Secret messages with public and private keys: Teacher Instructions

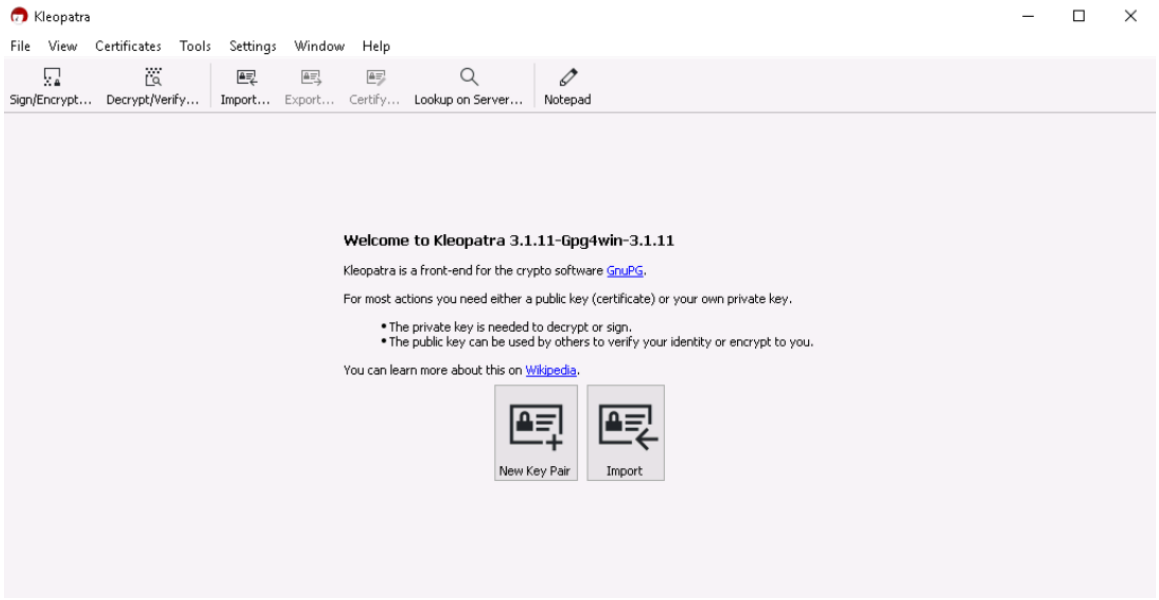
Introduction:

Welcome to the secret messages workout where you will learn about public and private key encryption. When transmitting messages across the Internet, there's a possibility they may be intercepted by a man-in-the-middle attack. To counteract this, encryption algorithms were created to make reading messages much more difficult for attackers.

The mission:

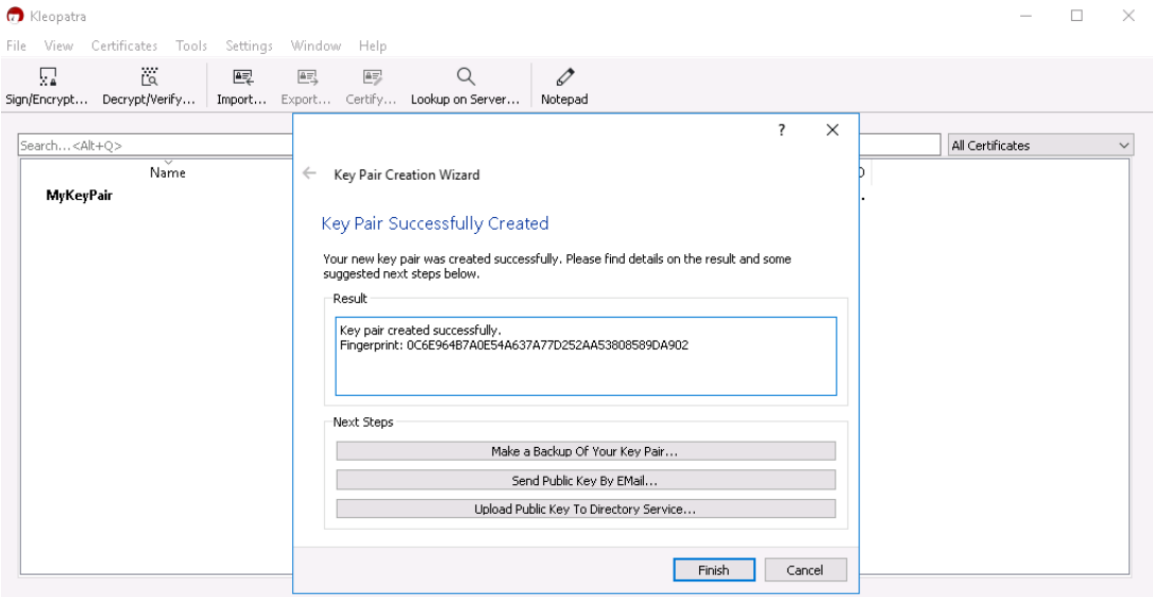
In this lab, students will learn how to generate and use public and private keys for use in encryption.

To begin, students must click on Kleopatra. The program should start and look like this.

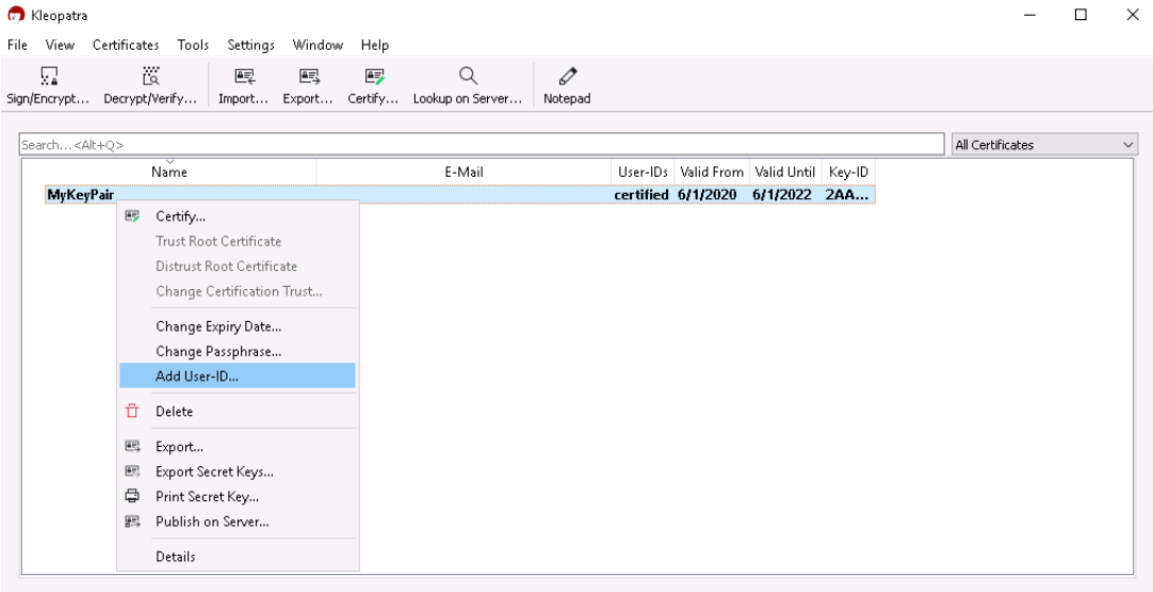


Click new key pair and go thru and choose the default options. At some point, it will ask you about adding a new passphrase.

Once you've done that and finished the other options, it should end up like this screen.

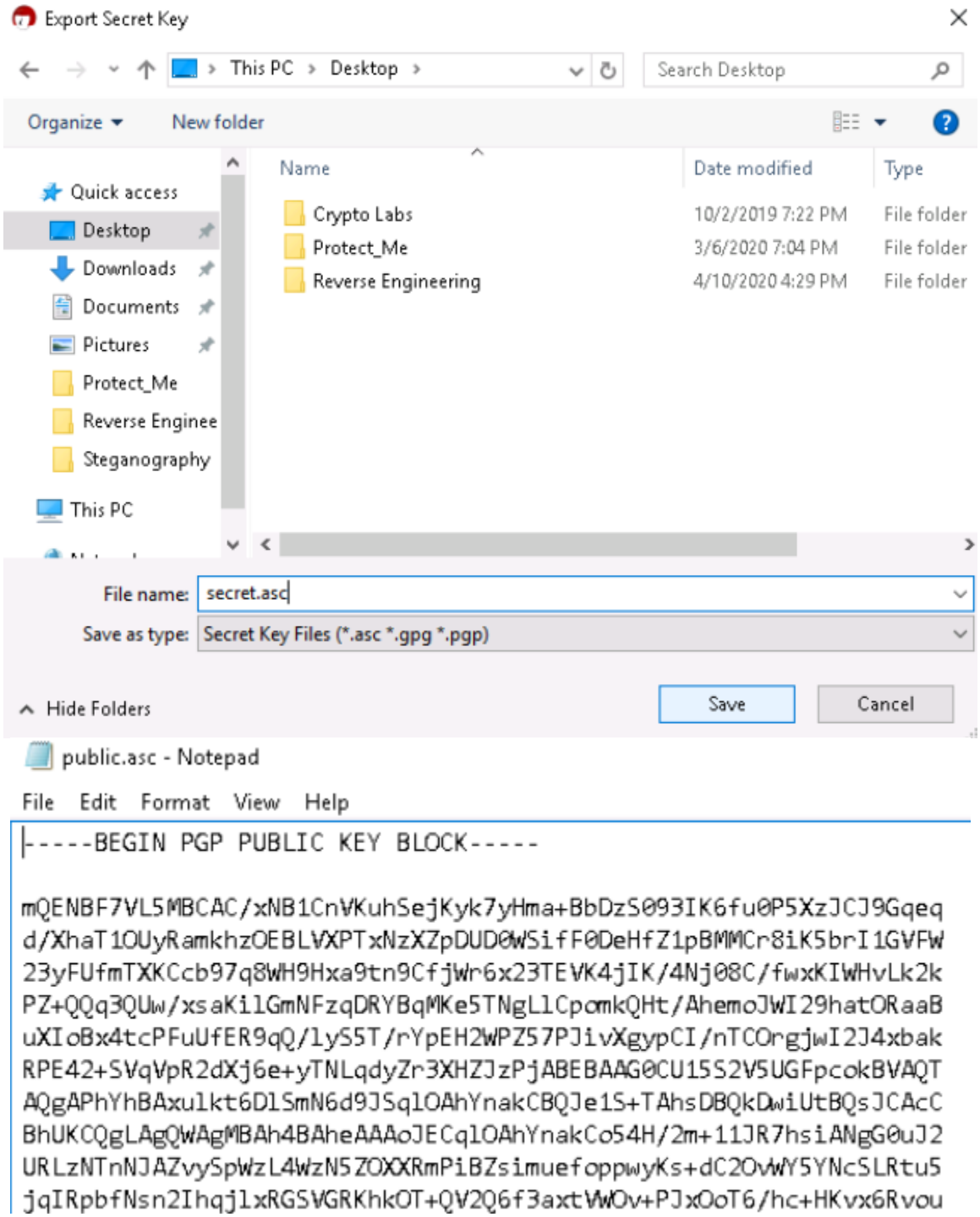


Right click on the my key pair and you should be presented with a number of options. For this lab, the most important features are the export and export secret key.



Export will allow you to save your public key to your desktop. You will be able to read the contents of the .asc file in a text editor like Notepad.

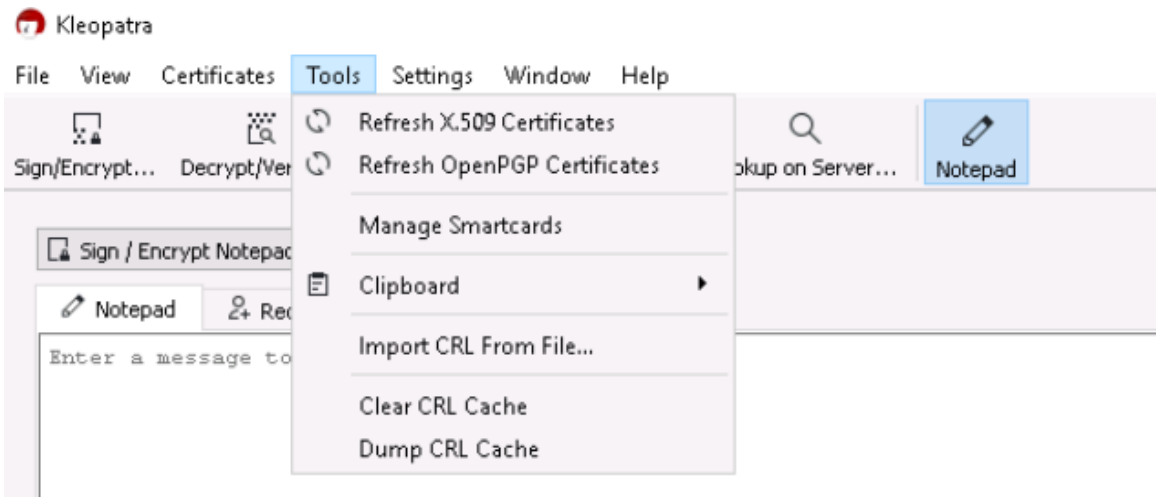
Export secret will allow you to save your private key to your desktop. You will not be able to read the contents of the .asc file but that won't be important.



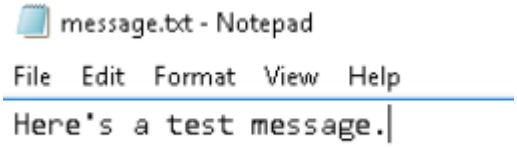
Open up the public key and select the entire text. Right click and copy it to the clipboard.

Now go to tools on Kleopatra and here you will be presented with a number of options.

Certificate import should be available, click it to import your public key.



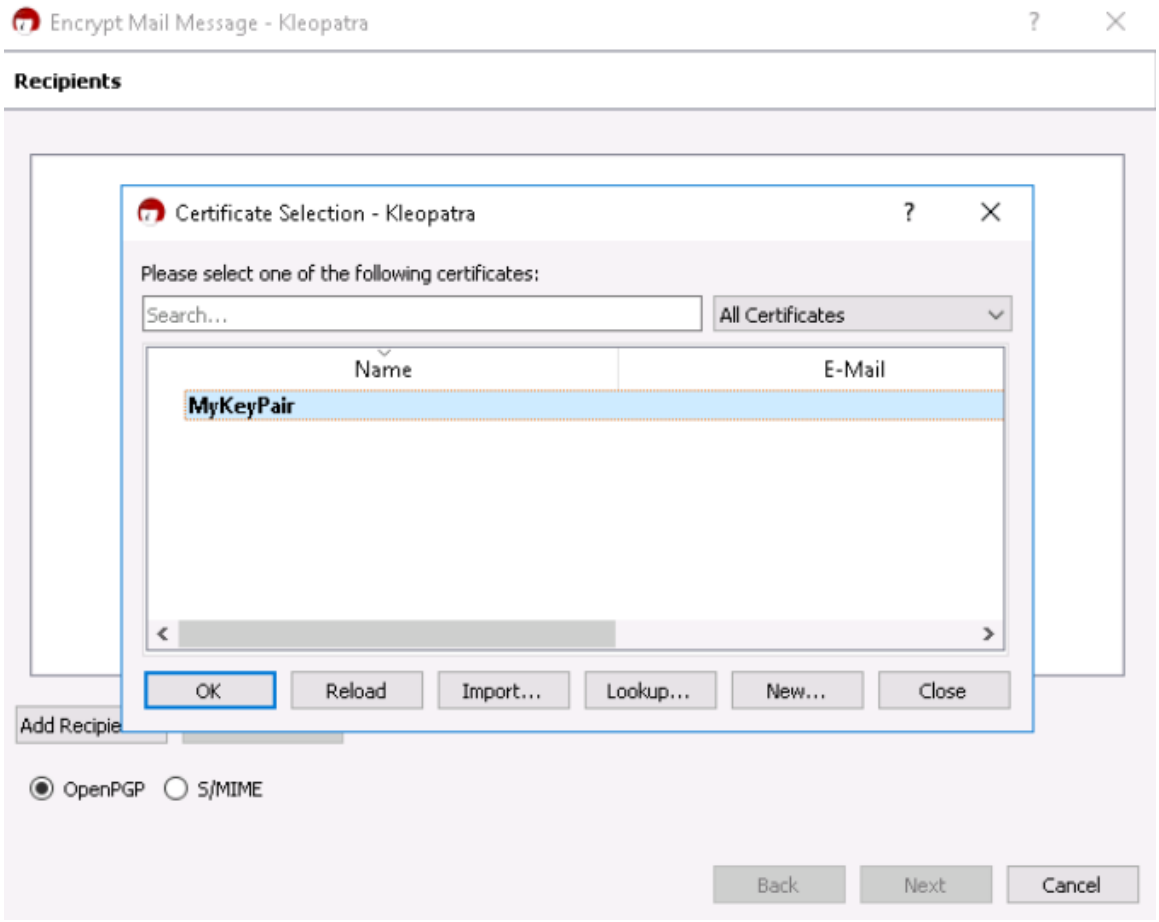
Now create a new text file and write a message in it.



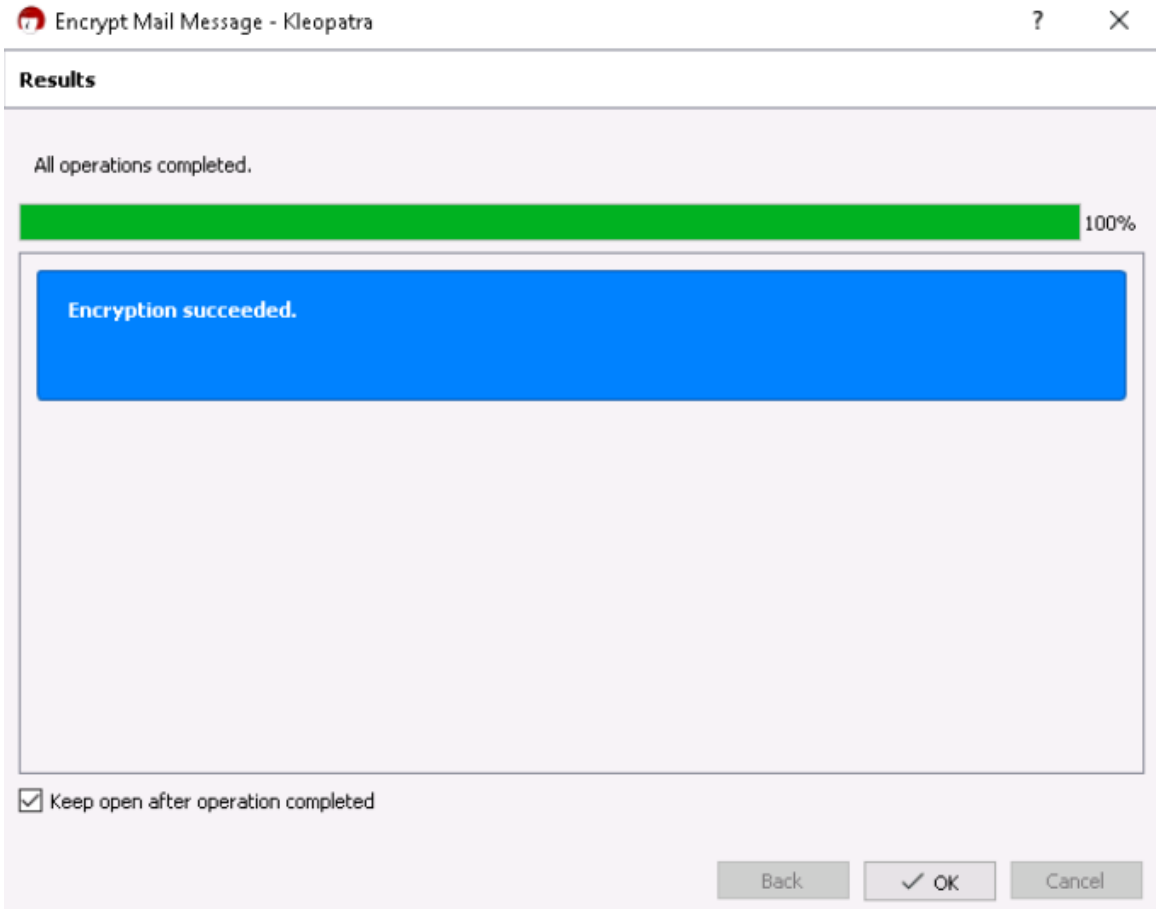
Select all the text, right click and then copy it to the clipboard.

Go back to the tools in Kleopatra, clipboard, and Encrypt.

It will ask you to choose a recipient, choose the key pair you generated and hit ok.



Go through the next button until it looks like the following.

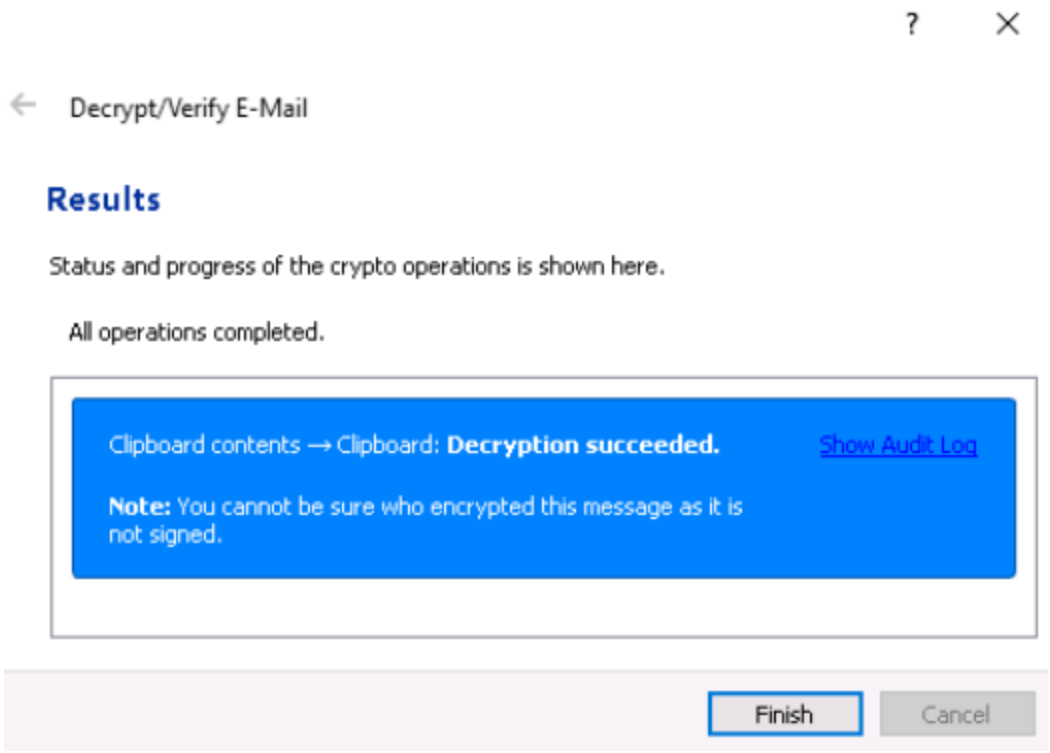


Now, open up a text editor and paste the contents. You should see a PGP encrypted message now like the following:

```
-----BEGIN PGP MESSAGE-----

hQEMA1DbLYC1lJ6IAQf/aKbpeI6QivNGb6GszCr7DchO/psEP4LSP21/QfPlVROK
yRo2b0J05osyE3Up7fRHjmovQUtDkQJJfoRfrffr9pNP6+R95gsGxYktL7IAH1qT
yyKUBk8TZgCOKv4F1KUzHy5OAYTVLS4IM8Jlj4RqdY9h2zfEcDe/YJ45p4xEKT4J
I0VmAWKA73PuHO7Nn//4YlP4Emfsr8BumQjGo0kfnmmyYkQIl5AvG6KfCDljw84v
oDnDNZ+LZ//czTBkKRes26zITV2R4HtesR9LkAYxjKACunBFRaad1epMQ+S7kYhd
bHpwKaM4O06uZ/ULF3AaKyfOY4Ikvj6jvs51xmLn3NJRAbtQRjncw5jaJWKSoLa9
mAniB6wShumjAkt0sW2O0R//P8hBvakezMblnyfffyq+pbxLAZ1iz2LlsO1v5rzm
+9IVhaejGaQ03N/CbxsQOZZw
=E9Rw
-----END PGP MESSAGE-----
```

To decrypt this, select the entire message and copy it to clipboard. Go to tools and then the clipboard. Click on the decrypt/verify and the message should now be decrypted. It will be successful with the following message:



If you paste the message into a text editor, it should now be decrypted.