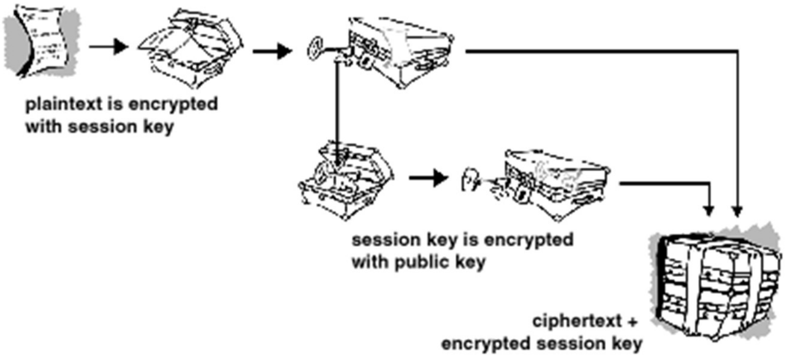
Sno:10	**Experiment name:** Examine how PGP works.	**Date:**

Aim: Examine how PGP works.

Description:

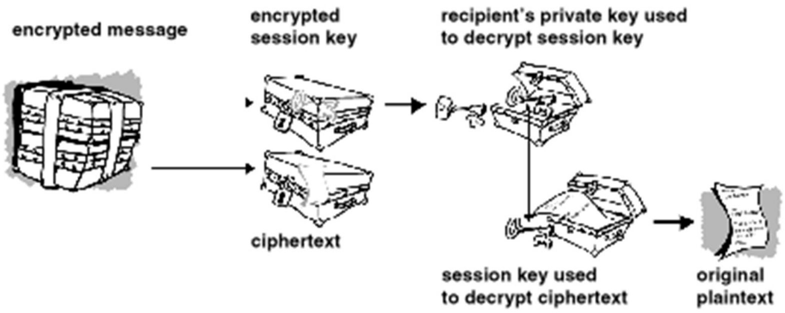
PGP combines some of the best features of both conventional and public key cryptography. PGP is a hybrid cryptosystem. When a user encrypts plaintext with PGP, first compresses the plaintext. Data compression saves modem transmission time and disk space and, more importantly, strengthens cryptographic security.

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 ciphertext. 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 ciphertext to the recipient.



How PGP encryption works

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.

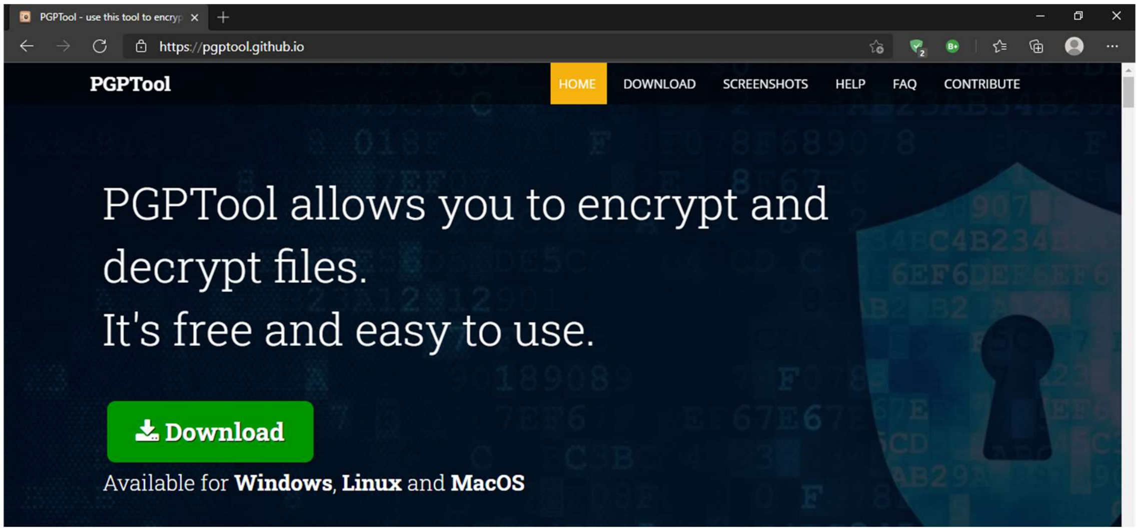

encrypted message
encrypted session key
recipient's private key used to decrypt session key
ciphertext
session key used to decrypt ciphertext
original plaintext

How PGP decryption works

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.

Steps to examine the PGP tool:

- Before installing the PGP tool, your computer must have JAVA installed in it.
- First download the **tool-pgptool.github.io**

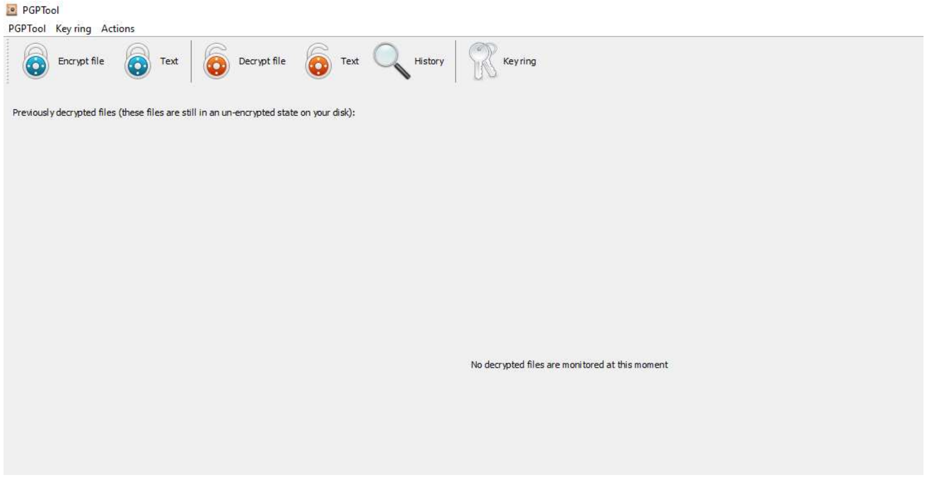


PGPTool allows you to encrypt and decrypt files.
It's free and easy to use.

Available for **Windows**, **Linux** and **MacOS**

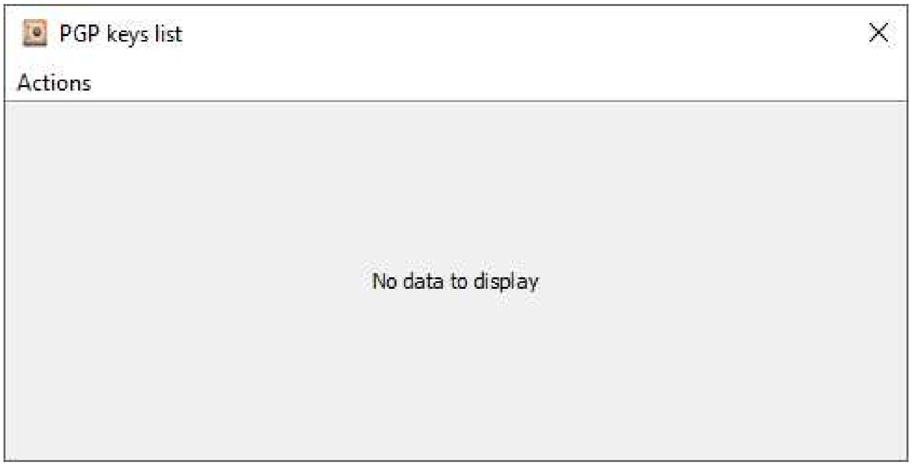
- Click on download icon to install PGP tool. After downloading, run the **.exe** file to use it.

- Finally, open the PGP tool and it looks like figure below.

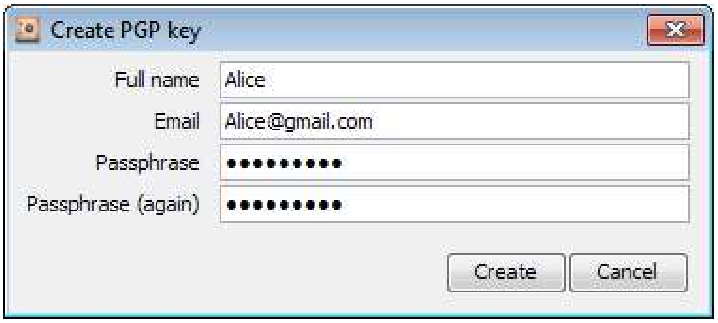


Previously decrypted files (these files are still in an un-encrypted state on your disk):

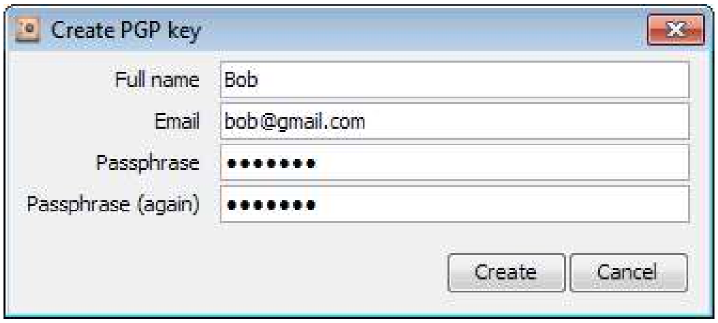
No decrypted files are monitored at this moment



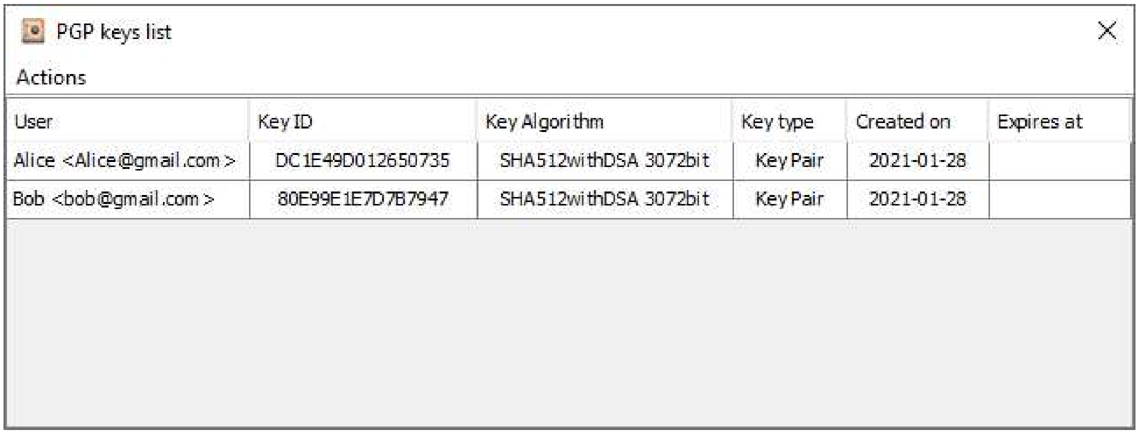
No data to display



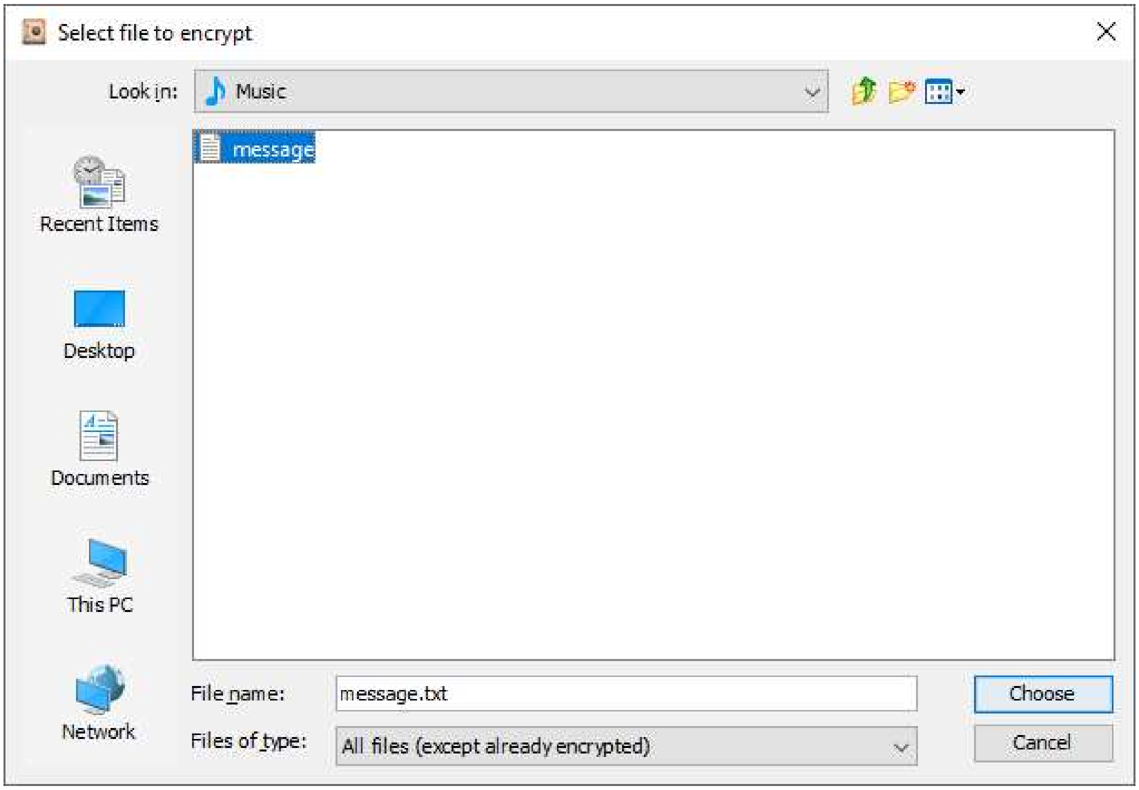
Full name: Alice
Email: Alice@gmail.com
Passphrase: ●●●●●●●●●
Passphrase (again): ●●●●●●●●●



Full name: Bob
Email: bob@gmail.com
Passphrase: ●●●●●●●
Passphrase (again): ●●●●●●●



User	Key ID	Key Algorithm	Key type	Created on	Expires at
Alice <Alice@gmail.com >	DC1E49D012650735	SHA512withDSA 3072bit	Key Pair	2021-01-28	
Bob <bob@gmail.com >	80E99E1E7D7B7947	SHA512withDSA 3072bit	Key Pair	2021-01-28	

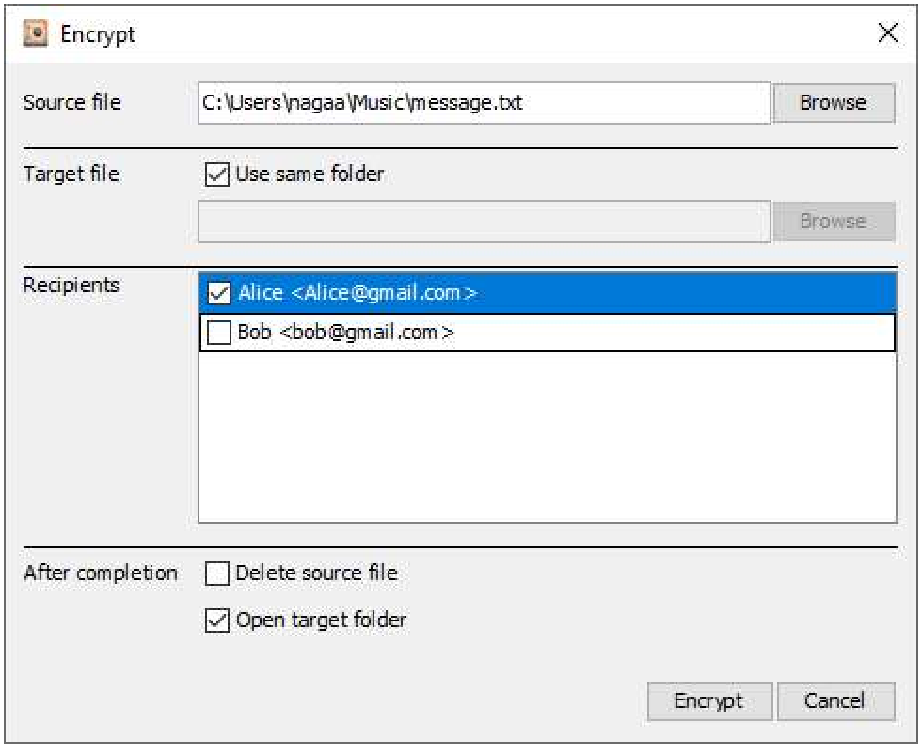


Look in: Music

message

File name: message.txt

Files of type: All files (except already encrypted)



Encrypt

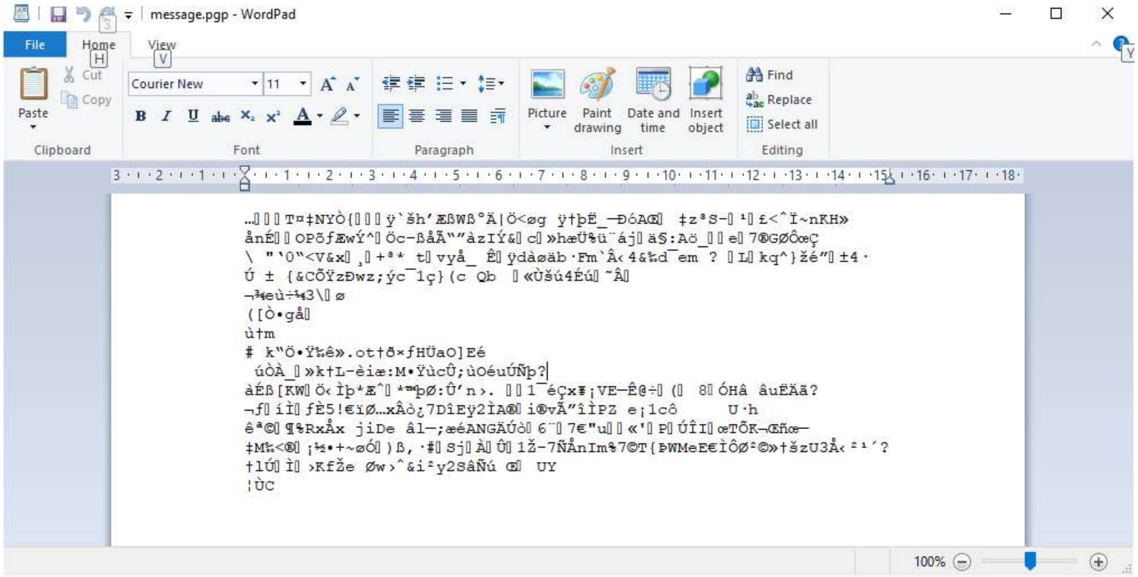
Source file: C:\Users\nagaa\Music\message.txt

Target file: ☑ Use same folder

Recipients:
- ☑ Alice <Alice@gmail.com>
- □ Bob <bob@gmail.com>

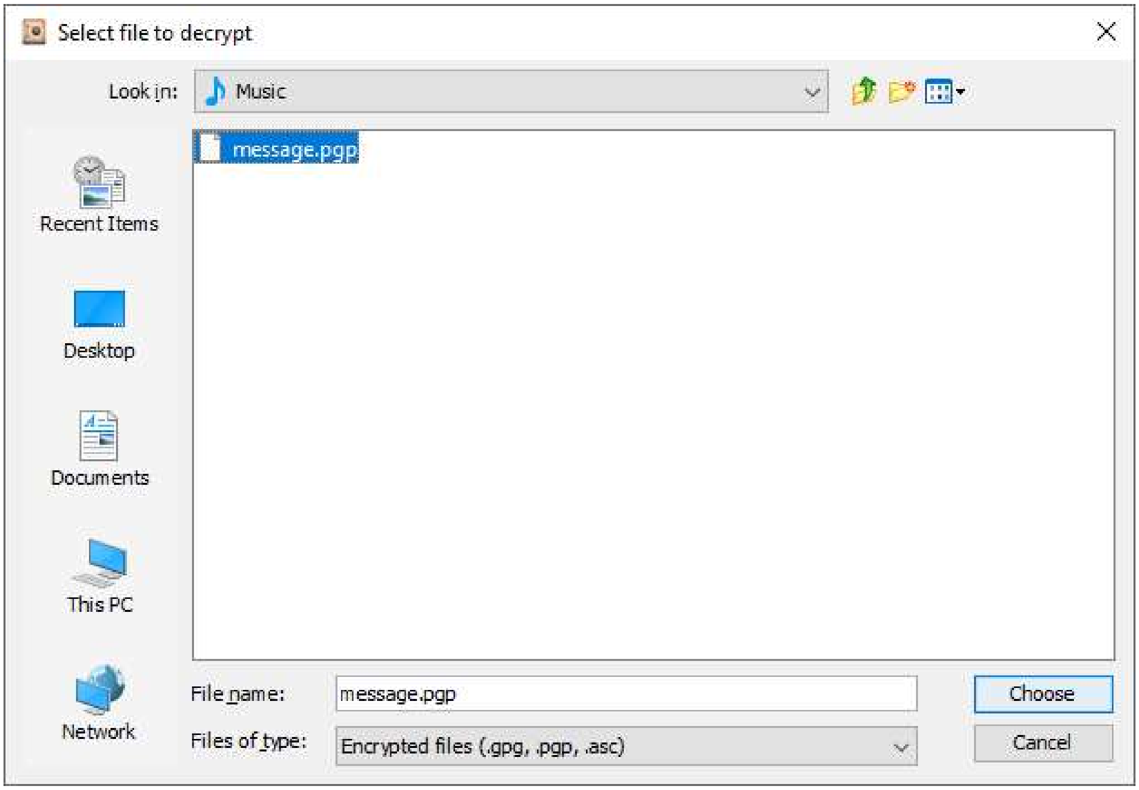
After completion:
- □ Delete source file
- ☑ Open target folder

After Performing Encryption



message.pgp - WordPad

```
…▯▯▯T¤‡NYÒ{▯▯▯ÿ`šh’ÆßWß°Ä|Ö<øg ÿ†þË_—ÐóAŒ▯ ‡z³S–▯ ¹▯£<ˆÏ~nKH»
ånÉ▯▯OPõƒÆwÝ^▯Öc–ßåÃ“”àzIÝ&▯c▯»hæÜ‰ü¨áj▯ä§:Aö_▯▯e▯7®GØÔœÇ
\ "‘0“<V&x▯¸▯+³* t▯vyå_ Ê▯ÿdàøäb·Fm`Â‹4&‰d¯em ? ▯L▯kq^}žé”▯±4·
Ú ± {&CÕŸzÐwz;ýc¯1ç}(c Qb  ▯«ÙšúÉú▯˜Â▯
¬¾eù÷¼3\▯ø
([Ò•gå▯
ù†m
# k“Ö•Ÿ‰ê».ot†ð×ƒHÜaO]Eé
 úÒÀ_▯»k†L-èiæ:M•ŸùcÛ;ùOéuÚÑþ?
àÉß[KW▯Ö‹Ìþ*Æˆ▯*™þØ:Û’n›. ▯▯1¯éÇx¥¡VE—Ê@÷▯(▯ 8▯ÓHâ âuËÄã?
¬ƒ▯íÌ▯ƒÈ5!€ïØ…xÂò¿7DîEÿ2ÌA®▯i®vÃ”îÌPZ e¡1cô      U·h
êª©▯¶‰RxÅx jiDe âl–;æéANGÄÚò▯6¨▯7€"u▯▯«'▯P▯ÚÎI▯œTÕK¬Œñœ—
‡M‰<®▯¡½•+~øÓ▯)ß,·#▯Sj▯À▯Û▯1Ž–7ÑÅnIm‰7©T{ÞWMeE€ÌÔØ²©»†šzU3Å‹²¹´?
†1Ú▯Ì▯›KfŽe Øw›ˆ&i²y2SâÑú Œ▯ UY
¦ÙC
```

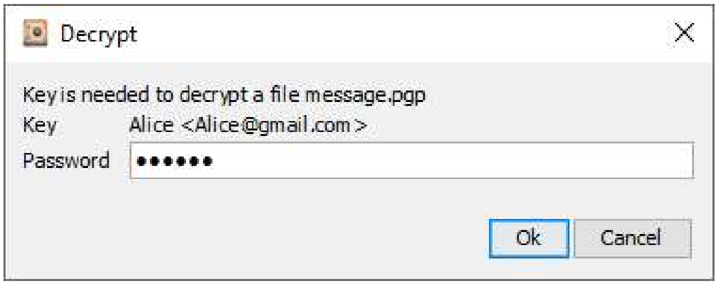


Look in: Music

message.pgp

File name: message.pgp

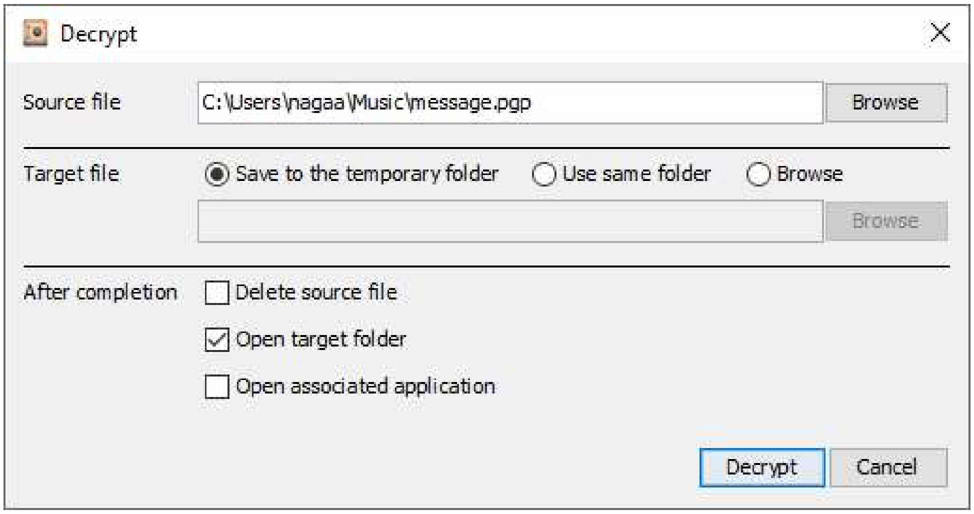
Files of type: Encrypted files (.gpg, .pgp, .asc)



Key is needed to decrypt a file message.pgp

Key Alice <Alice@gmail.com>

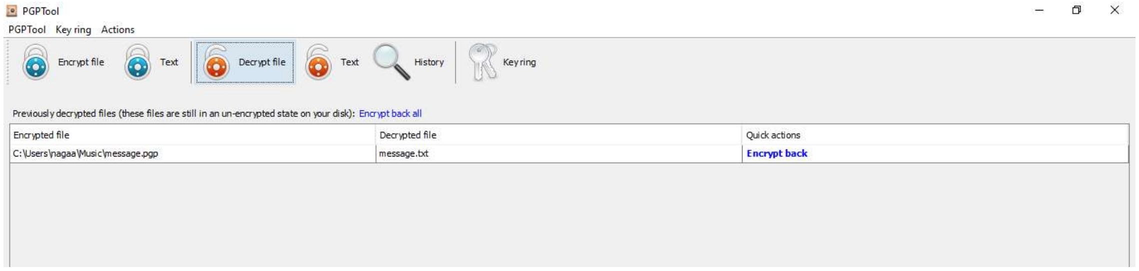
Password ••••••



Source file C:\Users\nagaa\Music\message.pgp

Target file ● Save to the temporary folder ○ Use same folder ○ Browse

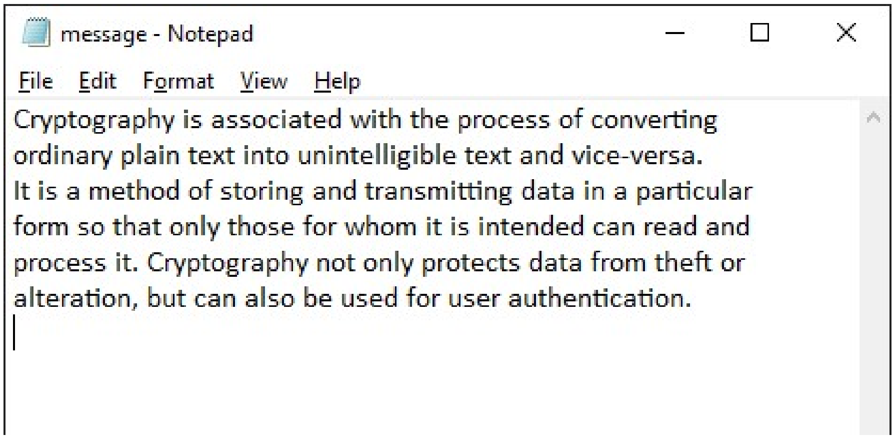
After completion
□ Delete source file
☑ Open target folder
□ Open associated application



Previously decrypted files (these files are still in an un-encrypted state on your disk): Encrypt back all

Encrypted file	Decrypted file	Quick actions
C:\Users\nagaa\Music\message.pgp	message.txt	**Encrypt back**

After Performing Decryption.



Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.
It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

<u>Result:</u> Successfully completed performing encryption and decryption using PGP tool.