# Exp 17. Encrypting and Decrypting the Files Using GnuPG in Linux

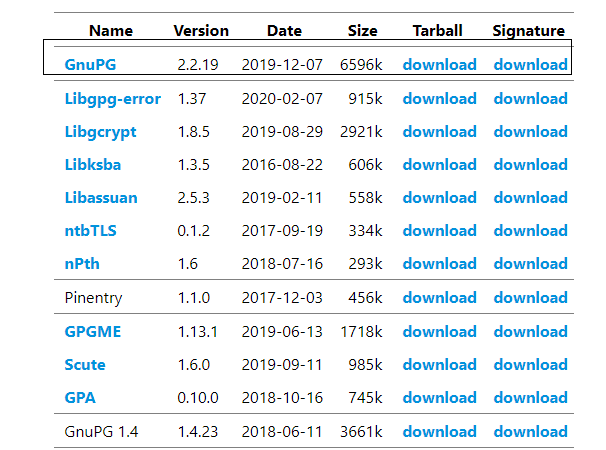
**Theory:** GnuPG is an encryption module that uses OpenPGP at its core. [PGP](https://en.wikipedia.org/wiki/Pretty_Good_Privacy) stands for Pretty Good Privacy. It is an encryption program that provides authentication and cryptographic privacy for data communication. In the age where ***data is the new oil***, the modern age thieves won’t intrude in through doors, windows or roofs, but instead, via wires and electrical signals in form of a few lines of code and commands. Nothing in this world is secure, which leads to an obvious conclusion that these thieves are inevitable.

But instead of trying to figure out which door these thieves will intrude through, we might just need to focus on what is it they need … *Data*. Data is the holy grail of wine which contains the ingredients of an individual’s social, financial, emotional, habitual and sometimes physical well-being. Encryption can serve as a solution to elude hackers, private organizations and government surveillance systems from monitoring your data. Encryption makes data useless to the person who does not possess a decryption key and useful to the one who does. If the key is lost, the data create remains locked forever.

Implementation:

### Using GnuPG through Linux Terminal

We are assuming that you have installed GnuPG already. If not, go to [**GnuPG**](https://gnupg.org/download/index.html) official website and download the required software and install it.



**Encryption Process:**

1. You can start the encryption process by generating a key.

gpg --gen-key

**2.** A name and an email address will later serve you like an easy way to remember your key rather than the long key-id. 



**3.** As soon as you choose okay a prompt for entering a passphrase will popup. This passphrase serves as a password for confirmation of the decryption key. It is a last line of defense for verification that the key belongs to you.

**4.** To see all the keys in your keyring, you can use the below command

$gpg --list-keys

**5.** Considering a file named *sample.txt* which is to be encrypted. For encrypting, use the below command

$gpg --output encryptionoutput.gpg --encrypt --recipient geek@geeksforgeeks.org sample.txt

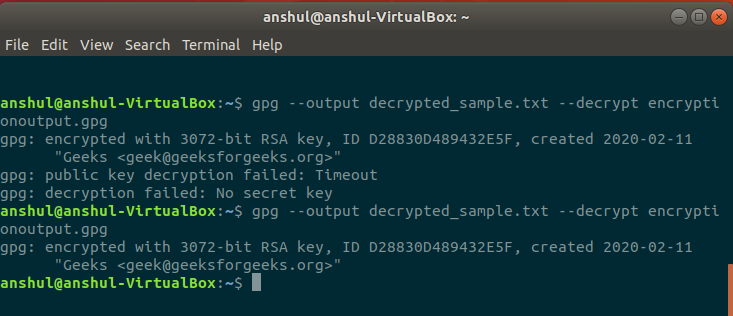
Here, *.gpg* is an extension used for encrypted files.

**Decryption Process:**

**1.** The encrypted file named *encryptionoutput.gpg* from the above given encryption process is to be sent to the recipient and in case you being the recipient, decryption is needed. Use the below command:

$gpg --output decrypted\_sample.txt --decrypt encryptionoutput.gpg

**2.** Now it will ask you to enter the passphrase to unlock the OpenPGP secret key.



Now, you can check the result using [ls](https://www.geeksforgeeks.org/practical-applications-ls-command-linux/) command. The decryption process will only work if the private key has been imported into the keyring. You can also confirm the decryption by reading the content of the original file and decrypted file.

