|  |
| --- |
| **Operating Systems Principles and Programming [18ECSC202]** |
| Open Challenge |
| **Report** |

|  |
| --- |
| **School of Computer Science and Engineering**  **2021-22** |

DEMONSTRATION OF PGP ENCRYPTION AND DECRYPTION ON LINUX

**Contents**

|  |  |
| --- | --- |
| **Si. No.** | **Topics** |
| 1. | Course and Team Details |
| 2. | Introduction |
| 3. | Problem Statement |
| 4. | Solution |
| 5. | References |

**1. Course and Team Details**

**1.1 Course details**

|  |  |
| --- | --- |
| **Course Name** | Operating Systems Principles and Programming |
| **Course Code** | 18ECSC202 |
| **Semester** | IV |
| **Division** | B |
| **Year** | 2021-22 |
| **Faculty In Charge** | Dr. Shrinivas D Desai |

**1.2 Team Details**

|  |  |  |  |
| --- | --- | --- | --- |
| **Si. No.** | **Roll No.** | **Name** | **USN** |
| 1. | 230 | Mayuri Kalmat | 01FE20BCS095 |
| 2. | 231 | Parag R Hegde | 01FE20BCS096 |
| 3. | 234 | Pranav B Jadhav | 01FE20BCS099 |
| 4. | 253 | Pranavi P Kulkarni | 01FE20BCS118 |

**2. Introduction**

**PGP** describes as **“PRETTY GOOD PRIVACY”**, is pretty much the standard in email security and encryption. PGP is an **encryption system** developed in 1991 initially as freeware (until its purchase by Symantec in 2010 when it became a licensed software) that fuses two encryption standards:

i. **Symmetric**

ii. **Asymmetric**.

It’s based on technology called **RSA public key encryption** whose name is derived from the initials of the developers of the encryption technology: **Rivest, Shamir, and Adelmen**.

**3. Problem Statement**

Demonstrate the functioning of PGP Key pair-based encryption and decryption on Linux.

**4. Solution**

1. PGP uses both a **public** and **private key** and can take the efficiency from the symmetric system and the security of the asymmetric system.
2. i. In **symmetric encryption**, only **one key** is used to encrypt and decrypt.

ii. **Asymmetric encryption**, on the other hand, uses **two keys** like stated above – private and public.

1. PGP supports:

i. **UNIX/Linux**

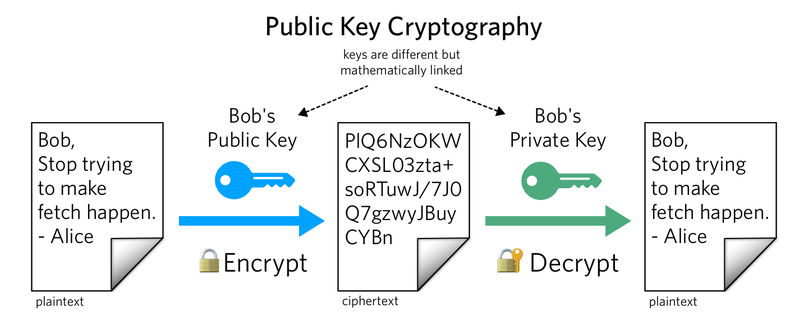
ii. **Windows**

iii. **DOS**

iv. **Macintosh**.

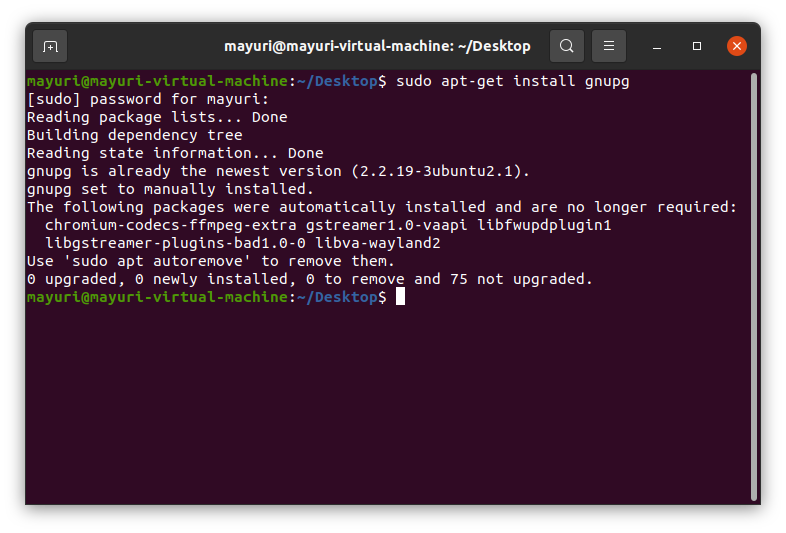
In UNIX/Linux systems PGP can be executed either using the **command line interface** or the **graphical interface (GUI)**.

1. There are wide range of PGP distribution.viz, web sites and subsequent versions. Most of PGP versions are located at this web site <http://www.pgpi.org>
2. The **primary use** of PGP is to **encrypt computer files** and **data communication**(email and network connection). Ex: **PGP VPN** gateway is used for establishing secure connection to remote network systems.
3. According to **PGP International Organization**, PGP uses a public-key encryption system. PGP includes the best features of **public key cryptography (PKC)**. The Mathematical  Algorithms generate public/private keys for encrypting and decrypting computer files/data.

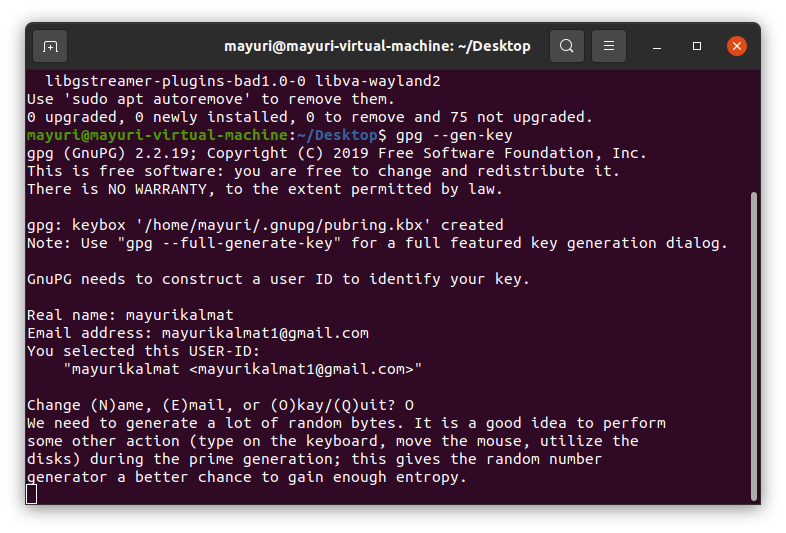


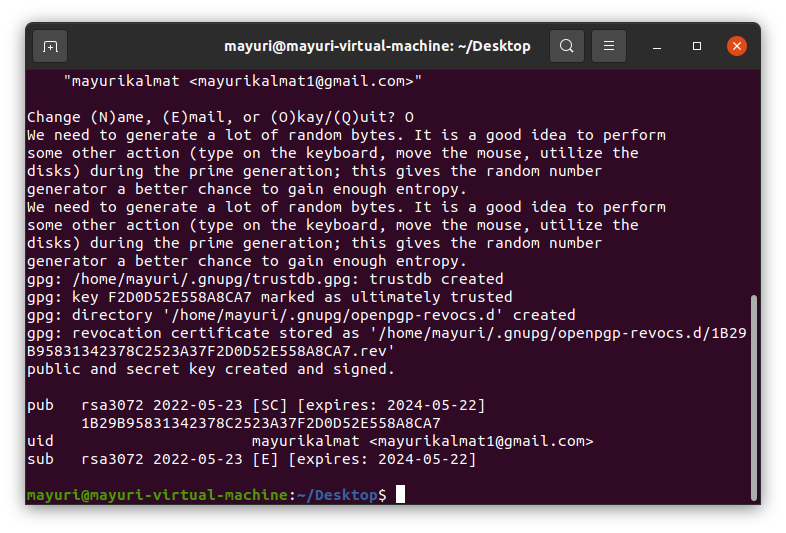
1. **User** makes a **copy of public key** available to other users such **friends or co- workers** to encrypt information intend to send to her or him. Therefore, recipient/owner/holder of the associated public key can decrypt information uses a corresponding private key.
2. **PGP** uses a file called a **key ring** “keys.asc” to store public/private keys which is resided usually in HDD. Therefore, because the key ring file is stored in local hard disk it is more susceptible to be compromised. Ex: although the key.asc file is stored in encryption form but someone with sufficient privileges i.e., system administrator would have access to user key ring file. Indeed, it is essential to make sure the key ring file is well secured.

Step 1: Installation of GPG

$ sudo apt-get install gnupg

Step 2 : Generation of key

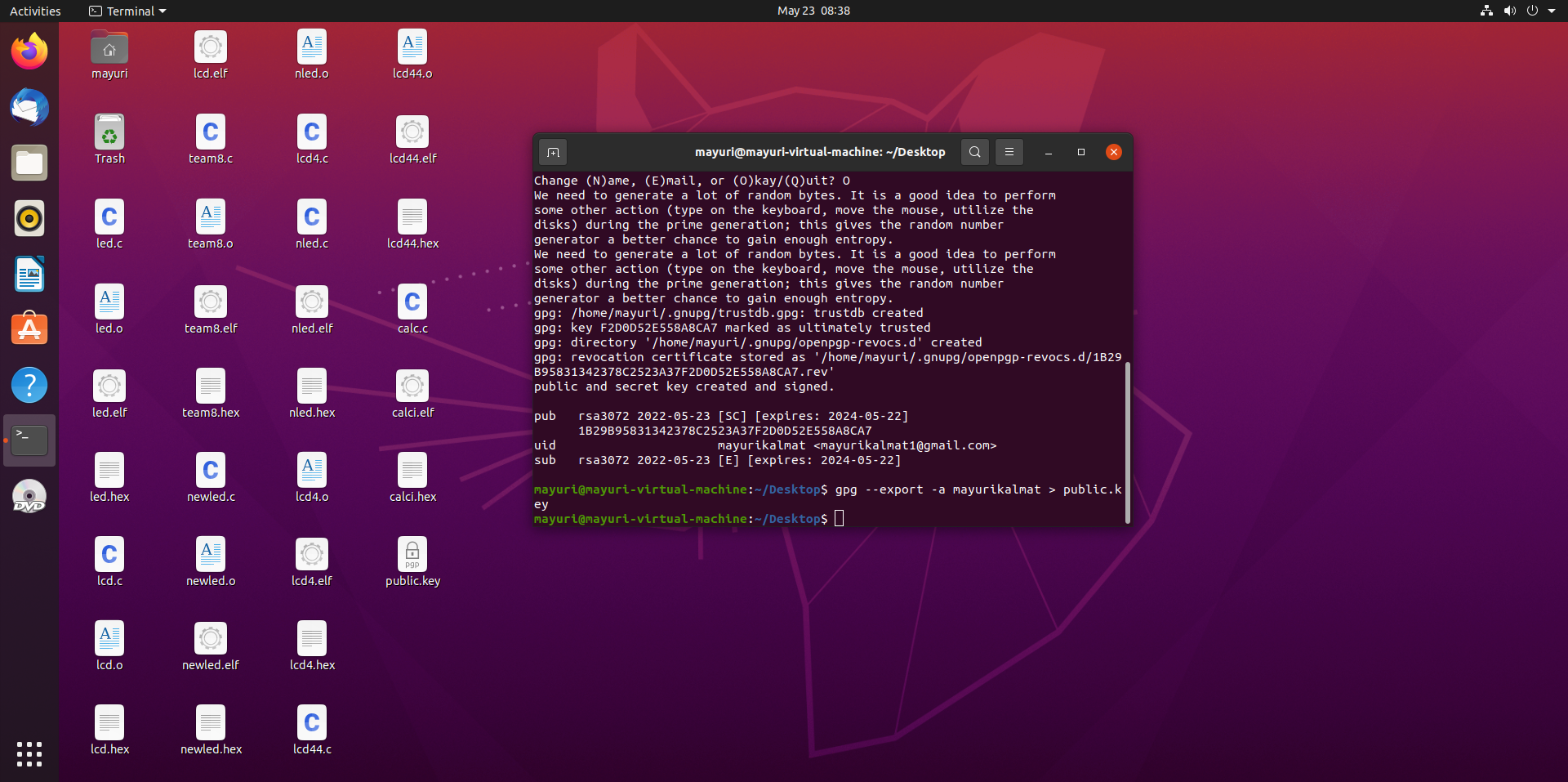
$ gpg --gen-key

Key has been generated.

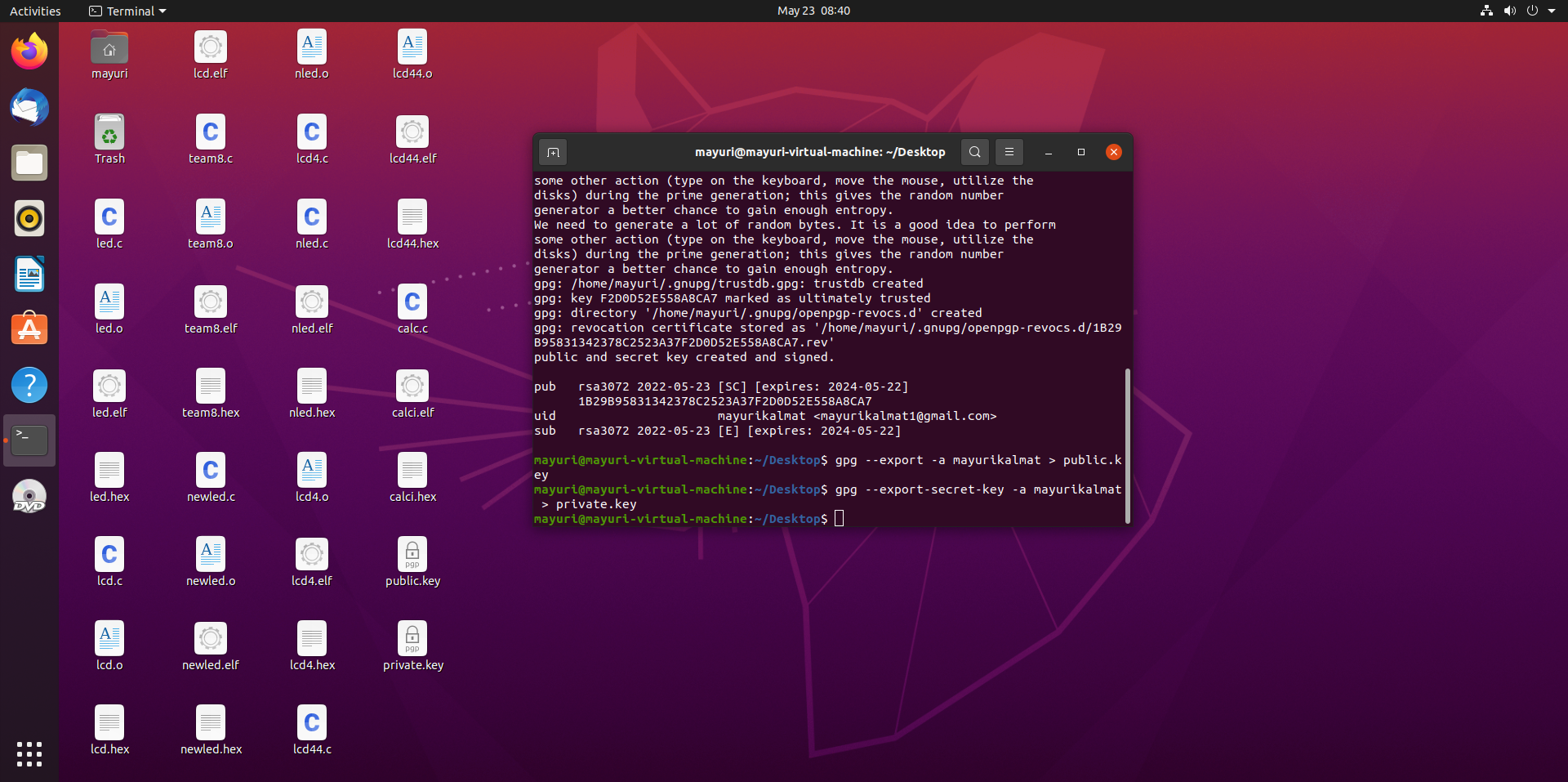
Step 3: Export the PUBLIC KEY

to export a public key into file public.key:

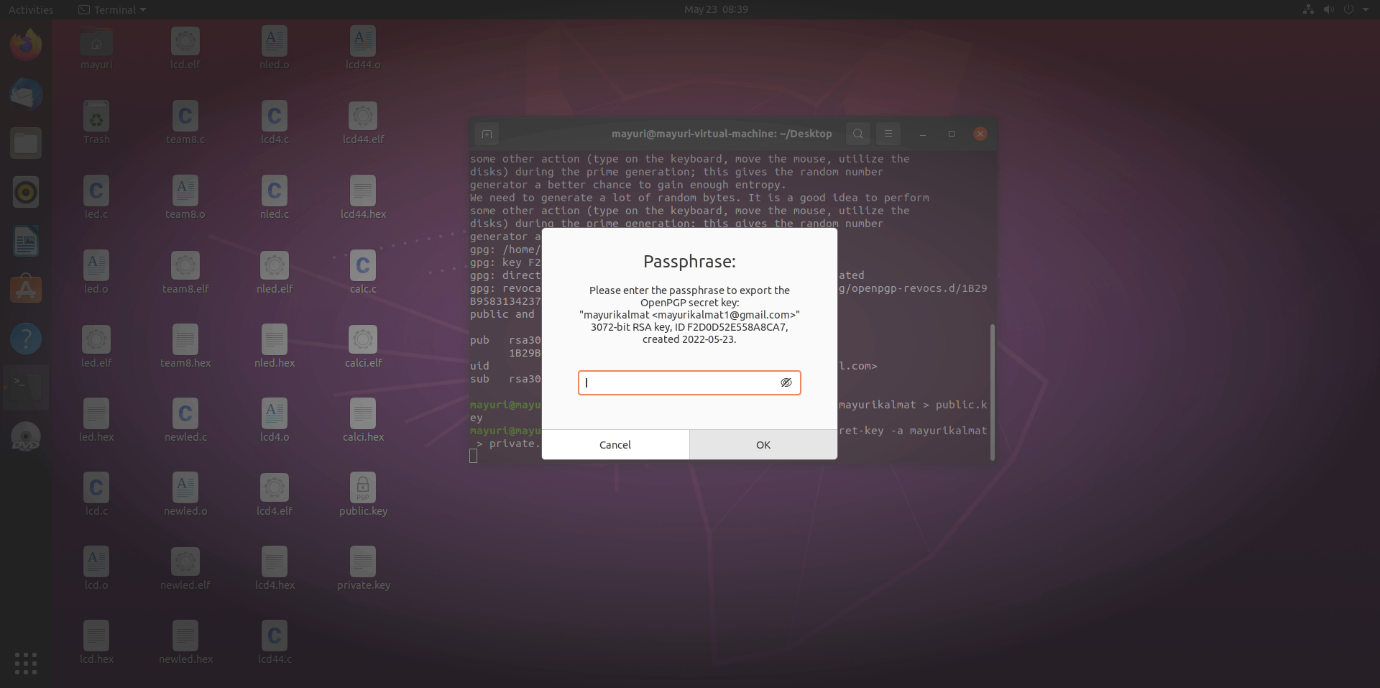
gpg --export -a “User name” > public key



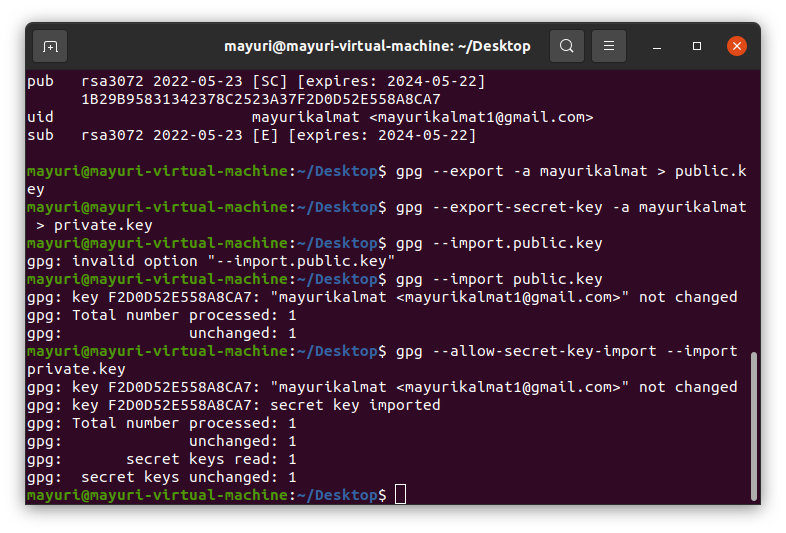
Step 4: Export the PRIVATE KEY

gpg --export-secret-key -a “UserName” > private.key

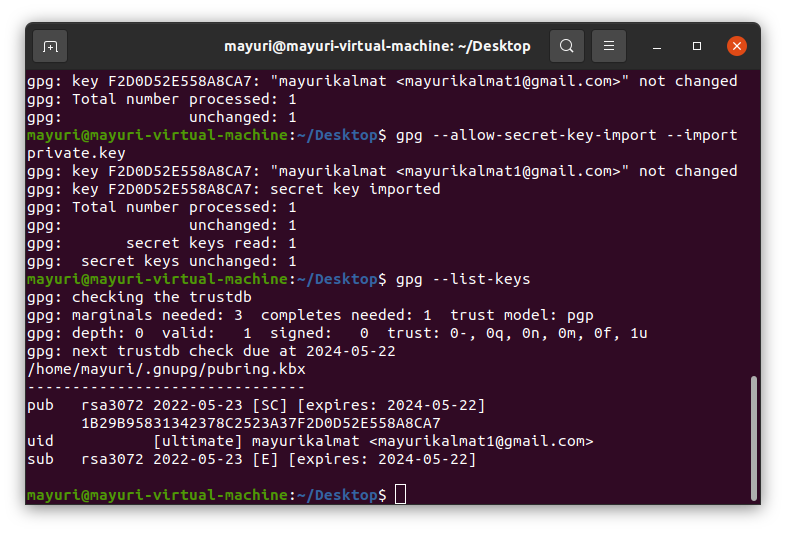
It asks you for a Passphrase.i.e, the password you entered during the installation.



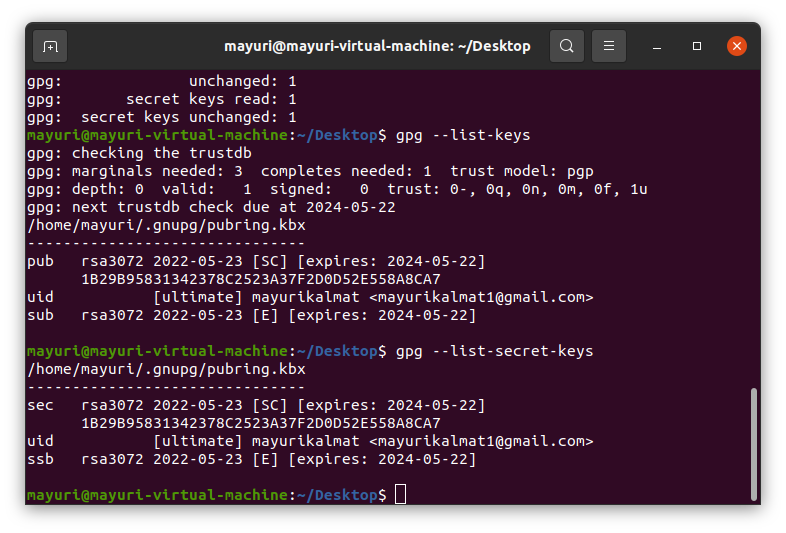
Step 5: Import a public key and Private Key:

gpg --import public.key and

gpg --allow-secret-key-import --import private.key

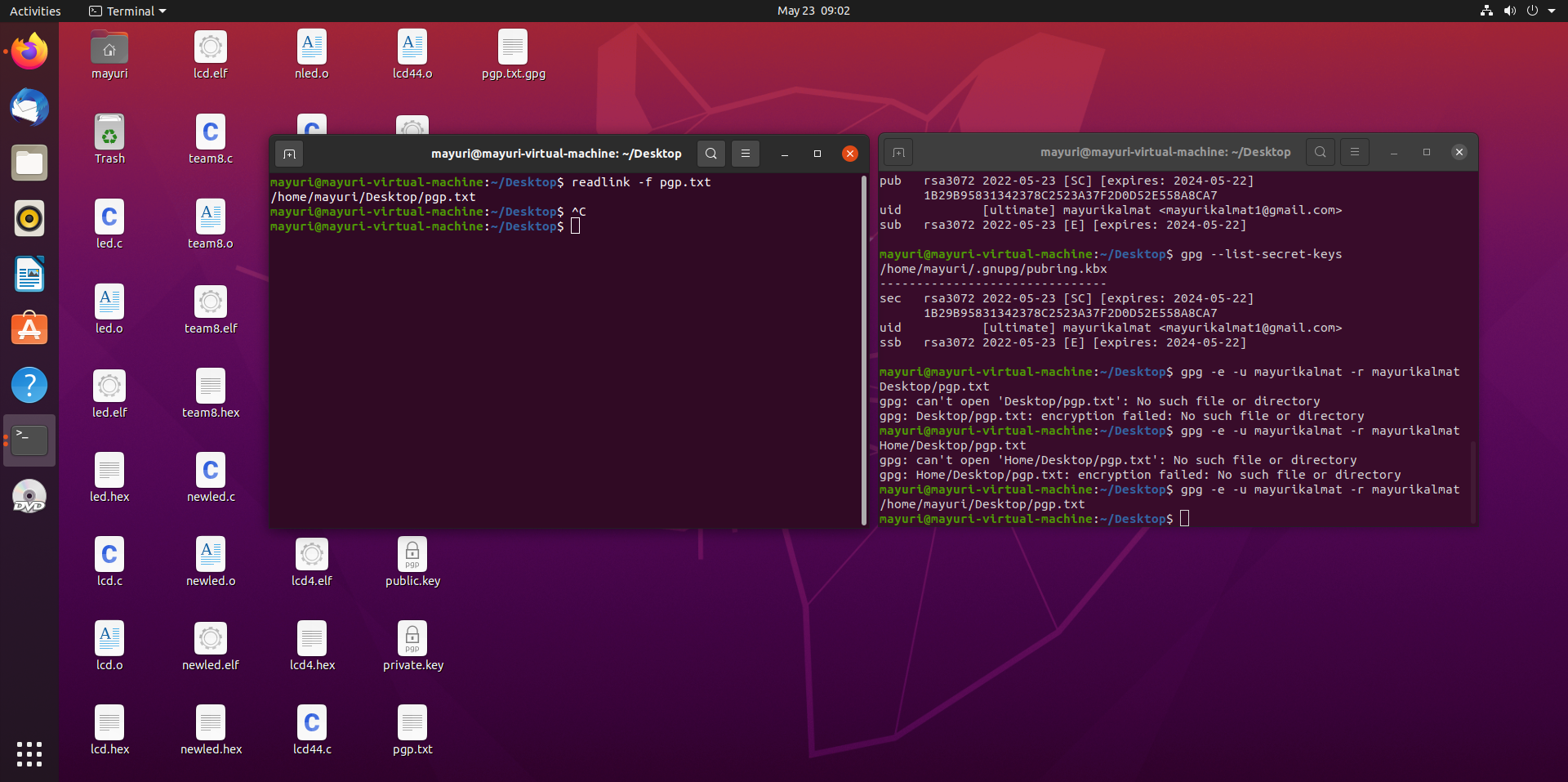
Step 6: List the keys in your public key ring:

gpg --list-keys

Step 7:  List the keys in your secret key

gpg --list-secret-keys

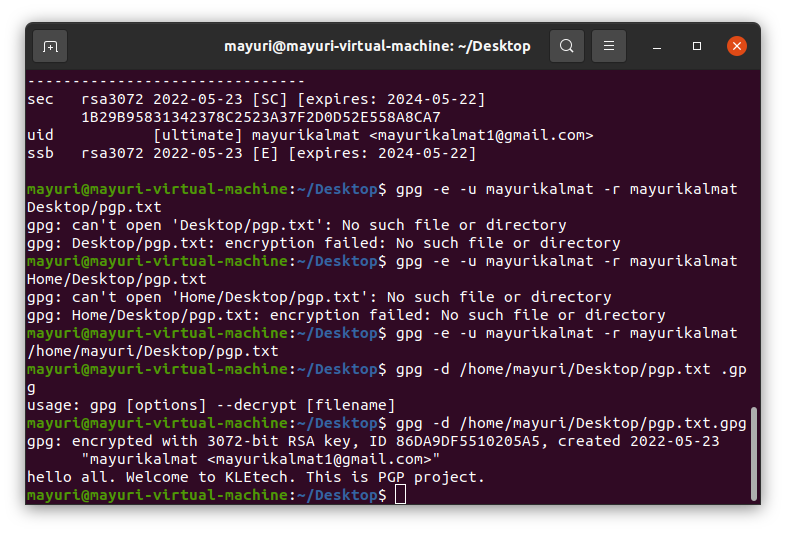
Step 8: To encrypt data:

****gpg -e -u “Sender User name” –r “Receiver User Name” somefile

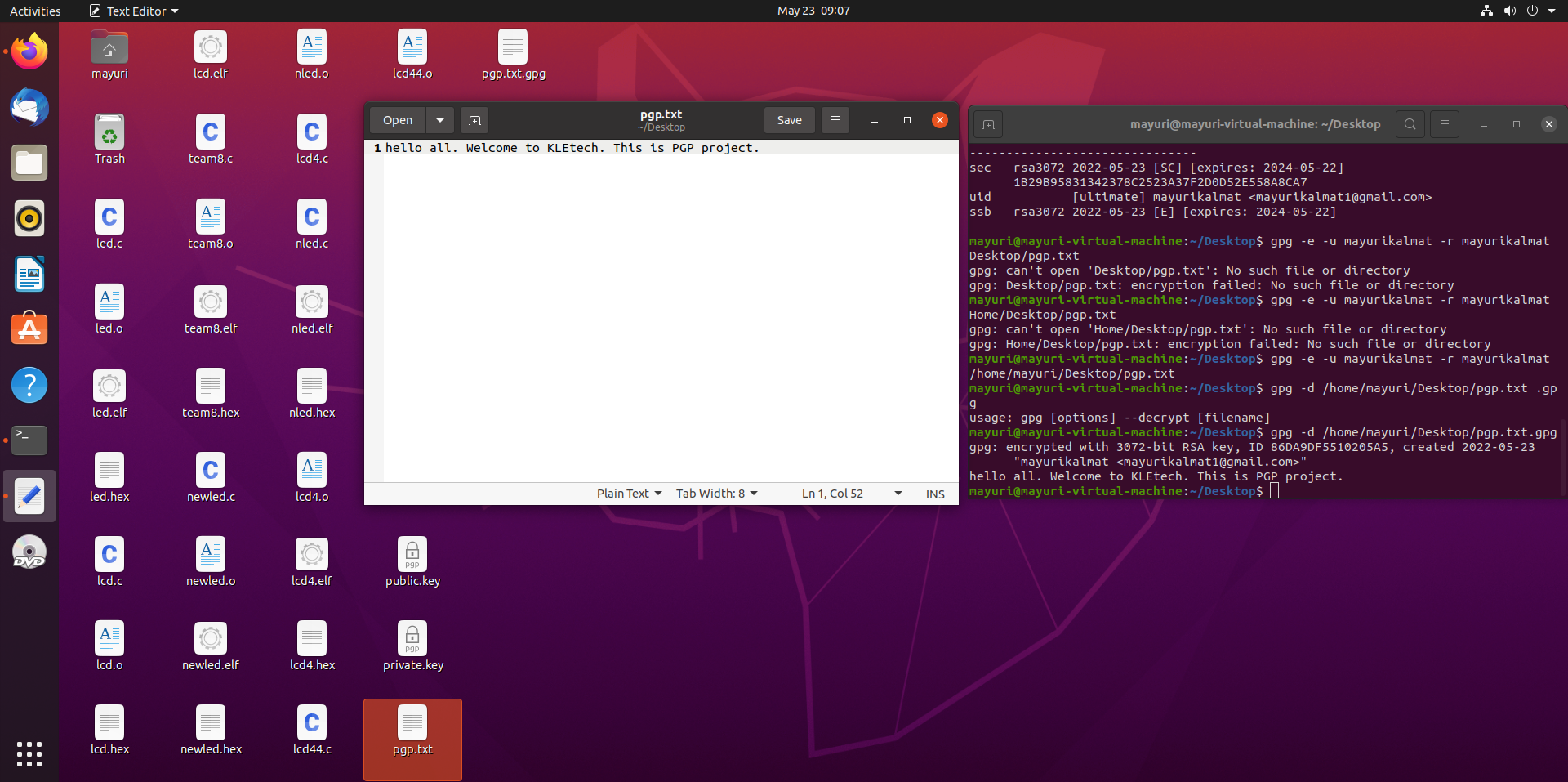
This is how the encrypted file looks like.



Step 9: To decrypt data:

****gpg -d mydata.tar.gpg

After decryption, the message present in file is displayed on the console.



**5. Experience:**

This course project exposed us to the world of open source.

As security and privacy are two of the key aspects of present world, it was interesting knowing about the encryption techniques that can be used on Linux.

The RSA based PGP encryption is one of the best and secure ways to encrypt as we have generated a ciphered data, using which it is impossible to figure out theactual data.

When the smaller prime numbers are used in RSA, there is a chance of compromise. But, when larger numbers are used, it cannot be cracked.

**6. References**

Lake, J. (2021, March 2021). *What is RSA encryption and how does it work?.*

Comparitech Limited.

<https://www.comparitech.com/blog/information-security/rsa-encryption/>

Dizak, M. (2020, December 23). *How to Use GnuPG for Encryption on Linux*. MakeUseOf.

<https://www.makeuseof.com/gnupg-encryption-on-linux/>

Robinson, K. (2018, September 21). *What is Public Key Cryptography?.* Twilio Inc.

<https://www.twilio.com/blog/what-is-public-key-cryptography>

**~\*~\*~\*~\*~\*~\*~\*~**