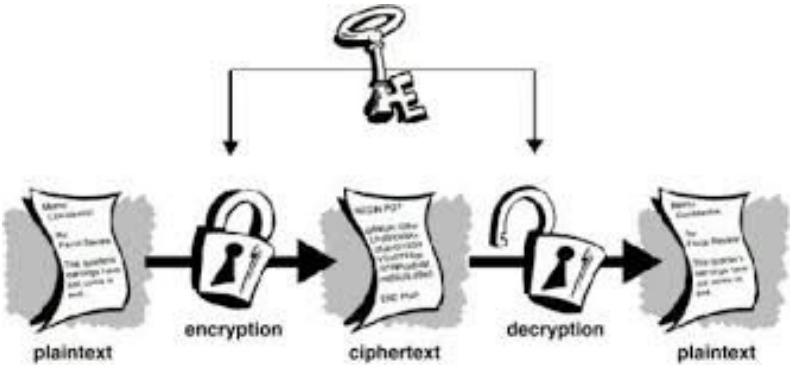
Practica criptografía



Por:
Antonio Quiles Sempere

Ejercicio 1:

Creamos un fichero con nano antonioquiles1 para crear el documento y utilizamos el comando gpg -c antonioquiles1 para crearlo y ponemos la contraseña acordada

```
perico@perico-virtual-machine:~/Desktop$ ls
destino.txt  documento  Untitled Document~
perico@perico-virtual-machine:~/Desktop$ mv documento antonioquiles1
perico@perico-virtual-machine:~/Desktop$ gpg -c antonioquiles1
```

Ahora le he pedido el documento que ha encriptado mi compañero para desencriptarlo, llamado jose1.gpg, con el comando gpg jose1.gpg y poniendo la contraseña acordada y con un ls nos pondrá el documento sin el .gpg, el que se podria leer

```
perico@perico-virtual-machine:~/Desktop$ gpg jose1.gpg
gpg: CAST5 encrypted data
gpg: encrypted with 1 passphrase
gpg: WARNING: message was not integrity protected
perico@perico-virtual-machine:~/Desktop$ ls
antonioquiles1  antonioquiles1.gpg  jose1  jose1.gpg  Untitled Document~
perico@perico-virtual-machine:~/Desktop$
```

Ejercicio 2:

Utilizando el fichero que hemos creado en el ejercicio anterior utilizamos el comando gpg -c -a antonioquiles1 y al hacer ls veremos el fichero con terminación .asc y ponemos la contraseña acordada:

```
perico@perico-virtual-machine:~/Desktop$ gpg -c -a antonioquiles1
perico@perico-virtual-machine:~/Desktop$ ls
antonioquiles1      antonioquiles1.gpg  jose1.gpg
antonioquiles1.asc  jose1               Untitled Document~
```

Ahora le he pedido el documento que ha encriptado mi compañero para desencriptarlo, llamado jose1.asc, con el comando gpg jose1.asc y poniendo la contraseña acordada y con un ls nos pondrá el documento sin el .asc, el que se podría leer.

```
erico@perico-virtual-machine:~/Desktop$ gpg jose1.asc
pg: CAST5 encrypted data
pg: encrypted with 1 passphrase
ile `jose1' exists. Overwrite? (y/N) y
pg: WARNING: message was not integrity protected
erico@perico-virtual-machine:~/Desktop$
```

Ejercicio 3

Con el comando gpg –gen-key nos pedira hacer cosas para guardar caracteres aleatoriamente para crear la clave privada.

```
perico@perico-virtual-machine:~/Desktop$ gpg --gen-key
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

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)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 1m
Key expires at Sun 09 Apr 2017 07:30:51 PM CEST
Is this correct? (y/N) y
```

Aquí ponemos el nombre y el correo:

```
You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Antonio
Email address: antonio@correo.com
Comment:
You selected this USER-ID:
    "Antonio <antonio@correo.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
```

Hacemos un ls y vemos la clave creada

```
perico@perico-virtual-machine:~/Desktop$ ls
antonioquiles1      antonioquiles1.gpg       jose1      jose1.gpg
antonioquiles1.asc  clave_antonioquiles.asc  jose1.asc  Untitled Document~
perico@perico-virtual-machine:~/Desktop$
```

Ejercicio 4

Utilizamos el siguiente comando para encriptar con tu clave pública un fichero llamado documento_conclave.

```
perico@perico-virtual-machine:~/Desktop$ gpg -a -r Antonio --encrypt documento_c
onclave
perico@perico-virtual-machine:~/Desktop$ ls
antonioquiles1      clave_antonioquiles.asc  jose1      jose_roda.asc
antonioquiles1.asc  documento_conclave       jose1.asc  Untitled Document~
antonioquiles1.gpg  documento_conclave.asc   jose1.gpg
perico@perico-virtual-machine:~/Desktop$
```

Ejercicio 5

Creamos un documento que vamos a firmar y usamos el siguiente comando para encriptar y firmar un documento:

```
perico@perico-virtual-machine:~/Desktop$ gpg -sb -a documento_firmado_Antonio

You need a passphrase to unlock the secret key for
user: "Antonio Quiles (gg wp easy tutorial) <sombraop@gmail.com>"
2048-bit RSA key, ID 46D12A4D, created 2016-12-14

gpg: Invalid passphrase; please try again ...

You need a passphrase to unlock the secret key for
user: "Antonio Quiles (gg wp easy tutorial) <sombraop@gmail.com>"
2048-bit RSA key, ID 46D12A4D, created 2016-12-14

perico@perico-virtual-machine:~/Desktop$ ls
antonioquiles1           documento_conclave.asc         jose1.asc
antonioquiles1.asc       documento_firmado_Antonio      jose1.gpg
antonioquiles1.gpg       documento_firmado_Antonio.asc  jose_roda.asc
clave_antonioquiles.asc  documentojose2                 Untitled Document~
documento_conclave       jose1
```

Ahora modificas el documento firmado ligeramente y al usar el comando para confirmar la firma nos dara el siguiente error:

```
perico@perico-virtual-machine:~/Desktop$ gpg --verify documento_firmado_Antonio
asc
gpg: CRC error; A03568 - B57F47
gpg: [don't know]: invalid packet (ctb=4e)
gpg: no signature found
gpg: the signature could not be verified.
Please remember that the signature file (.sig or .asc)
should be the first file given on the command line.
```