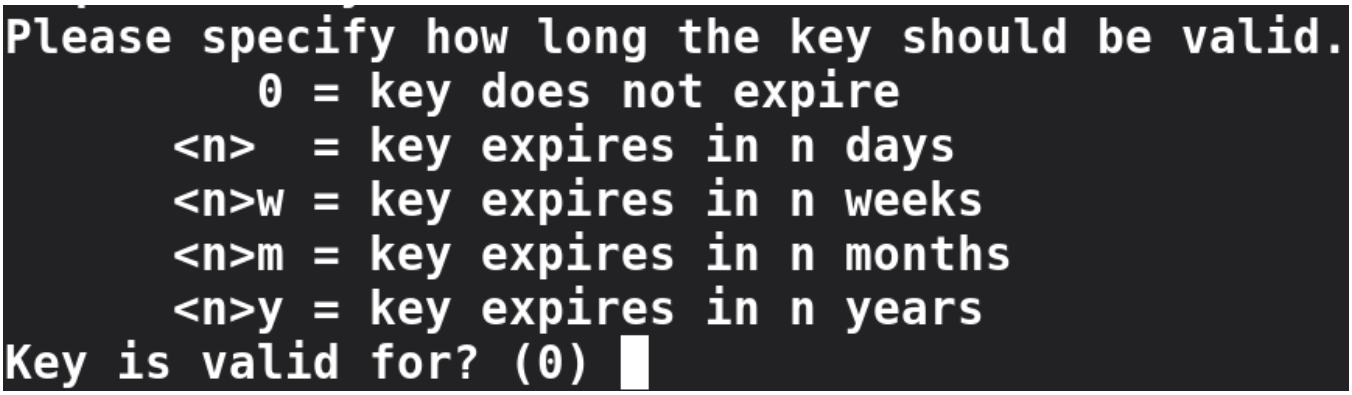
Este comando nos despliega un prompt en el que nos va a ir pidiendo las caracteristicas de la key a crear.

```
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection?
```

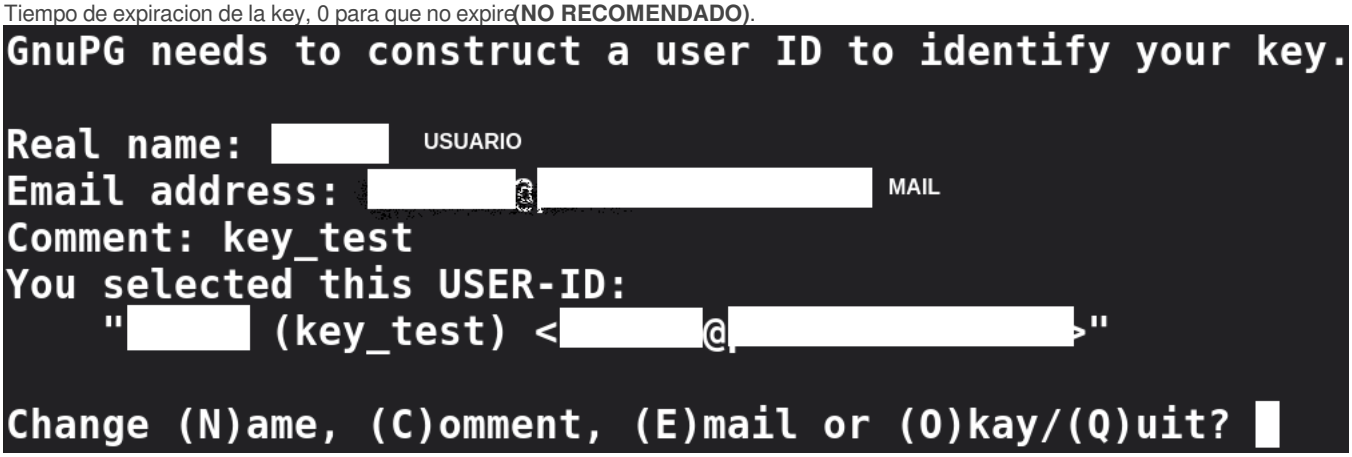
Elegir tipo de algoritmo, aca queda a gusto de cada uno, el default esta perfecto.

```
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072)
```

Longitud de la clave en un algoritmo de cifrado. Este tamaño se mide generalmente en bits. Tambien el default esta bien.



Tiempo de expiracion de la key, 0 para que no expire**(NO RECOMENDADO)**.



Aca pide los datos para generar el ID de la llave.

Se pide que se mueva el mouse o use la PC para ayudar a generar un numero aleactorio y la key esta creada.

Se puede verificar con el comando

```
gpg --list-keys
```

Exportar pubkey

Una vez creado el juego de llaves, se debe exportar la pubkey para poder enviarla.

```
gpg --armor --export $MAIL@example.com > pubkey_1.asc
#--armor genera la clave en formato ASCII, lo que facilita
# su envío a través de correos o mensajes
```

Encriptado del mensaje

Primero se debe importar en nuestro sistema la pubkey recibida.

```
gpg --import pubkey_1.asc
```

Ahora ya se puede encriptar en mensaje alojado en un archivo.

```
gpg --encrypt --armor -r $MAIL@example.com msjsecreto.txt
# -r especifica al destinatario
```

Recepcion del archivo

Una vez recibido el archivo .asc se desencripta con el comando

```
gpg --decrypt msjsecreto.txt.asc
```

En Windows

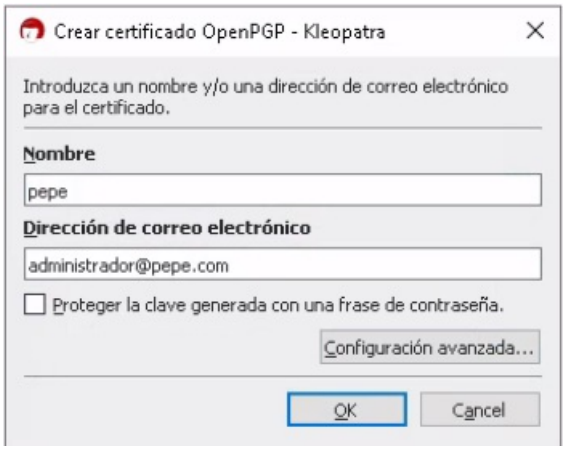
Se debe instalar GnuPG, el software que se deja a continuacion aparte de no necesitar licencia instala una GUI para realizar el procedimiento mas facil, pero se aclara que se podria usar solamente powershell.

Link a Gpg4win

Una vez instalado, sino se abrio automaticamente, abrir la aplicacion "Kleopatra".

Aca se debe crear un nuevo par de claves desde "File > New Key Pair"

Se abre un prompt en el que nos pide el nombre y el mail, ademas se da la opcion de usar una pass para asegurar el juego de llaves.



En la configuracion avanzada nos deja elegir el algoritmo de encriptado, la duracion de la key y su destino.



En este punto ya tenemos creado el par de llaves, ahora nos queda exportar la pubkey para poder enviarla, esto se hace con el boton **"EXPORT"** en la barra de herramientas.

Una vez enviada la pubkey al que nos debe enviar el msj, este debe encriptarlo haciendo uso de esta y enviarnos el archivo cifrado.

Por ultimo, con la opcion**"Descifrar**/**Verificar"** nos abre el explorador de archivos, donde elegimos el mensaje encriptado que nos mandaron, siguiente siguiente, y podemos guardar el archivo desencriptado donde queramos....zip zap

---

Revisión #7
★Creado 25 septiembre 2024 16:55:38 por Federico Alberto Bisso
✎Actualizado 9 octubre 2024 17:47:02 por Federico Alberto Bisso