

Criptografía de clave simétrica

Contenido

Introducción	1
Ejercicio 1. Comenzamos.....	1
Ejercicio 2. Firmar la clave del compañero	6
Ejercicio 3. Investiga y practica.....	9


Introducción

En la siguiente práctica, utilizaremos un programa llamado Cryptophane, que funciona bajo Windows. Se trata de una aplicación de software libre que además permite utilizar el sistema de cifrado simétrico y el asimétrico. Para el cifrado de clave pública utiliza GnuPG, una versión libre de PGP.

Cryptophane permite encriptar archivos y firmarlos para verificar su autenticidad. También permite descifrar archivos cifrados y verificar firmas generadas con cualquier aplicación de OpenPGP.

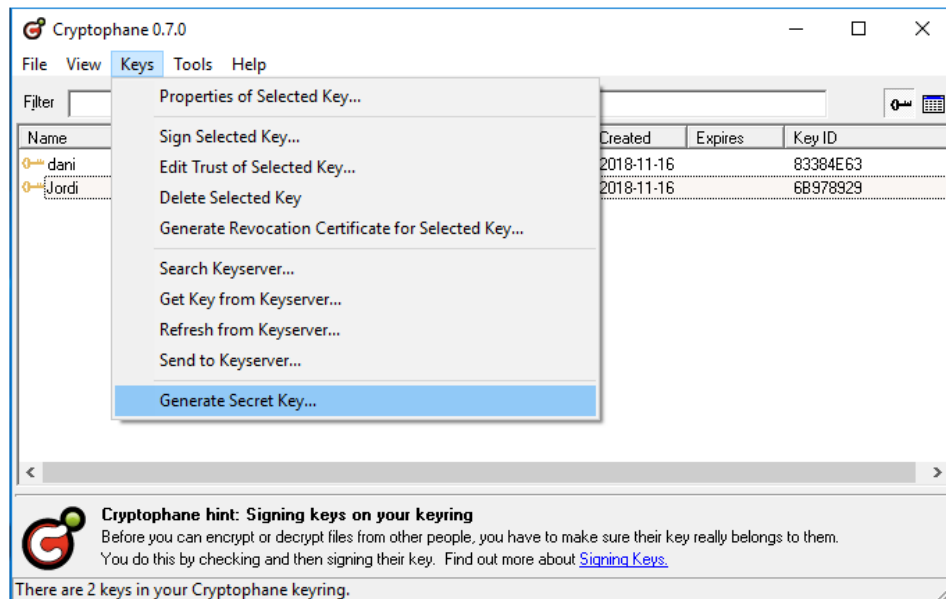
Ejercicio 1. Comenzamos...

1. En primer lugar, instalamos el programa **Cryptophane** descargándolo de la siguiente dirección web: <https://code.google.com/archive/p/cryptophane/downloads>

Project	 cryptophane
Source	
Issues	
Wikis	
Downloads	

File	Summary + Labels	Uploaded	Size
cryptophane-0.7.0.exe.sig	Cryptophane 0.7.0 signature file Type-Archive Featured OpSys-Windows	Aug 11, 2009	65
cryptophane-0.7.0.exe	Cryptophane 0.7.0 beta installer (requires GnuPG) Type-Installer Featured OpSys-Windows	Aug 11, 2009	602.08KB
cryptophane-0.7.0-gnupg-1.4.2.exe.sig	Cryptophane 0.7.0 + GnuPG signature file Featured OpSys-Windows Type-Archive	Aug 11, 2009	65
cryptophane-0.7.0-gnupg-1.4.2.exe	Cryptophane 0.7.0 beta + GnuPG 1.4.2 full installer Type-Installer OpSys-Windows Featured	Aug 11, 2009	1.04MB

2. A continuación, creamos nuestra clave, haciendo clic en Keys -> “Generate Secret Key...” y rellenamos los campos:



The 'Generate Secret Key' dialog box prompts the user to enter details for a new key. It includes fields for Name, E-mail address, Comment, New passphrase, and Confirm passphrase. There is also a checkbox for 'Key expires' and dropdown menus for 'DSA key length' and 'ElGamal key length', both set to 1024. 'Generate' and 'Cancel' buttons are at the bottom.

Enter your details below to create a new key for your Cryptophane keyring.

Name:

E-mail address:

Comment:

New passphrase:

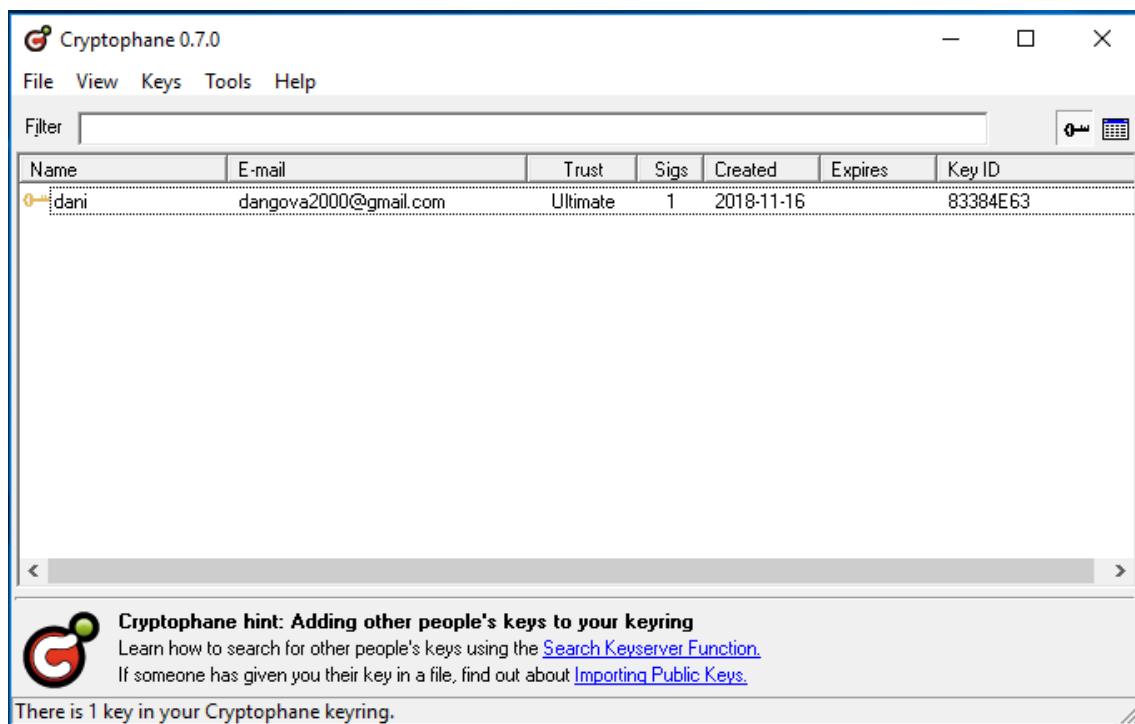
Confirm passphrase:

☐ Key expires

DSA key length:

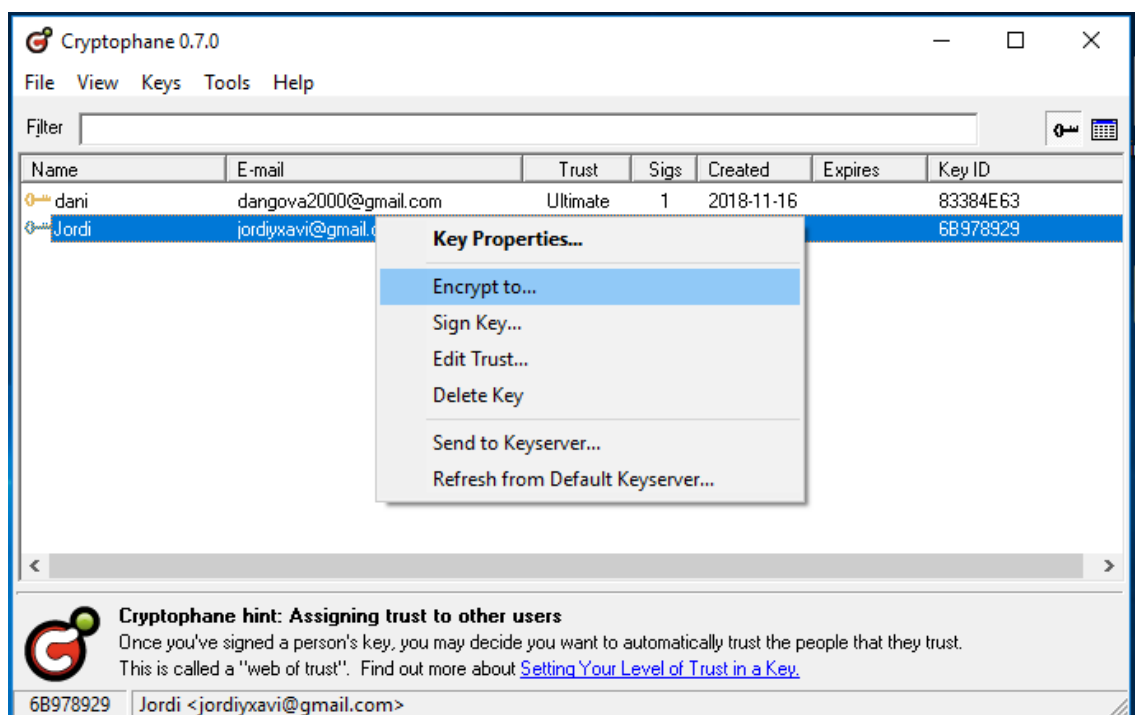
ElGamal key length:

3. Pulsamos en Generate, y se nos ha debido crear una clave en nuestra aplicación:



4. A continuación creamos en el equipo un documento de texto. No es necesario que su extensión sea .doc u .odt, basta con un archivo en texto plano de tipo .txt. Le ponemos **nuestro nombre.txt** y escribimos un contenido dirigido a tu compañero.

5. Abrimos el programa y seleccionamos File/ Encrypt (o <Ctrl> + <E>) para seleccionar el documento creado anteriormente para encriptarlo.



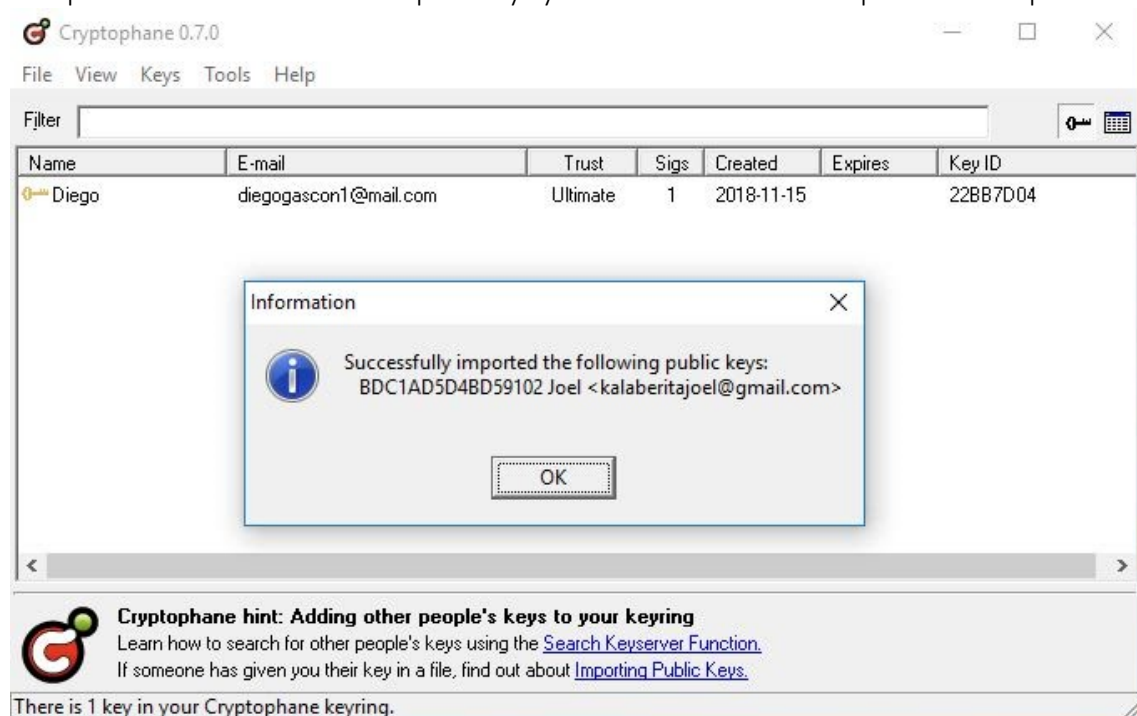
6. Seleccionamos el archivo e indicamos que se guarde con el nombre **Fichero-cifrado.txt** (botón Output into file...). En la ventana que aparece después, seleccionamos Encrypt with shared passphrase (symmetric encryption) y (desmarcamos Encrypt with public key).

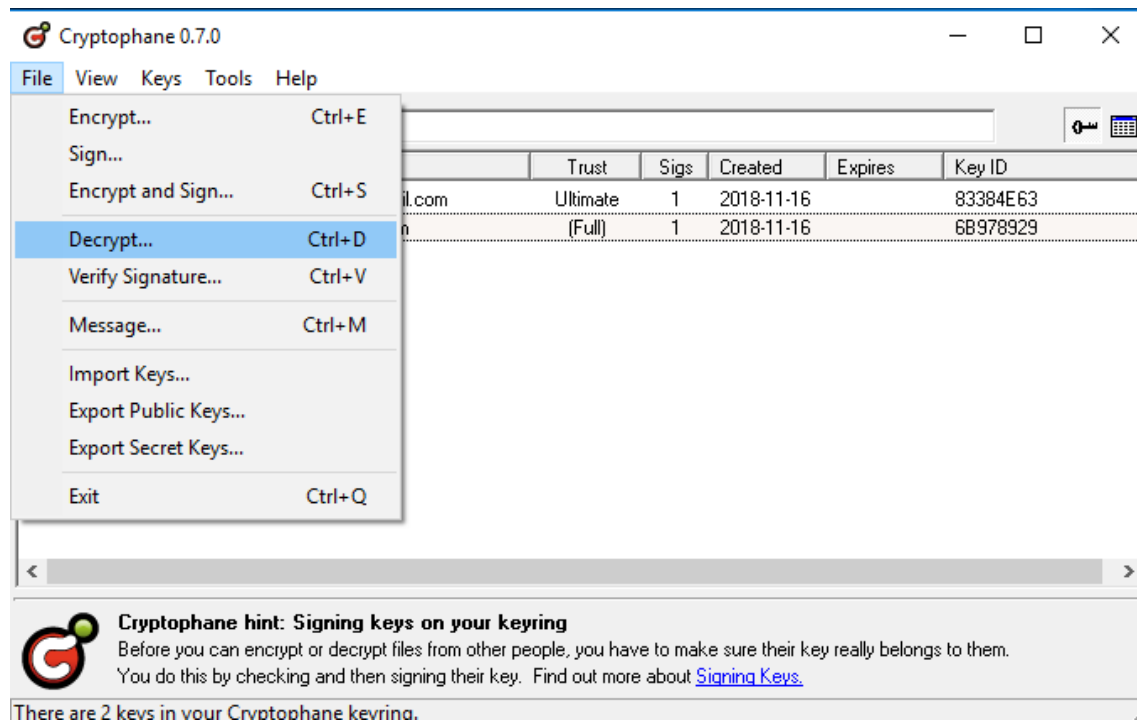
7. Hacemos click en el botón Process y luego escribimos dos veces la clave que vamos a usar para el cifrado simétrico.

8. Enviamos el documento al compañero y le indicamos la clave a través de un canal seguro, porque si no, la encriptación no serviría de nada (por ejemplo, si le enviamos el documento cifrado, lo que no podemos es enviarle la clave en el mismo mensaje).

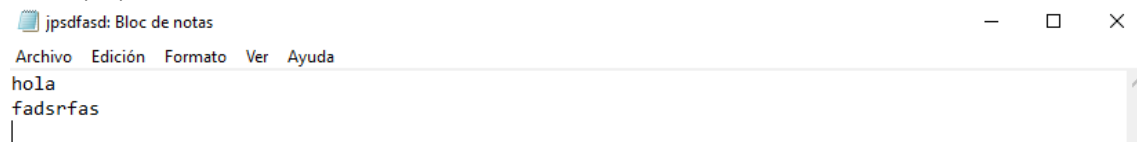
9. Cuando el destinatario del mensaje quiera abrir el fichero cifrado con el Bloc de notas, le pedirá la clave utilizada para encriptarlo, que le habrá sido proporcionada por el emisor. Sin esa clave, no podrá abrir el archivo. Evidentemente, este archivo es ininteligible para cualquier persona que lo abra sin tener la clave.

10. Como ambos tenemos el programa, pediremos al compañero que nos pase su clave y la usaremos para desencriptar el archivo o fichero que nos haya mandado nuestro compañero. Seleccionamos "import key" y seleccionamos la clave pública de la persona.





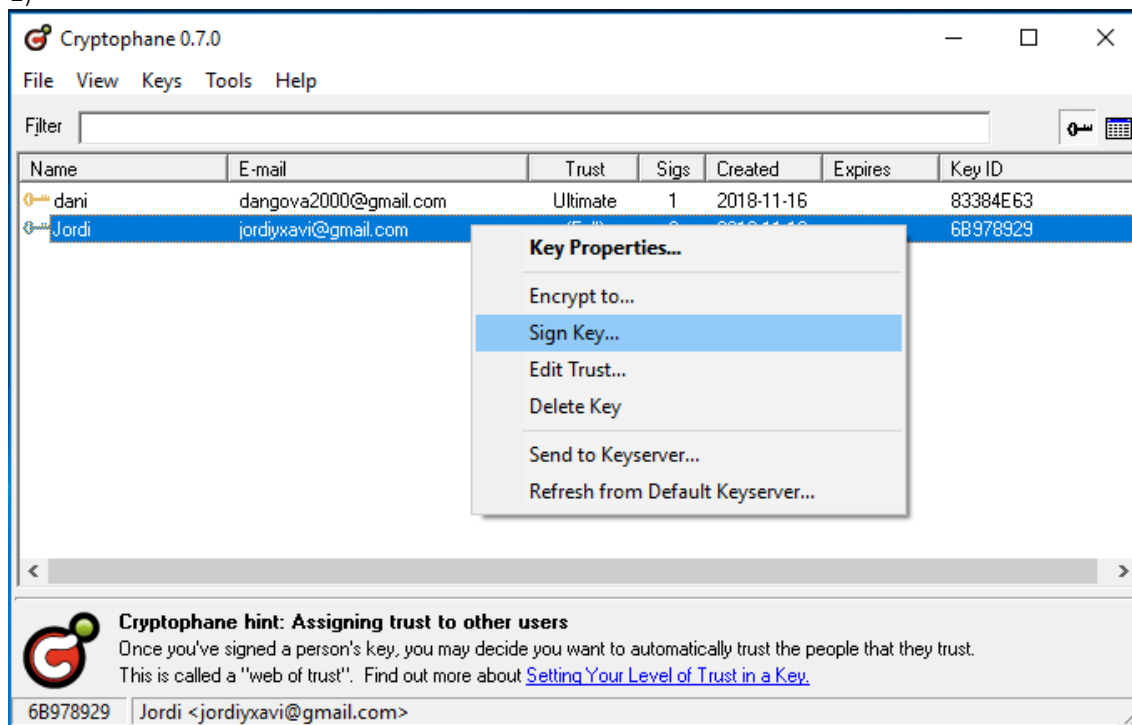
11. Y ya podríamos leer la información del documento:



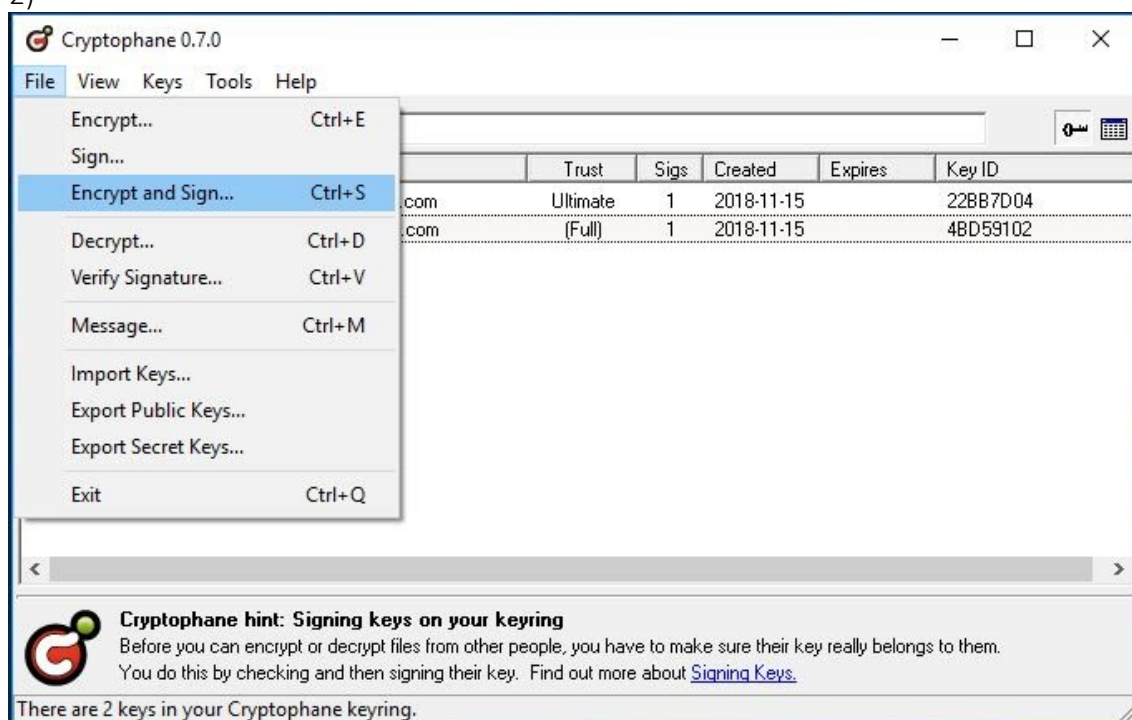
Ejercicio 2. Firmar la clave del compañero

1. Como anteriormente habíamos importado la clave, a continuación, firmaremos la clave del compañero haciendo click en 1) “Sign Key...” o en 2) “Encrypt and Sign ...”:

1)

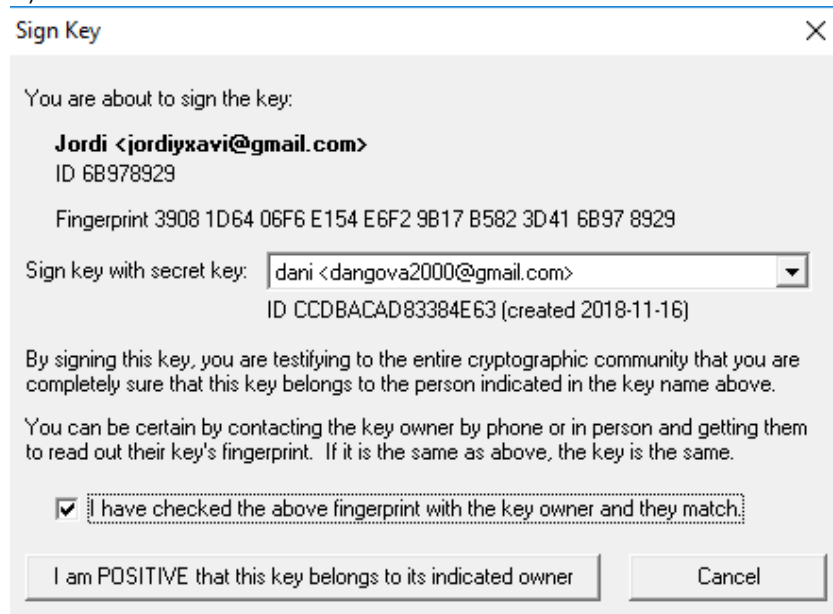


2)

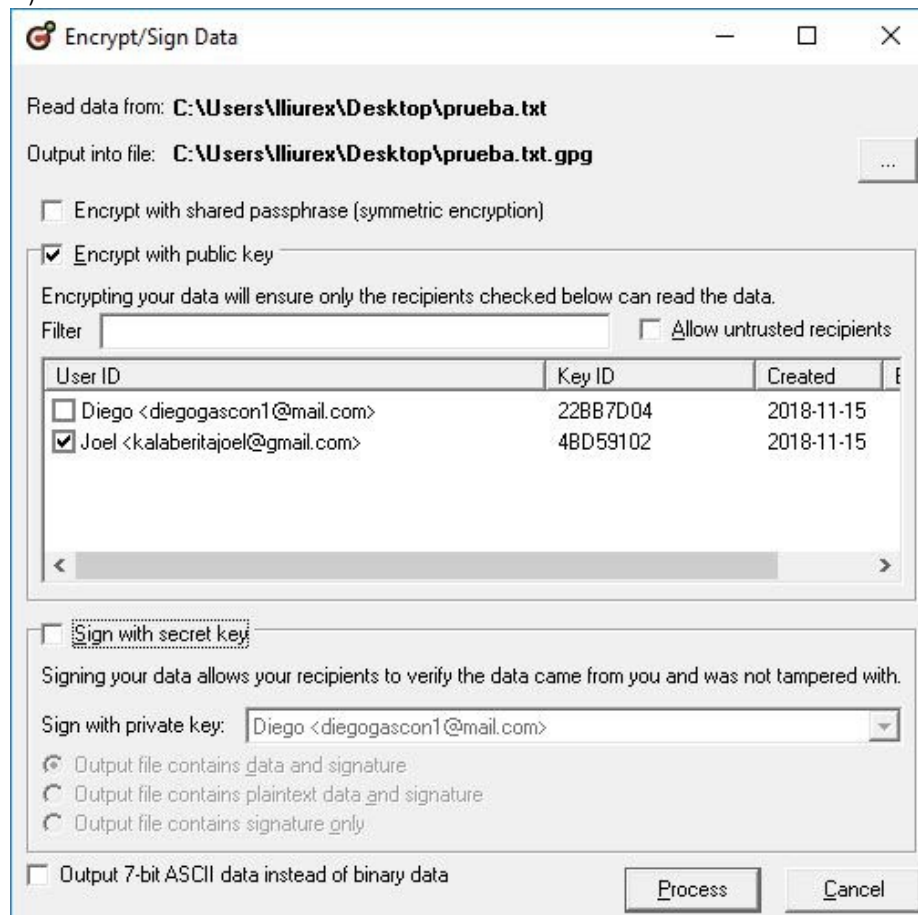


2. Firmaremos su clave con nuestra clave secreta creada al inicio del ejercicio1:

1)



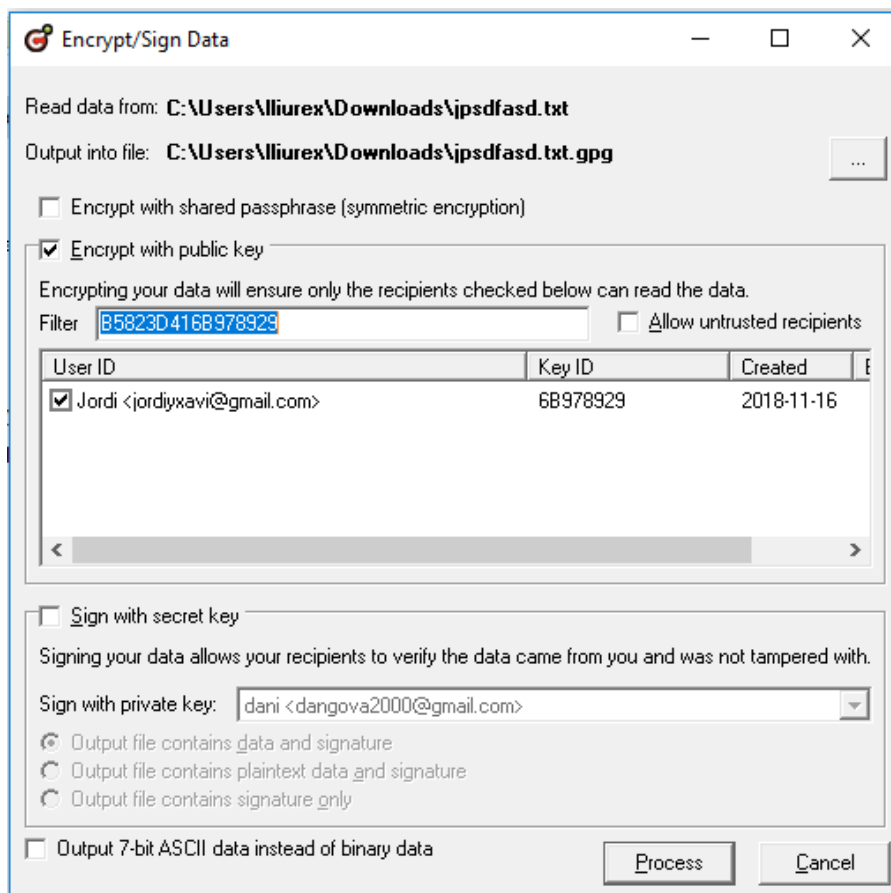
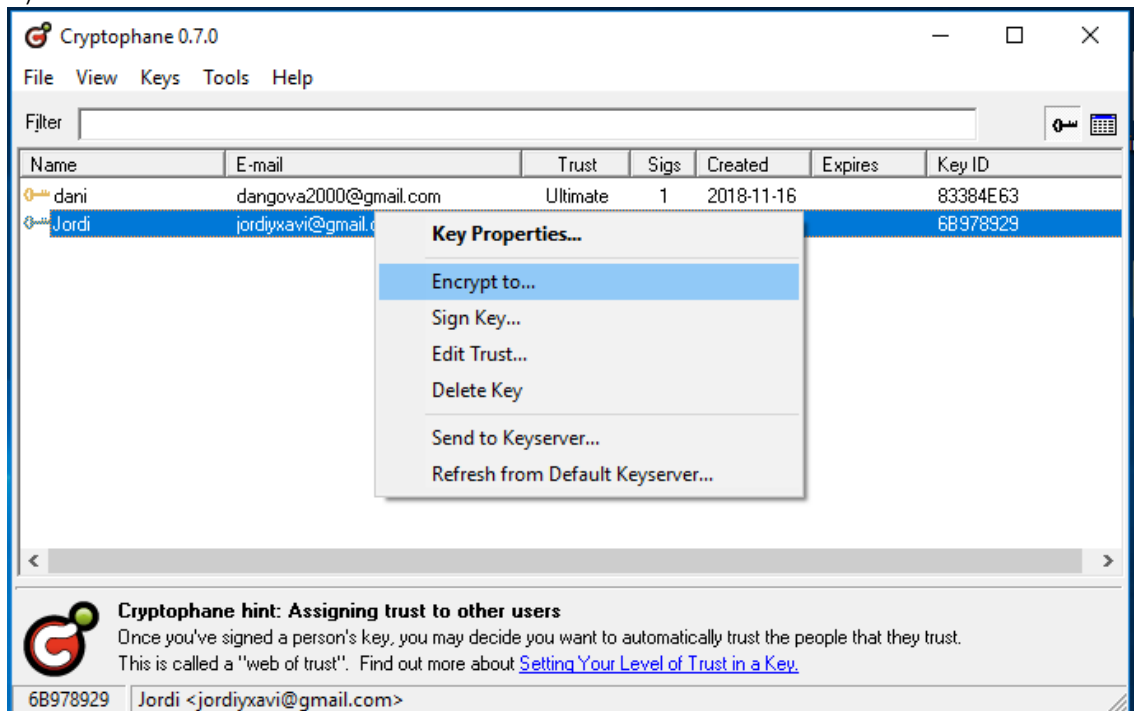
2)



2.1) Seleccionamos "Encrypt with public key" del usuario al cual queremos mandársela para que el con su privada pueda desencriptar el documento.

3. A continuación, encriptaremos el fichero que nos ha facilitado con su propia clave pública.

1)



4. Y después de todo el proceso el podrá abrir el archivo con su clave privada, pero estará firmado por nosotros. Se lo mandaremos por correo, por ejemplo, y le tendremos que mandar la clave publica y el texto firmado digitalmente. Para que él pueda ver el contenido del mensaje necesita nuestra clave pública.

5. Seleccionamos Decrypt y el archivo el cual queramos descriptar:

```
-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA1  
  
hds uiasd asjdkjasiod jasjk d asjkd askd ajksd aksdh  
dsa d  
asdjklajs da  
d  
asdjas  
d  
  
daios diaos  
-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v1.4.2 (MingW32)  
  
iD8DBQFb7o9YaMYqwiK7fQQRahJcAJ9UC2JaOuN0gm+Af+0LWM7xYhWWXwCgkoV2  
vpgw2dkrjE0VyCGwk556KIM=  
=+dVS  
-----END PGP SIGNATURE-----
```

Ejercicio 3. Investiga y practica...

1. Busca en internet herramientas alternativas de cifrado o encriptación de archivos como la anterior que has utilizado. Apunta como mínimo 10 y describe para qué se usan.

2. Descarga una gratuita y haz un pequeño manual explicando su uso (no vale elegir la misma herramienta que tu compañero de al lado). De esta manera, comprobaré que has entendido cómo funciona la encriptación.