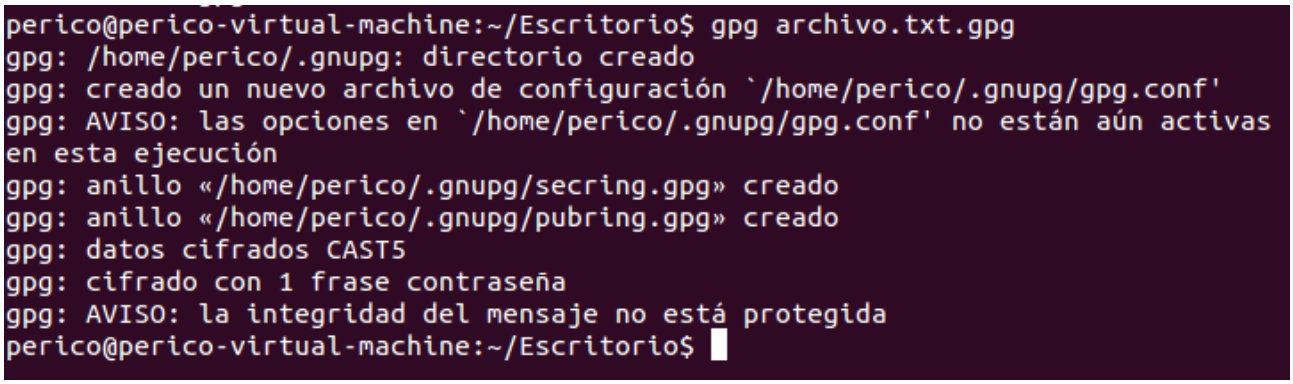
Práctica de Criptografía

Alejandro Abad

Ejercicio: Cifrado simétrico de un documento

Creo un documento y lo cifro:

Le mando el documento a mi compañera Morgana y lo descifra:



Lo ciframos con -a y le hacemos un cat al contenido:

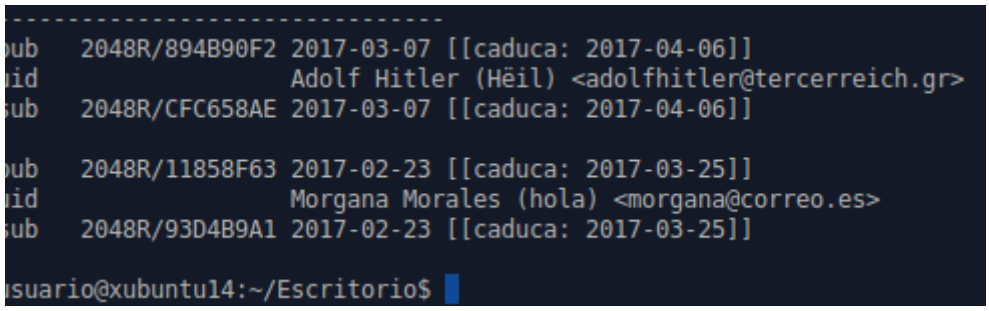
Ejercicio: Cifrado simétrico de un documento

Creo mi clave pública y privada:

```
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Por favor seleccione tipo de clave deseado:
   (1) RSA y RSA (predeterminado)
   (2) DSA y Elgamal
   (3) DSA (sólo firmar)
   (4) RSA (sólo firmar)
¿Su selección?: 1
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048)
El tamaño requerido es de 2048 bits
Por favor, especifique el período de validez de la clave.
         0 = la clave nunca caduca
      <n>  = la clave caduca en n días
      <n>w = la clave caduca en n semanas
      <n>m = la clave caduca en n meses
      <n>y = la clave caduca en n años
¿Validez de la clave (0)? 30
La clave caduca jue 06 abr 2017 20:20:50 CEST
¿Es correcto? (s/n) s

Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo electrónico de esta forma:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: Alejandro Adolf
Dirección de correo electrónico: heilhatler@gmail.com
Comentario: Hëil Hatler
Está usando el juego de caracteres `utf-8'.
Ha seleccionado este ID de usuario:
    «Alejandro Adolf (Hëil Hatler) <heilhatler@gmail.com>»

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v
Necesita una frase contraseña para proteger su clave secreta.

gpg: el agente gpg no esta disponible en esta sesión
```

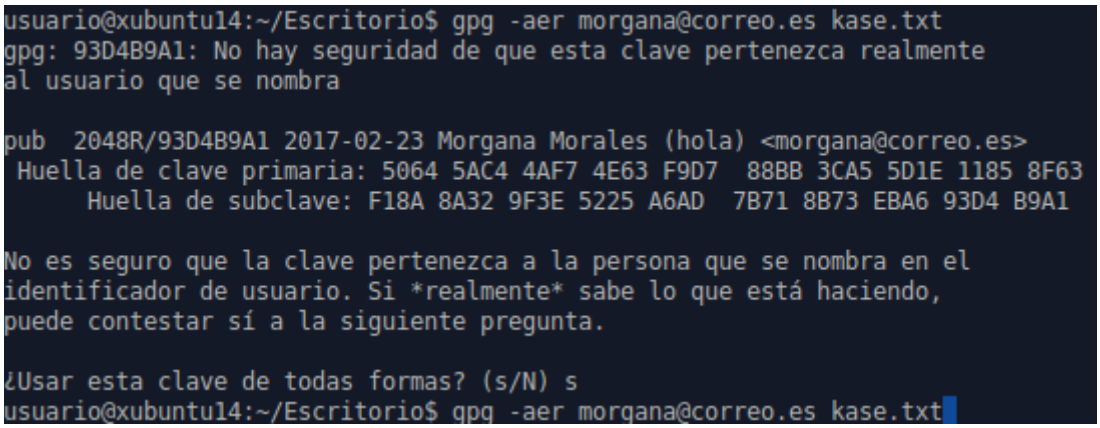
Ejercicio: Exportar e importar

Mi compañera Morgana me pasa su llave y la importo a mi llavero de claves:

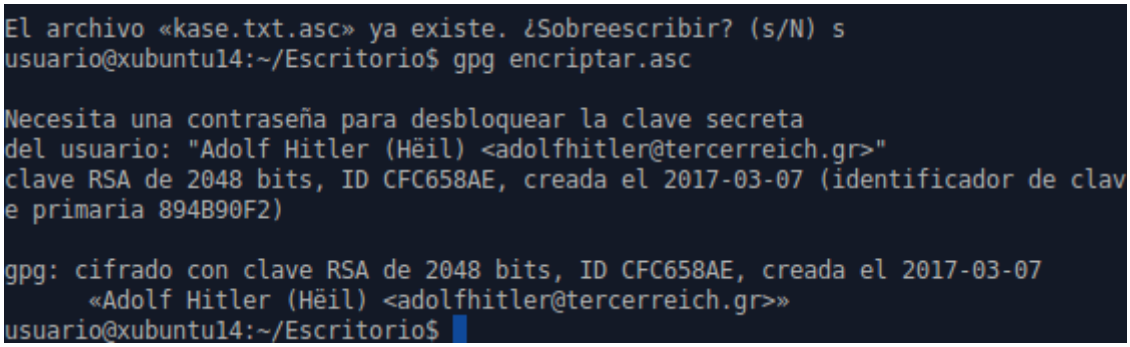


Ejercicio: Cifrado y descifrado de un documento

Cifro un archivo con la clave pública de Morgana:



Morgana me pasa un archivo codificado con mi clave pública y lo descifro:



Ejercicio: Firma digital de un documento

Creo un archivo y lo firmo:

```
usuario@xubuntu14:~/Escritorio$ gpg -sb -a firmameloscojones

Necesita una contraseña para desbloquear la clave secreta
del usuario: "Adolf Hitler (Hëil) <adolfhitler@tercerreich.gr>"
clave RSA de 2048 bits, ID 894B90F2, creada el 2017-03-07

usuario@xubuntu14:~/Escritorio$
```

Morgana me pasa un archivo firmado por ella, compruebo la firma, y es correcta:

```
usuario@xubuntu14:~/Escritorio$ gpg morganamorales.asc
gpg: Firmado el mar 07 mar 2017 20:42:33 CET usando clave RSA ID B922B1D3
gpg: Firma correcta de «Morgana Morales (hola) <morgana@correo.es>»
gpg: AVISO: ¡Esta clave no está certificada por una firma de confianza!
gpg:          No hay indicios de que la firma pertenezca al propietario.
Huellas digitales de la clave primaria: 1569 9D00 B554 AA2F 0963  6941 7EF3 E76F
 B922 B1D3
usuario@xubuntu14:~/Escritorio$
```

Modifico el archivo que me ha pasado firmado Morgana, y al volver a comprobar la firma me salta un error porque la integridad del archivo ya no es la misma:

```
usuario@xubuntu14:~/Escritorio$ gpg morganamorales.asc
gpg: Firmado el mar 07 mar 2017 20:42:33 CET usando clave RSA ID B922B1D3
gpg: Firma INCORRECTA de «Morgana Morales (hola) <morgana@correo.es>»
usuario@xubuntu14:~/Escritorio$
```