|  |  |
| --- | --- |
| **Name** | **Akshat Biniwale** |
| **UID** | **2021300014** |
| **Branch** | **BE COMPS A** |
| **Batch** | **VI** |
| **Subject** | **Cryptography and System Security** |
| **Experiment** | **7** |

About PGP:

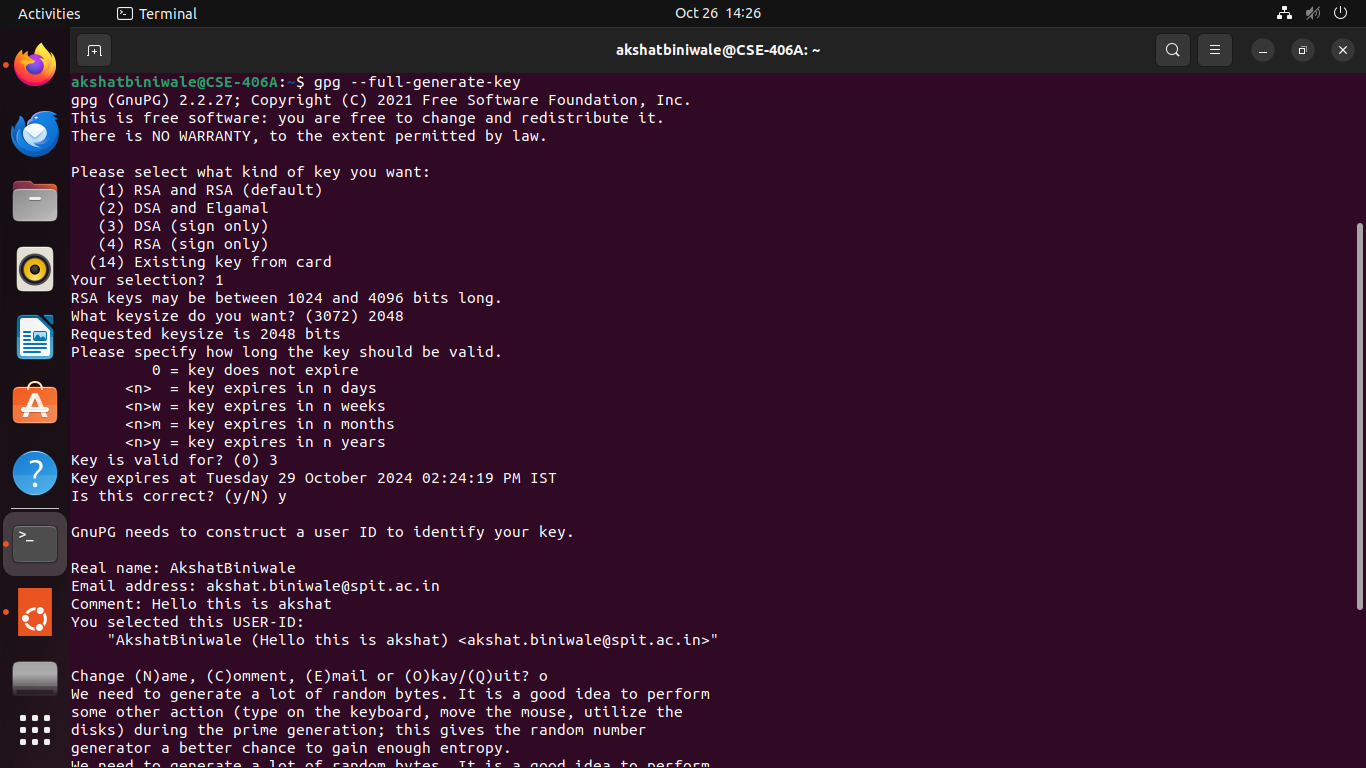
PGP (Pretty Good Privacy) is an encryption program designed to provide cryptographic privacy and authentication for data communication. It was created to secure sensitive information, ensuring confidentiality, integrity, and authentication in digital exchanges. PGP is widely used for securing emails, files, and digital signatures by encrypting data and verifying the identity of senders. Its primary purpose is to:

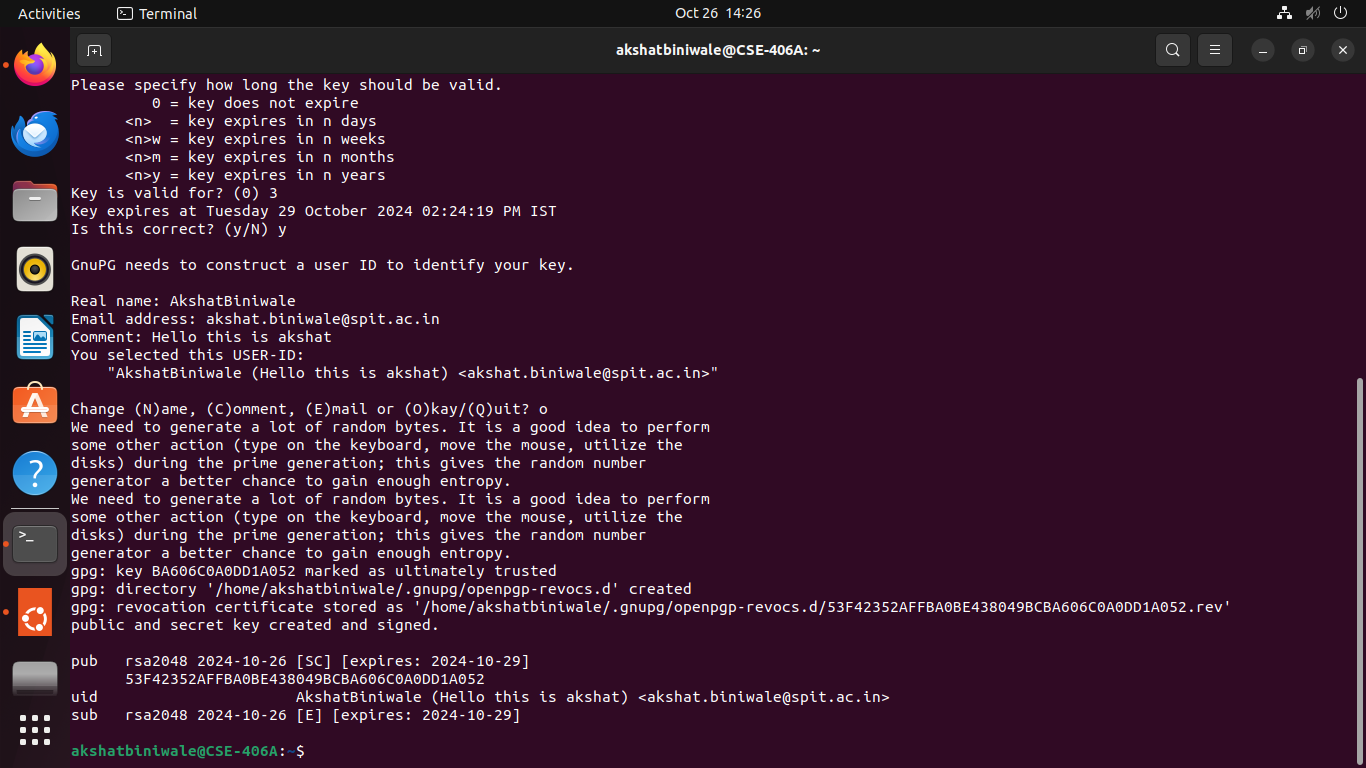
1. Confidentiality: Ensure only authorized recipients can read the encrypted content.
2. Integrity: Detect any alterations to the data during transmission.
3. Authentication: Verify the identity of the sender to prevent impersonation.
4. Non-repudiation: Prevent the sender from denying the transmission of data.

PGP achieves this through a combination of symmetric encryption for speed and public-key cryptography for secure key exchange, making it highly effective for secure communication across various platforms.

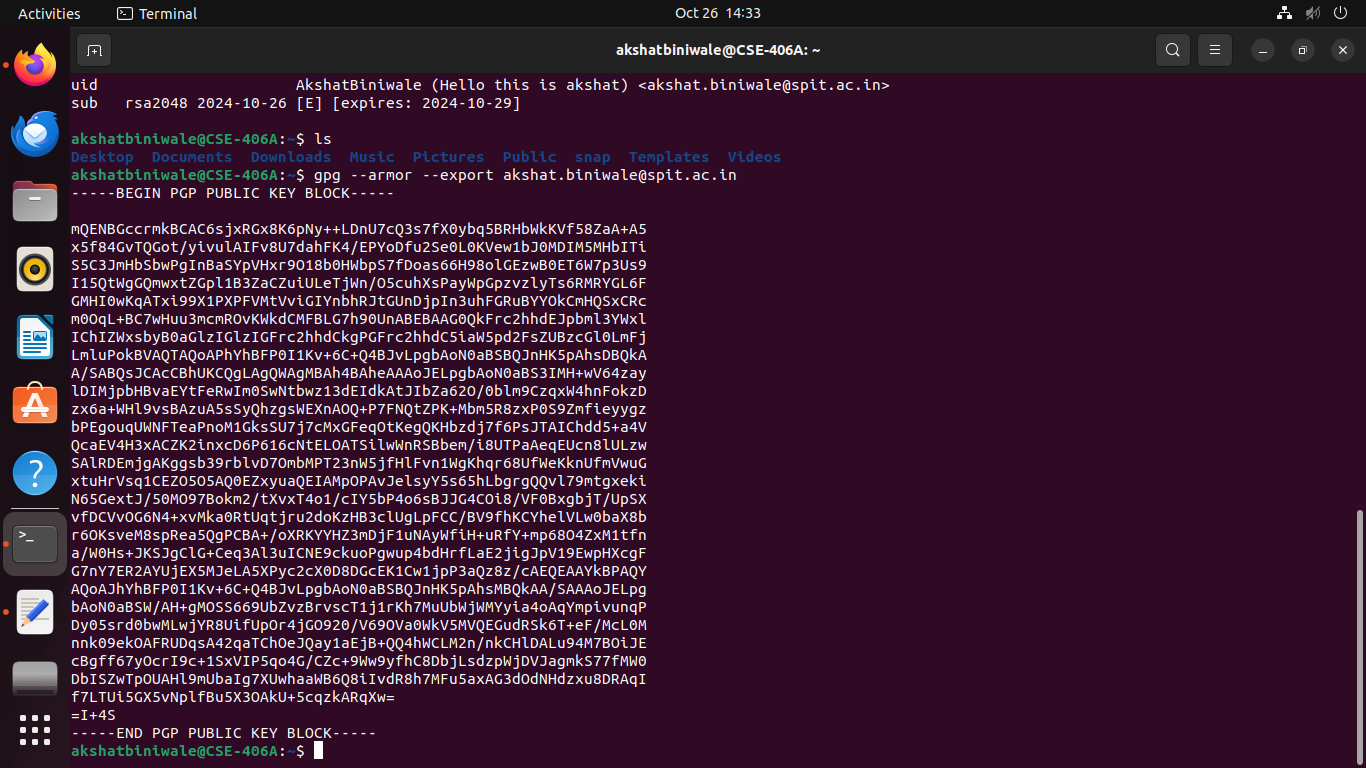
Procedure:

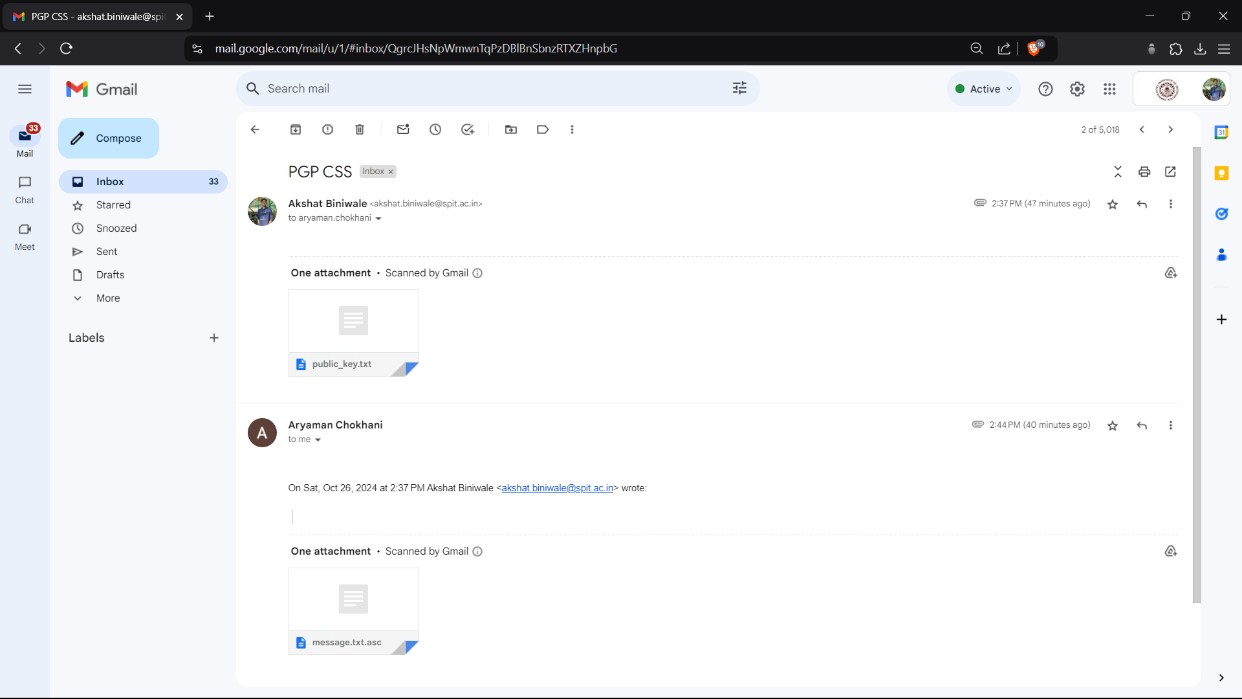
1. Key Generation



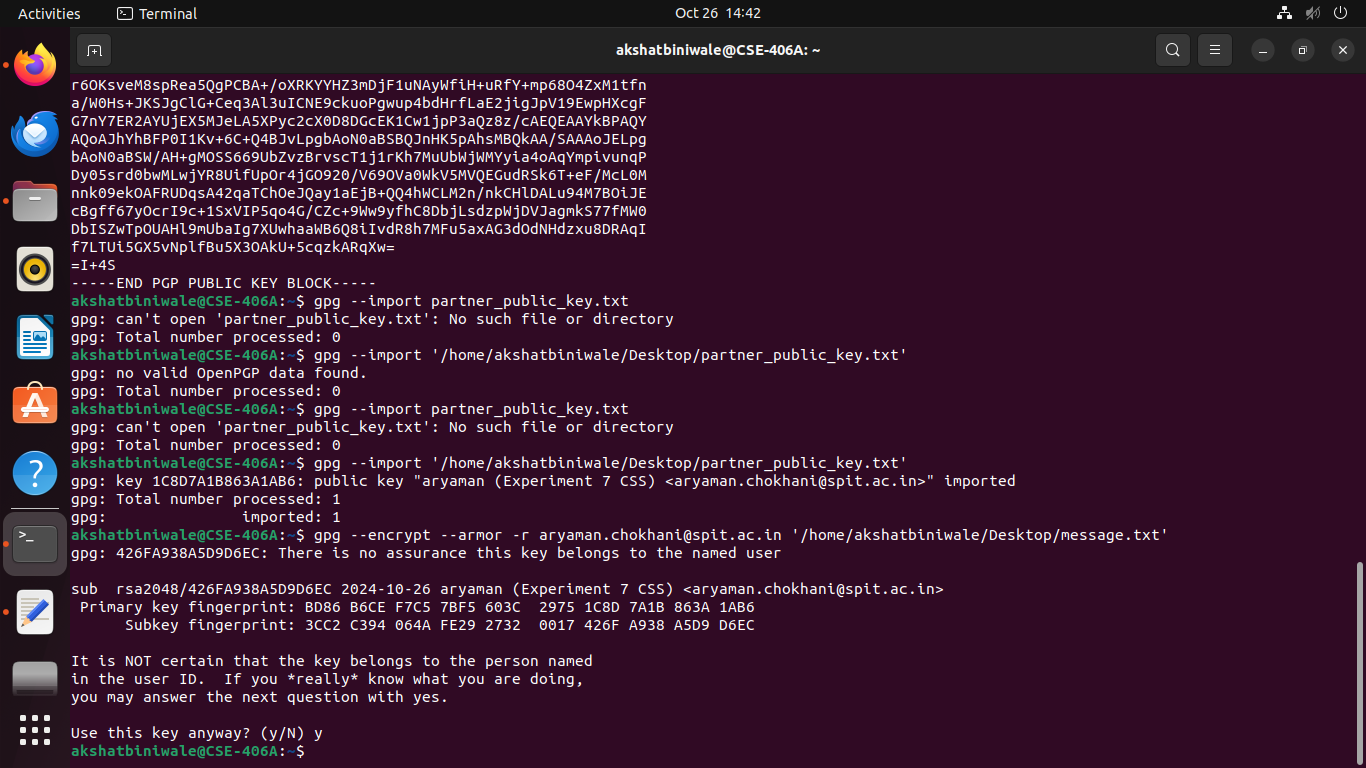


1. Export and send the public key to the receiver.

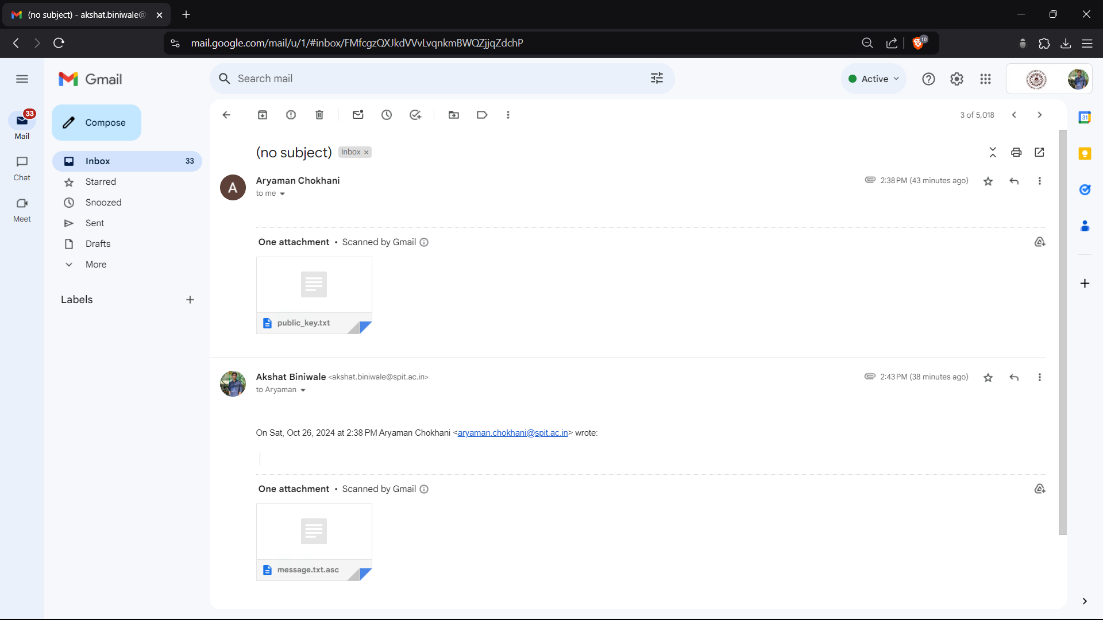


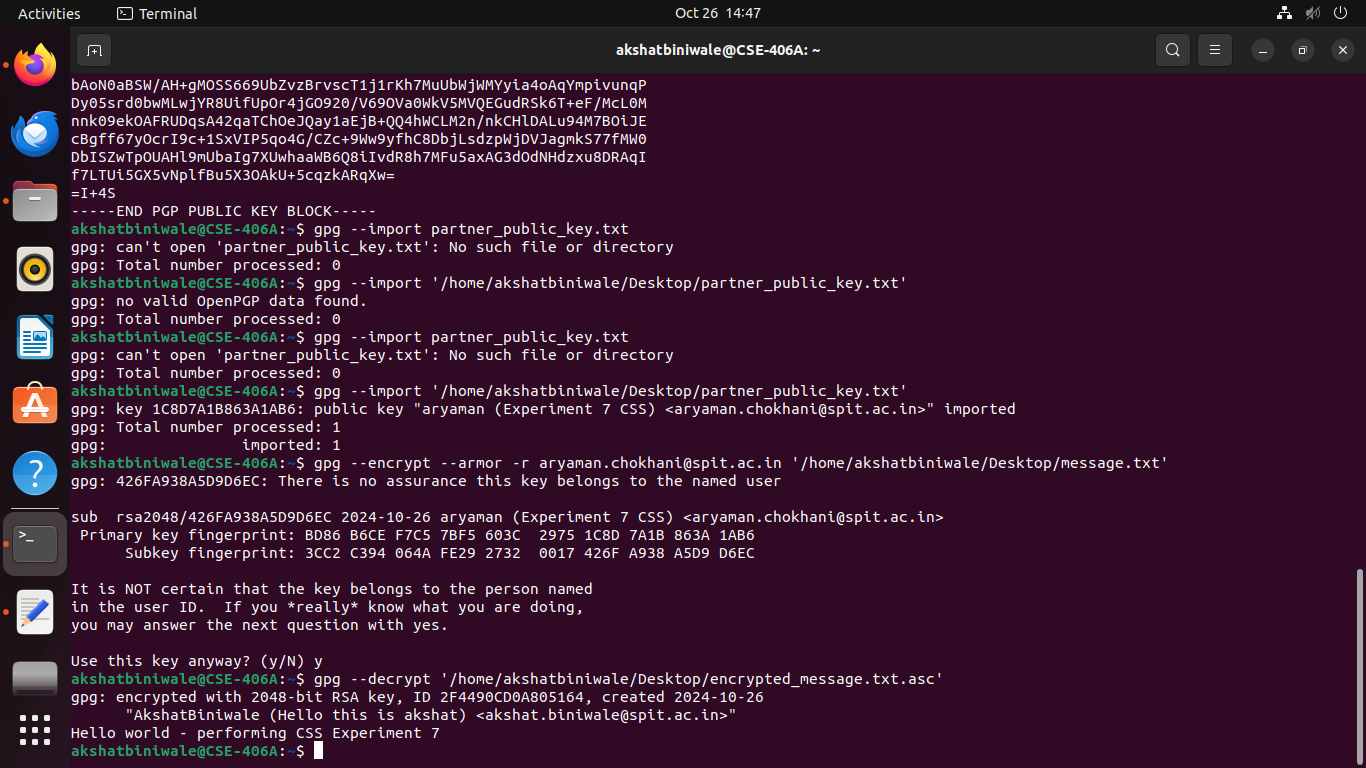


1. Create a message file and encrypt it using receiver’s public key.



1. Send the encrypted text file to the receiver, receiver decrypts the encrypted file.





Discussion:

The experiment demonstrates the core functionality of PGP, focusing on key generation, encryption, decryption, and digital signatures. PGP's practical strength lies in its ability to seamlessly combine symmetric encryption for data protection and asymmetric cryptography for secure key exchange. This ensures both speed and security during data transmission.

Security Implications

1. Confidentiality and Integrity: Encryption ensures that only the intended recipient can decrypt the content, protecting sensitive data from unauthorized access. The integrity of the data is preserved, as PGP detects any alterations during transmission.
2. Authentication through Digital Signatures: Digital signatures offer proof of the sender’s identity, mitigating risks related to impersonation attacks or spoofing.
3. Non-repudiation: By signing messages, senders cannot deny their involvement, enhancing accountability in communication.
4. Man-in-the-Middle Attacks: PGP mitigates these risks by relying on public-key cryptography and verification, ensuring the receiver can confirm the authenticity of both the sender and the message.

Practical Evaluation

While PGP is highly effective for email security, file encryption, and digital signatures, it does come with challenges:

1. Complexity: Key management can be cumbersome, especially for non-technical users.
2. Trust and Key Distribution: Users must ensure they receive authentic public keys, as a compromised key exchange can render the encryption ineffective.
3. Scalability Issues: Managing keys across large networks can be resource-intensive, particularly without automated systems.

In real-world applications, PGP remains widely used for email encryption and secure communication but requires proper education and infrastructure to manage keys effectively.

Conclusion:

PGP plays a crucial role in securing digital communication by providing **confidentiality, authentication, integrity,** and **non-repudiation**. It ensures that sensitive information can be shared safely, even over insecure networks, and that both senders and receivers can trust the data they exchange. Despite challenges with key management and user adoption, PGP remains a cornerstone in modern encryption practices. Its practical utility in email security, data protection, and digital signatures highlights its enduring importance in safeguarding privacy in the digital age.