LAB ASSIGNMENT - 2

Name: Ashwin Balaji
Roll Number: 2020PMD4221
Course: M.Tech (Mobile Computing and Data Analytics)

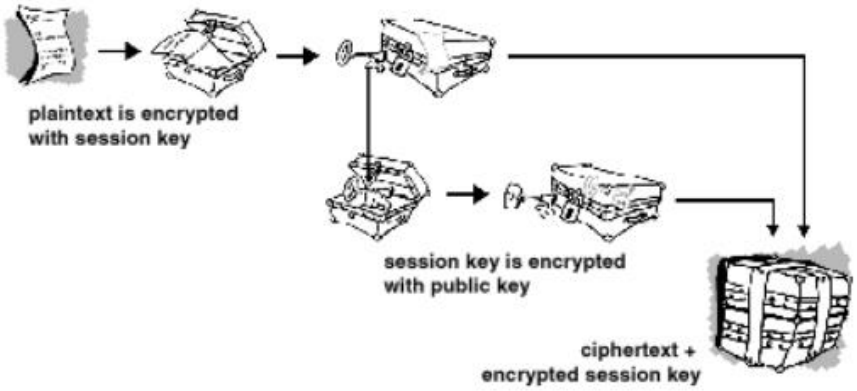
Title: Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures using tool GnuPG. (Download GPG4Win Tool). Create your public and private keys using Kleopatra Certificate management software. Check encryption –decryption of an email sent to you.

Software Requirements: Gpg4win 3.1.16 and Kleopatra 3.1.16

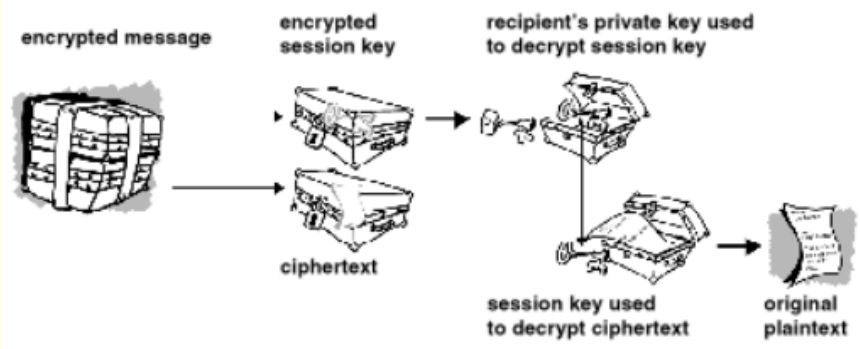
Theory:

PGP combines some of the best features of both conventional and public key cryptography. PGP is a hybrid cryptosystem. When a **user encrypts plaintext with PGP, PGP first compresses the plaintext**. Data compression saves modem transmission time and disk space and, more importantly, strengthens cryptographic security. Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher. Compression reduces these patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis. (Files that are too short to compress or which don't compress well aren't compressed.)

PGP then creates a session key, which is a **one-time-only secret key**. This key is a random number generated from the random movements of your mouse and the keystrokes you type. **This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is cipher text. Once the data is encrypted, the session key is then encrypted to the recipient's public key.** This public key-encrypted session key is transmitted along with the cipher text to the recipient.

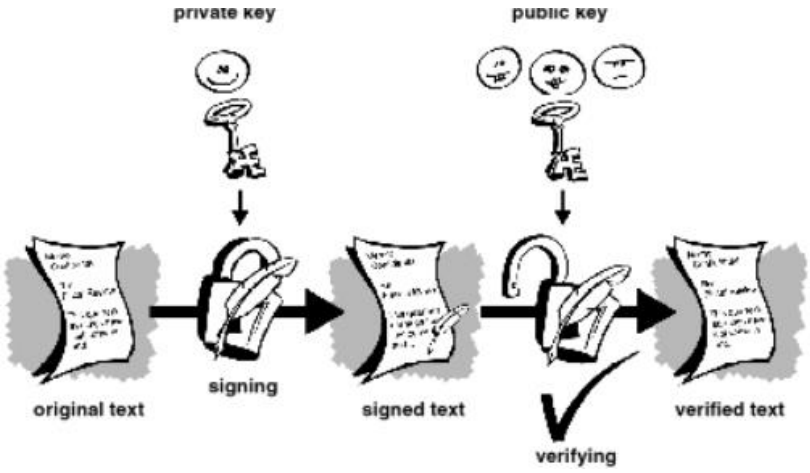


Decryption works in the reverse. The **recipient's copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the conventionally-encrypted ciphertext.**



The **combination of the two encryption methods combines the convenience of public key encryption with the speed of conventional encryption**. Conventional encryption is about 1, 000 times faster than public key encryption. Public key encryption in turn provides a solution to key distribution and data transmission issues. Used together, performance and key distribution are improved without any sacrifice in security.

PGP stores the keys in two files on your hard disk; one for public keys and one for private keys. **These files are called keyrings**. As you use PGP, you will typically add the public keys of your recipients to your public keyring. Your private keys are stored on your private keyring. If you lose your private keyring, you will be unable to decrypt any information encrypted to keys on that ring.



Digital certificates, or certs, simplify the task of establishing whether a public key truly belongs to the purported owner. A **certificate is a form of credential**. Examples might be your driver's license, your social security card, or your birth certificate. Each of these has some information on it identifying you and some authorization stating that someone else has confirmed your identity. Some certificates, such as your passport, are important enough confirmation of your identity that you would not want to lose them, lest someone use them to impersonate you. A digital certificate is data that functions much like a physical certificate. A **digital certificate is information included with a person's public key that helps others verify that a key is genuine or valid**. Digital certificates are used to thwart attempts to substitute one person's key for another.

A **digital certificate** consists of three things:

- A public key.
- Certificate information. ("Identity" information about the user, such as name, user ID, and so on.)
- One or more digital signatures.

The purpose of the digital signature on a certificate is to state that the certificate information has been attested to by some other person or entity. The digital signature does not attest to the authenticity of the certificate as a whole; it vouches only that the signed identity information goes along with, or is bound to, the public key.

PGP recognizes two different **certificate formats**:

- PGP certificates
- X.509 certificates

One unique aspect of the **PGP certificate format is that a single certificate can contain multiple signatures**. Several or many people may sign the key/ identification pair to attest to their own assurance that the public key definitely belongs to the specified owner. **Some PGP certificates consist of a public key with several labels, each of which contains a different means of identifying the key's owner (for example, the owner's name and corporate email account, the owner's nickname and home email account, a photograph of the owner — all in one certificate)**. The list of signatures of each of those identities may differ; signatures attest to the authenticity that one of the labels belongs to the public key, not that all the labels on the key are authentic. (Note that 'authentic' is in the eye of its beholder — signatures are opinions, and different people devote different levels of due diligence in checking authenticity before signing a key.)

Certificates are only useful while they are valid. It is unsafe to simply assume that a certificate is valid forever. In most organizations and in all PKIs, certificates have a restricted lifetime. This constrains the period in which a system is vulnerable should a certificate compromise occur. **Certificates are thus created with a scheduled validity period: a start date/time and an expiration date/ time.** The certificate is expected to be usable for its entire validity period (its lifetime). When the certificate expires, it will no longer be valid, as the authenticity of its key/ identification pair are no longer assured.

A **passphrase** is a longer version of a password, and in theory, a more secure one. Typically composed of multiple words, a passphrase is more secure against standard dictionary attacks, wherein the attacker tries all the words in the dictionary in an attempt to determine your password. The best passphrases are relatively long and complex and contain a combination of upper and lowercase letters, numeric and punctuation characters. PGP uses a passphrase to encrypt your private key on your machine. Your private key is encrypted on your disk using a hash of your passphrase as the secret key. You use the passphrase to decrypt and use your private key. A passphrase should be hard for you to forget and difficult for others to guess. It should be

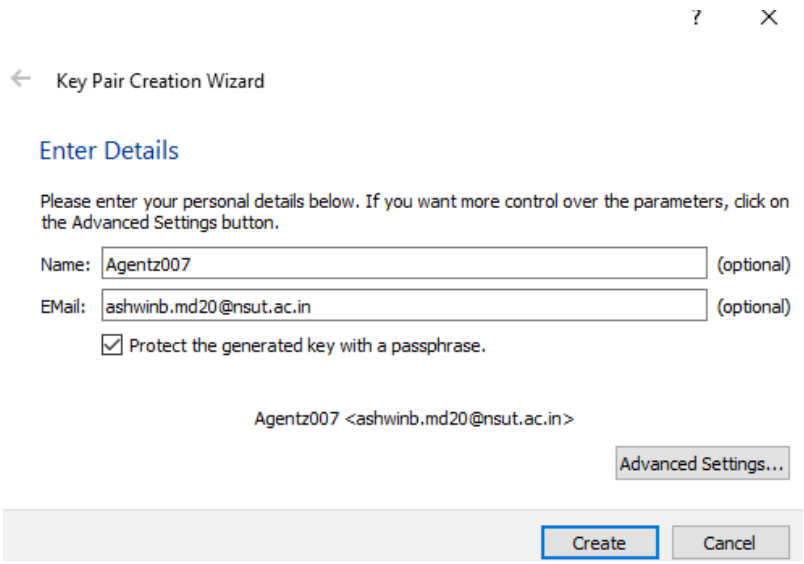
something already firmly embedded in your long-term memory, rather than something you make up from scratch.

Procedure:

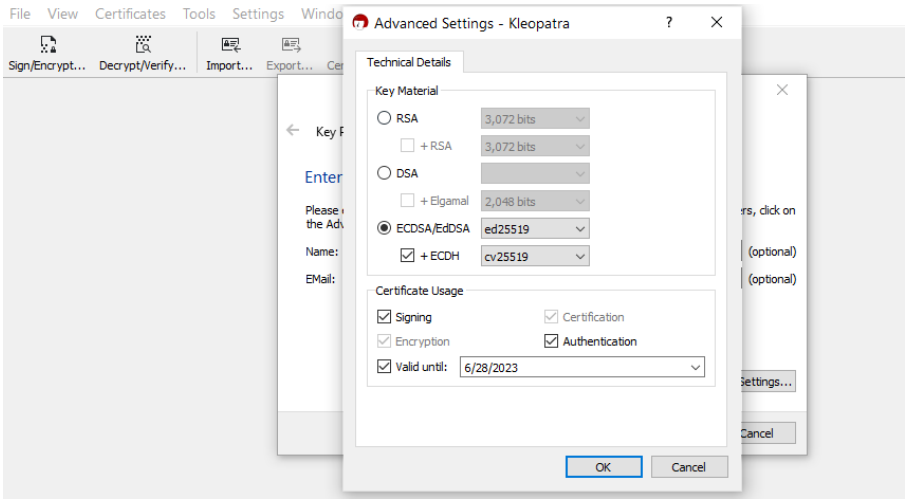
A) Create New PGP Key Pair in Kleopatra:

1. Click on New Key Pair

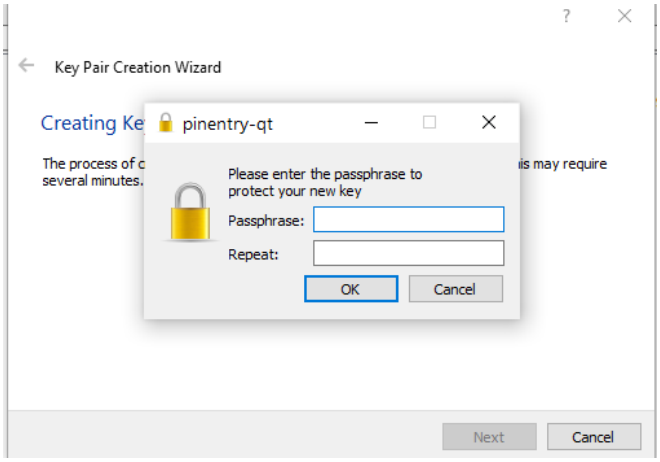
2. Add Username and Email (optional fields)



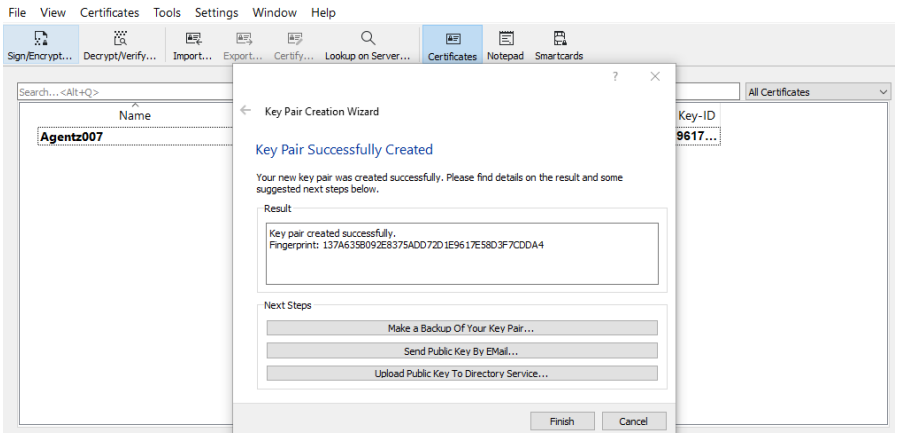
3. Click on **Advanced Settings** to incorporate digital signature algorithm and specify the various purpose of the like authentication, certification etc.
   Digital Signature: ECDSA (Elliptical Curve Digital Signature Algorithm)
4. Click **OK**



5. Click **Create**
6. You will be prompted to enter **Paraphrase** and Click **OK** button to generate Key Pair



7. Key Pair generated successfully

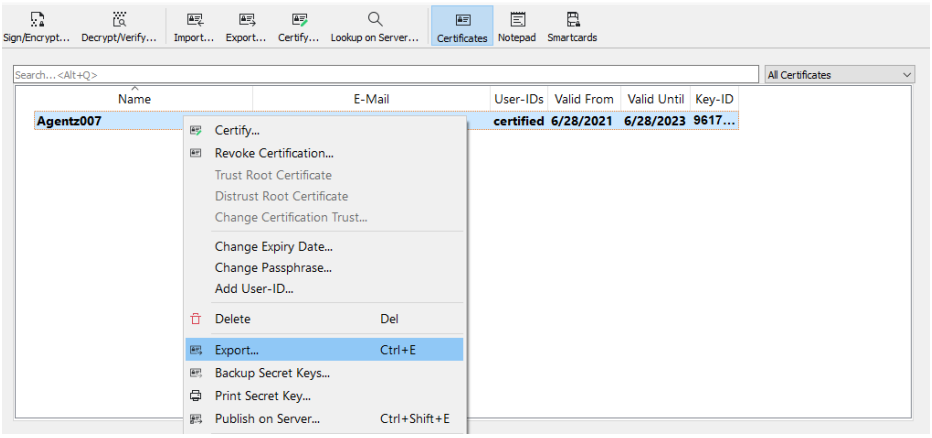


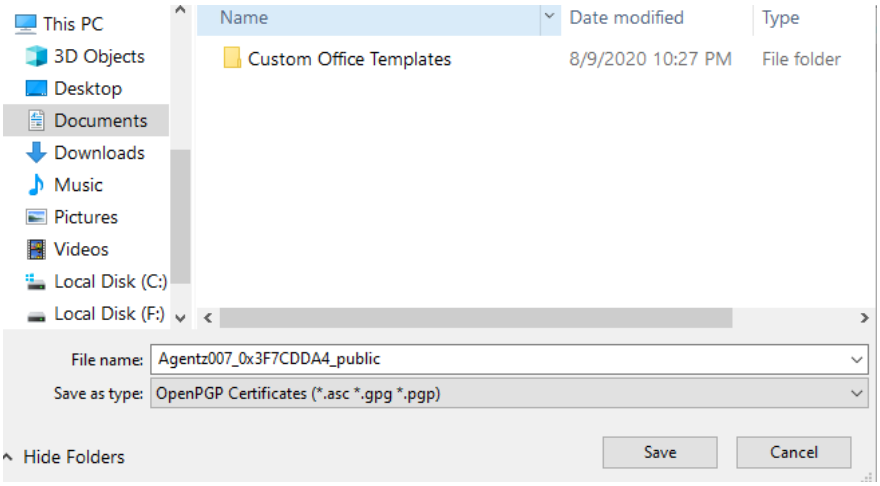
8. **OPENPGP certificate** contains **<Name, E-Mail, User-IDs, Valid From, Valid Until, Key-ID>**

Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Agentz007	**ashwinb.md20@nsut.ac.in**	**certified**	**6/28/2021**	**6/28/2023**	**9617...**

B) Secure storage of the Key-Value Pair.

1. Key-Value Pair can be stored/backed-up in the safe storage like cloud or can be saved basically at a high security storage system.
2. Currently for hands-on purpose, the Key-Value Pair is stored/exported to the desktop.
3. Browse to the location and save the public-key and secret/private-key (extensions *.gpg, *.pgp, *.asc)
4. Prompted to enter **Passphrase** (during private-key export)

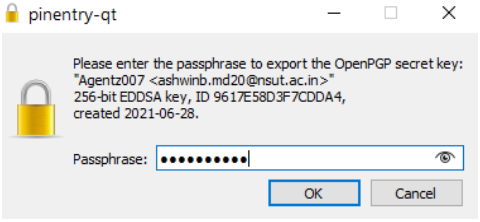





```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEYNnalRYJKwYBBAHaRw8BAQdApQlkuWlH9qaB0iF/43DlZKctTzQeYliBYB8+
enB9qhy0I0FnZW50ejAwNyA8YXNod2luYi5tZDIwQG5zdXQuYWMuaW4+iJYEExYI
AD4WIQQTemNbCS6Dda3XLR6WF+WNP3zdpAUCYNnalQIbIwUJA8H40wULCQgHAgYV
CgkICwIEFgIDAQIeAQIXgAAKCRCWF+WNP3zdpAsfAP0SatcFzZOSCKaDytI8rcr9
WGtuy4i+Mjrds6SnDwnAlgEAovezfJNiRuOaWAOYbqpiDUMe83h9T7eeMEro2kHm
bQi4OARg2dqVEgorBgEEAZdVAQUBAQdAbzYsqH4gA2bohMblwdjLscxqNGJixuHW
D60x/2EHNUwDAQgHiH4EGBYIACYWIQQTemNbCS6Dda3XLR6WF+WNP3zdpAUCYNna
```

```
lQIbDAUJA8H40wAKCRCWF+WNP3zdpJJeAP9DjJSoEqSzprnx/R2yQK14Kj0FVCFc
ZdxFWRDddITtPwEAyF2opJtUl1REx6AB0XHe2gkqNi7P0QF1OcViybZKFAQ=
=kUBa
-----END PGP PUBLIC KEY BLOCK-----
```



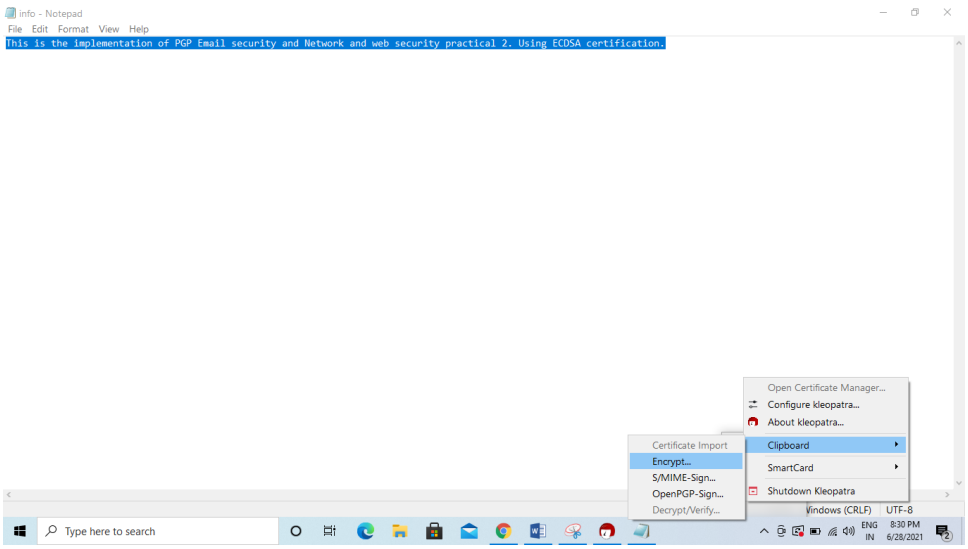

```
-----BEGIN PGP PRIVATE KEY BLOCK-----

lIYEYNnalRYJKwYBBAHaRw8BAQdApQlkuWlH9qaB0iF/43DlZKctTzQeYliBYB8+
enB9qhz+BwMC3Di834IvXES1DpCqko22m8g+pl+j2E67zJj6IB/FFlD2Xhha8noA
daYNWkzAI0Xc5Kodc3WFA4lIovH+eAWtzaLkv14Wk9810eKUfu7x17QjQWdlbnR6
MDA3IDxhc2h3aW5iLm1kMjBAbnN1dC5hYy5pbj6IlgQTFggAPhYhBBN6Y1sJLoN1
rdctHpYX5Y0/fN2kBQJg2dqVAhsjBQkDwfjTBQsJCAcCBhUKCQgLAgQWAgMBAh4B
AheAAAoJEJYX5Y0/fN2kCx8A/RJq1wXNk5IIpoPG0jytyv1Ya27LiL4yOt2zpKcP
CcCWAQCi97N8k2JG45pYA5huqmINQx7zeH1Pt54wSujaQeZtCJyLBGDZ2pUSCisG
AQQBl1UBBQE990BvNiyofiADZuiExuXB2MuxzGo0YmLG4dYPrTH/YQc1TAMBCAf+
BwMCeSs8PZT4QBm1xYEFIDo++-qCwrF4yjRHnRHRyeCXWsygK3DQkzNbBsNln9EZ
xXcSUvEDW3NoKxuM+cTlJP5QQ2n2/r9Zd0WA8sbSpfAx1Ih+BBgWCXAmFiEEE3pj
Wwkug3Wt1y0elhfljT983aQFAmDZ2pUCGwwFCQPB+NMACgkQlhfljT983aSSXgD/
Q4yUqBKks6a58f0dskCteCo9BVQhXGXcRVkQ3XSE7T8BAMhdqKSbVJdURMegAdFx
3toJKjYuz9EBdZnFYsm2ShQE
=LI0+
-----END PGP PRIVATE KEY BLOCK-----
```

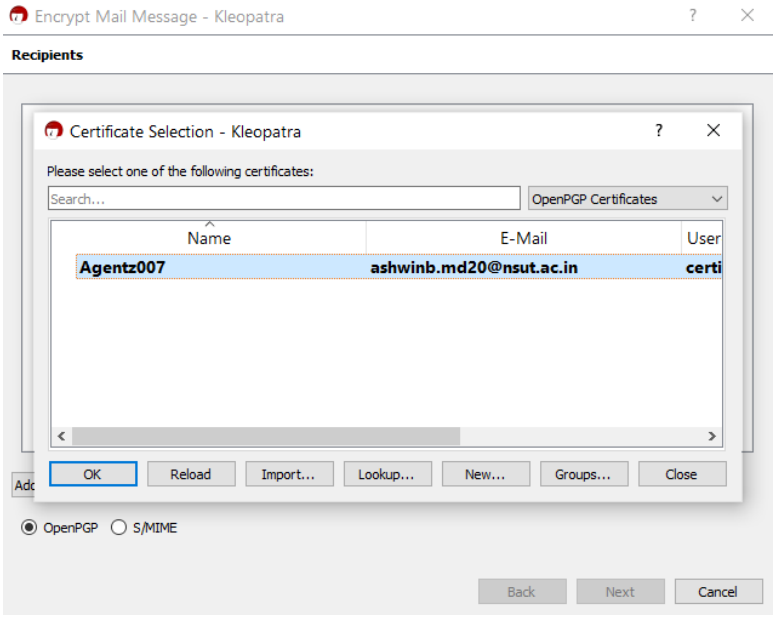
C) Providing security to the user information by performing PGP encryption and decryption:

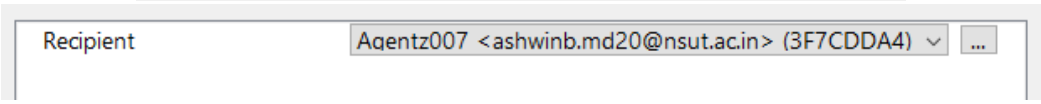
1. Save .txt (or any file like .docx, wordpad etc.) containing user information which is to be protected

2. Copy the text and right click on Kleopatra taskbar icon (hidden panel).
3. Click on **ClipBoard -> Encrypt**

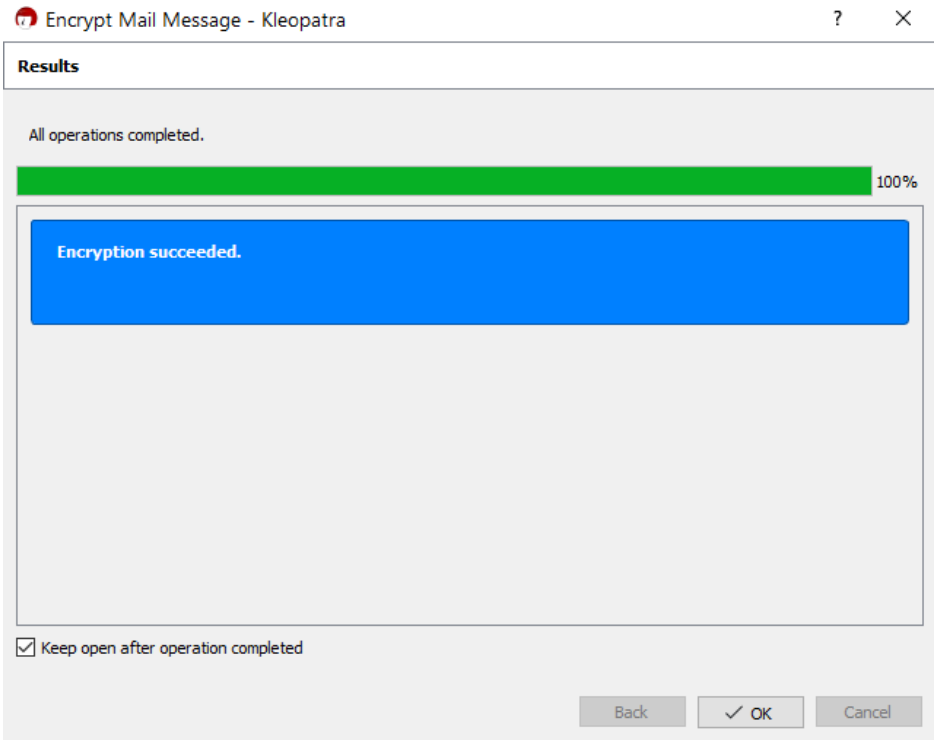


4. Add Recipient (i.e., Public key you want to send to the Bob for secure transmission)
5. Here, **OPENPGP certification** is used





6. Click **OK -> Next**

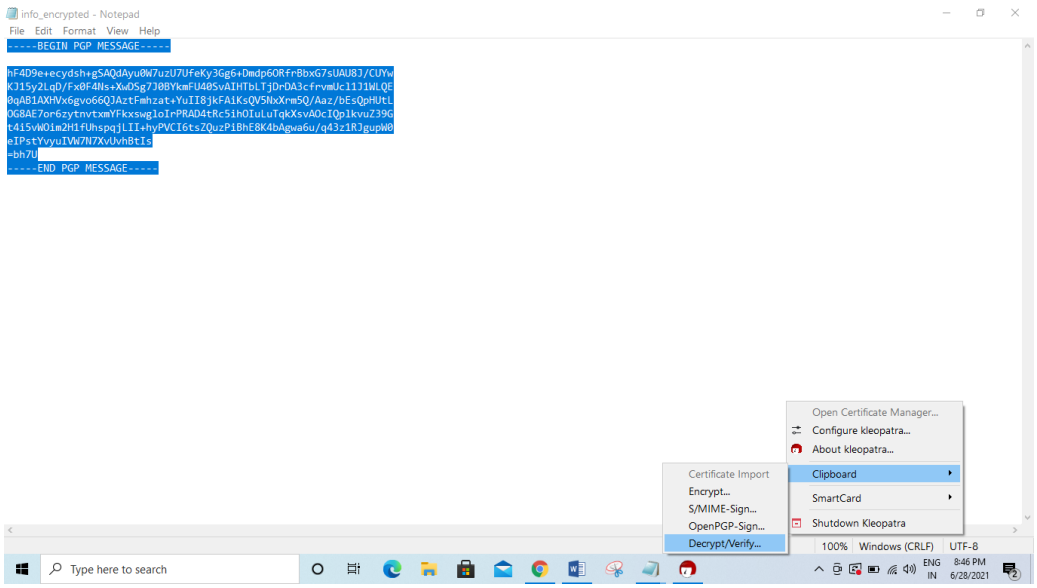


7. Open same/another text file and Press Ctrl + V. The encrypted message gets pasted.

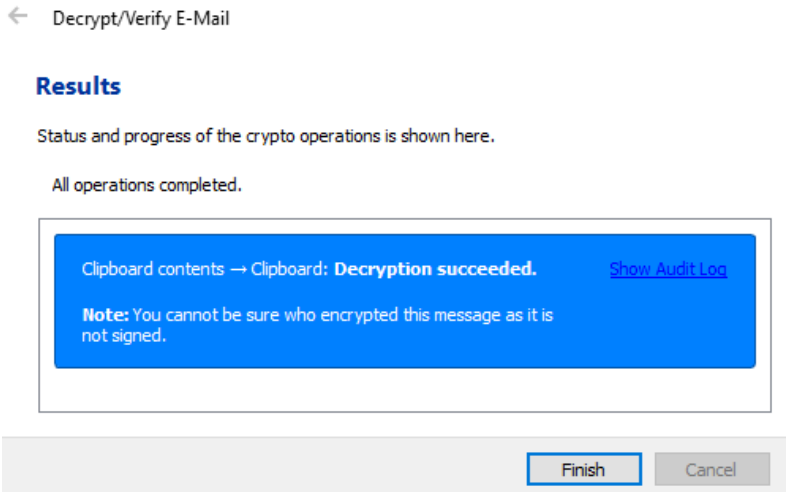
```
-----BEGIN PGP MESSAGE-----

hF4D9e+ecydsh+gSAQdAyu0W7uzU7UfeKy3Gg6+Dmdp6ORfrBbxG7sUAU8J/CUYw
KJ15y2LqD/Fx0F4Ns+XwDSg7J0BYkmFU40SvAIHTbLTjDrDA3cfrvmUcl1J1WLQE
0qAB1AXHVx6gvo66QJAztFmhzat+YuII8jkFAiKsQV5NxXrm5Q/Aaz/bEsQpHUtL
OG8AE7or6zytnvtxmYFkxswgloIrPRAD4tRc5ihOIuLuTqkXsvAOcIQplkvuZ39G
t4i5vWOim2H1fUhspqjLII+hyPVCI6tsZQuzPiBhE8K4bAgwa6u/q43z1RJgupW0
eIPstYvyuIVW7N7XvUvhBtIs
=bh7U
-----END PGP MESSAGE-----
```

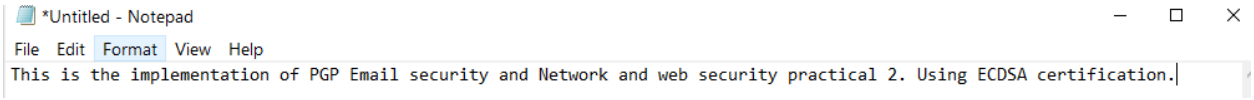
8. User information protected successfully
9. This encrypted data will be sent to the user with whom we want to communicate (Bob).
10. Assume that the Bob received the encrypted text along with the public-key sent by Alice
11. Now Bob may use Kleopatra software to decrypt the text
12. Copy the text and right click on Kleopatra taskbar icon (hidden panel).
13. Click on **ClipBoard -> Decrypt/Verify**



14. Enter **Passphrase** (required to decrypt the message)



15. Open a new text file and press Ctrl + V to identify the message sent by Alice.



16. Message decrypted successfully