Somaiya Vidyavihar University
K J Somaiya School of Engineering

Course Name:	**Information Security (116U01L602)**	**Semester:**	**VI**
Date of Performance:	13 / 03 / 2025	**DIV/ Batch No:**	A-4
Student Name:	Hyder Presswala	**Roll No:**	16010122151

Title: Email Security using PGP

Objectives:

PGP (Pretty Good Privacy) is a robust email security protocol that uses encryption and digital signatures to ensure the confidentiality, integrity, and authenticity of email communications. By encrypting the content of the message, PGP ensures that only the intended recipient with the correct private key can decrypt and read it. Additionally, digital signatures verify the sender's identity and protect the email from tampering. This makes PGP an essential tool for protecting sensitive information and maintaining privacy in email communication.

Expected Outcome of Experiment:

CO4 :- Illustrate and Compare network security mechanisms

Books/ Journals/ Websites referred:

https://www.geeksforgeeks.org/how-to-setup-dvwa-in-windows/#step-3-download-dvwa
https://www.youtube.com/watch?v=GBxTcM9IM3Q

Pre Lab/ Prior Concepts:

New Concepts to be learned:

Public and Private Keys:

Public Key: A cryptographic key shared publicly for encrypting messages.

Private Key: A secret key kept by the recipient to decrypt messages.

Asymmetric Encryption:
The encryption method used by PGP, where a pair of keys (public and private) are used for encryption and decryption, ensuring that only the intended recipient can decrypt the message.

Digital Signatures:
A cryptographic method to verify the authenticity and integrity of the sender's identity and the message content.

Symmetric Encryption:
A simpler form of encryption where the same key is used for both encryption and decryption, often used within PGP after the message is encrypted with the public key.

Key Management:
The process of generating, distributing, and securely storing public and private keys. Effective key management is essential for secure email communication.

Web of Trust:
A decentralized trust model used in PGP where users validate each other's keys, creating a "web" of trusted connections instead of relying solely on centralized authorities.

Message Integrity:
Ensuring that the message has not been altered in transit by using hashing techniques, as part of the digital signature process.

PGP Encryption Algorithms:
Learning the different algorithms used in PGP, such as RSA (for public-key encryption) and AES (for symmetric encryption), helps understand the cryptographic mechanisms behind PGP.

Abstract:

PGP (Pretty Good Privacy) is a widely used encryption protocol that ensures the security and privacy of email communications. By employing asymmetric encryption, PGP allows users to encrypt messages with a public key and decrypt them with a private key, ensuring confidentiality. It also utilizes digital signatures to authenticate the sender’s identity and verify message integrity. With a focus on key management and a decentralized trust model, PGP offers a robust solution for protecting sensitive information against unauthorized access and tampering in email exchanges.

Related Theory:

- **Public Key Cryptography (Asymmetric Encryption)**:
  PGP uses two keys—one public and one private. The public key is used to encrypt the message, while the private key is used by the recipient to decrypt it. This ensures that only the recipient with the corresponding private key can read the message, providing confidentiality.

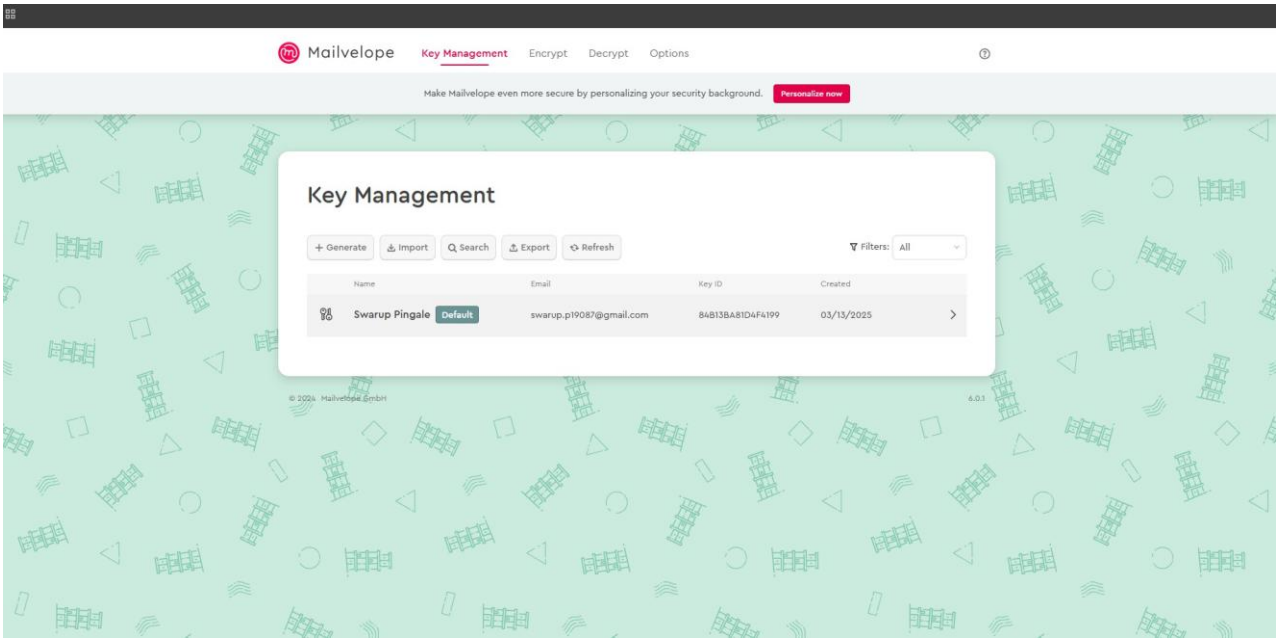
- **Digital Signatures**:
  A digital signature verifies the sender's identity and ensures that the message has not been altered. It works by generating a hash (a unique value) of the message, which is then encrypted with the sender's private key. The recipient can decrypt the hash using the sender's public key, ensuring that the message is authentic and unchanged.

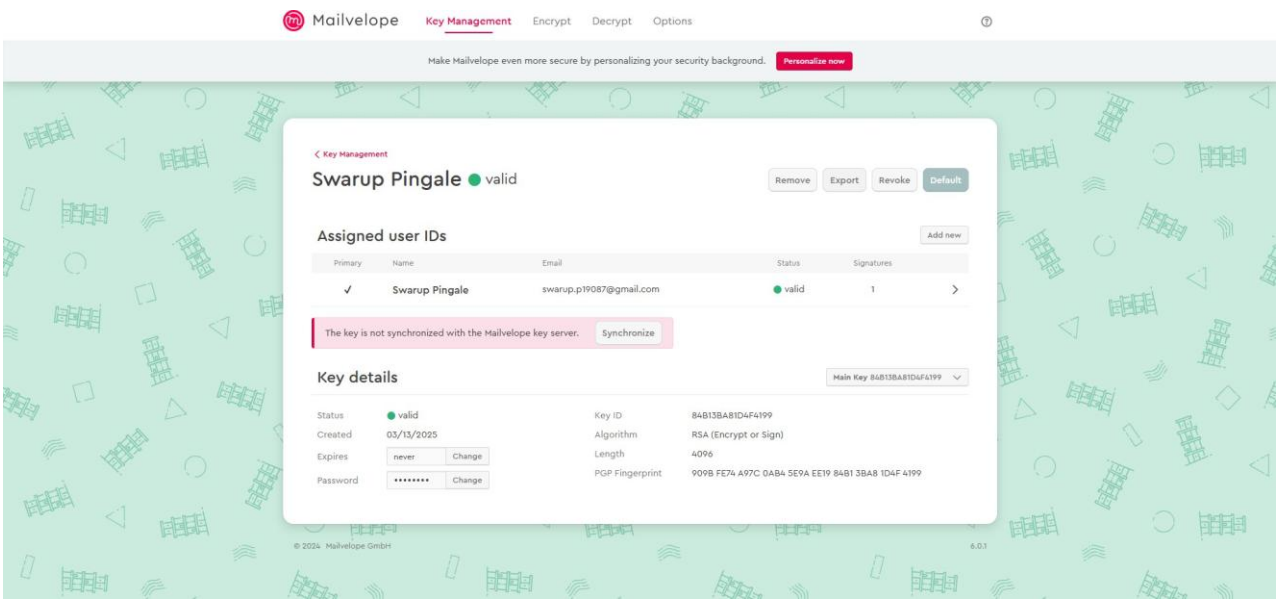
- **Symmetric Encryption**:
  For efficiency, after the message is encrypted with the recipient's public key, PGP often uses symmetric encryption (e.g., AES) to encrypt the actual message content. This method uses a shared secret key to encrypt and decrypt the data, offering faster encryption than asymmetric methods.

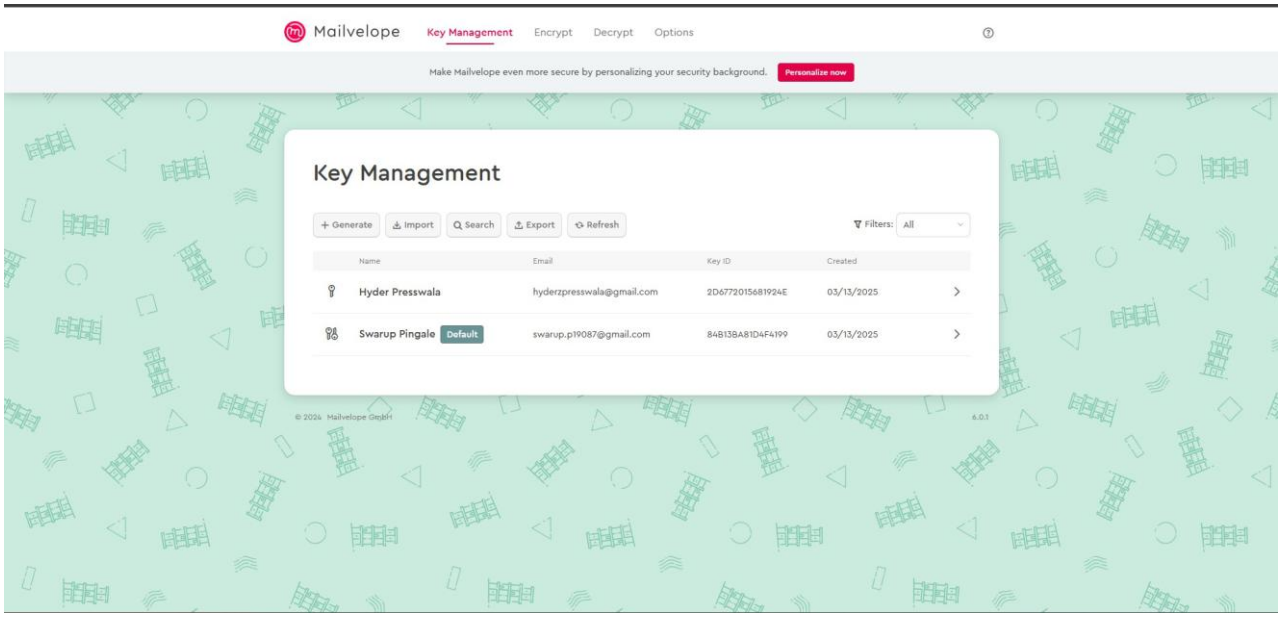
- **Key Management**:
  Effective key management is critical for ensuring the integrity and security of communication. PGP allows users to manage their encryption keys, ensuring that private keys remain confidential while public keys are shared securely with trusted parties.

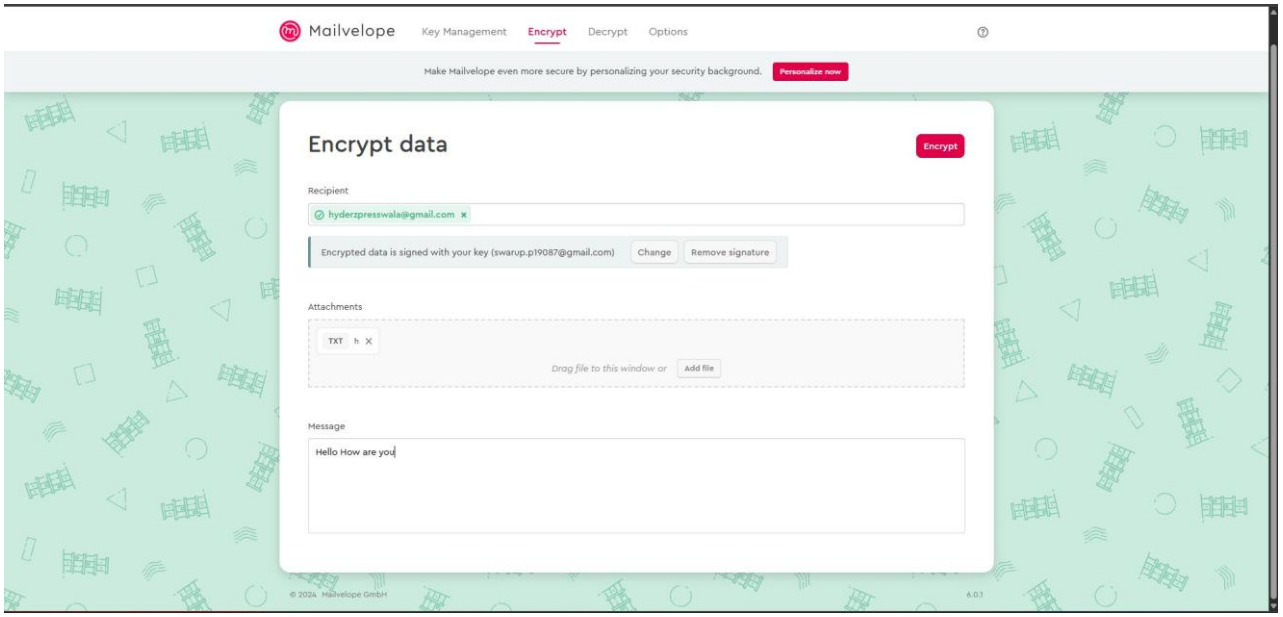
- **Web of Trust**:
  PGP's decentralized trust model allows users to validate one another's public keys. Instead of relying on centralized authorities, users create a "web" of trust by signing each other's keys, ensuring the authenticity of public keys in the system.

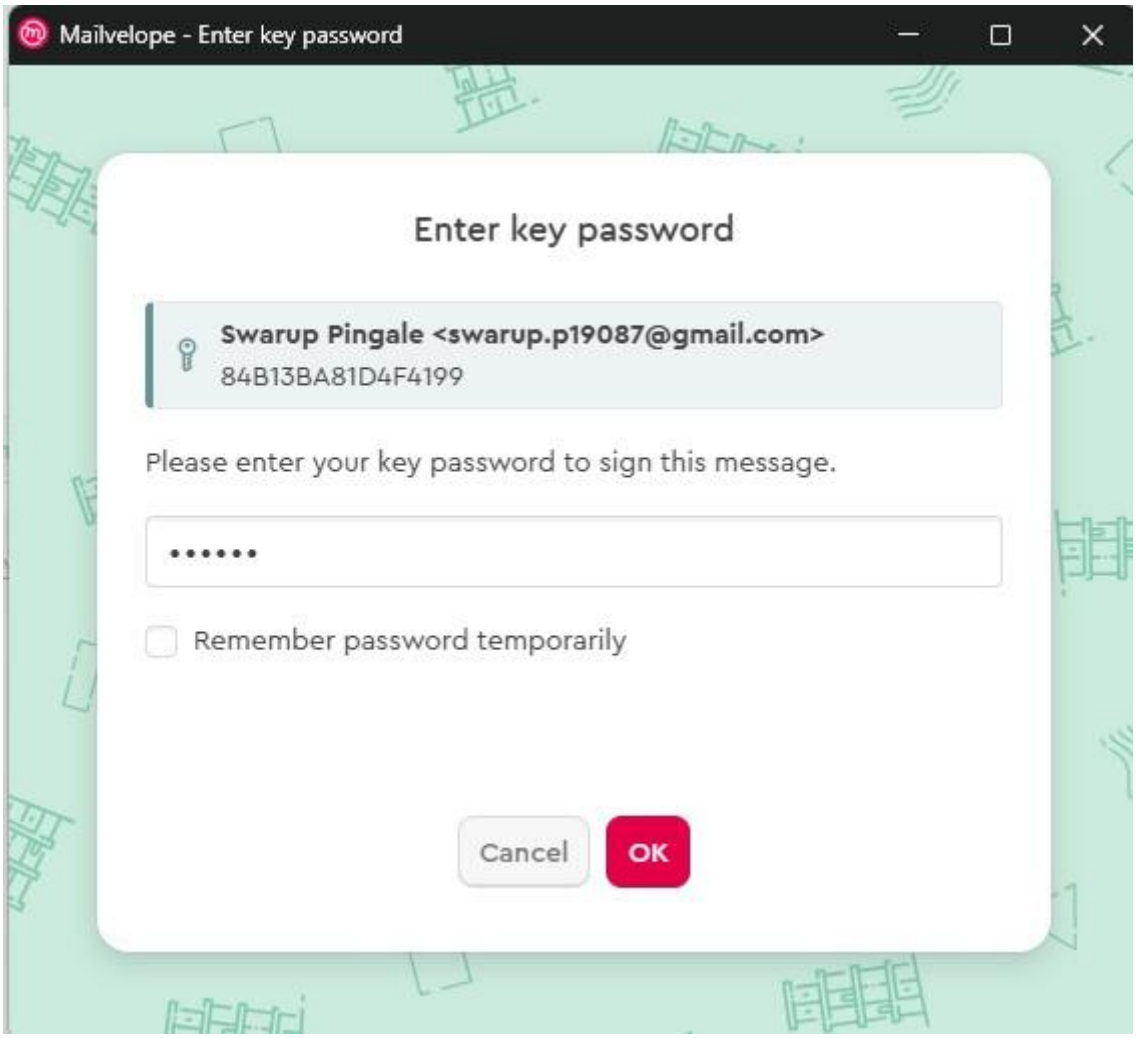
Implementation Details:

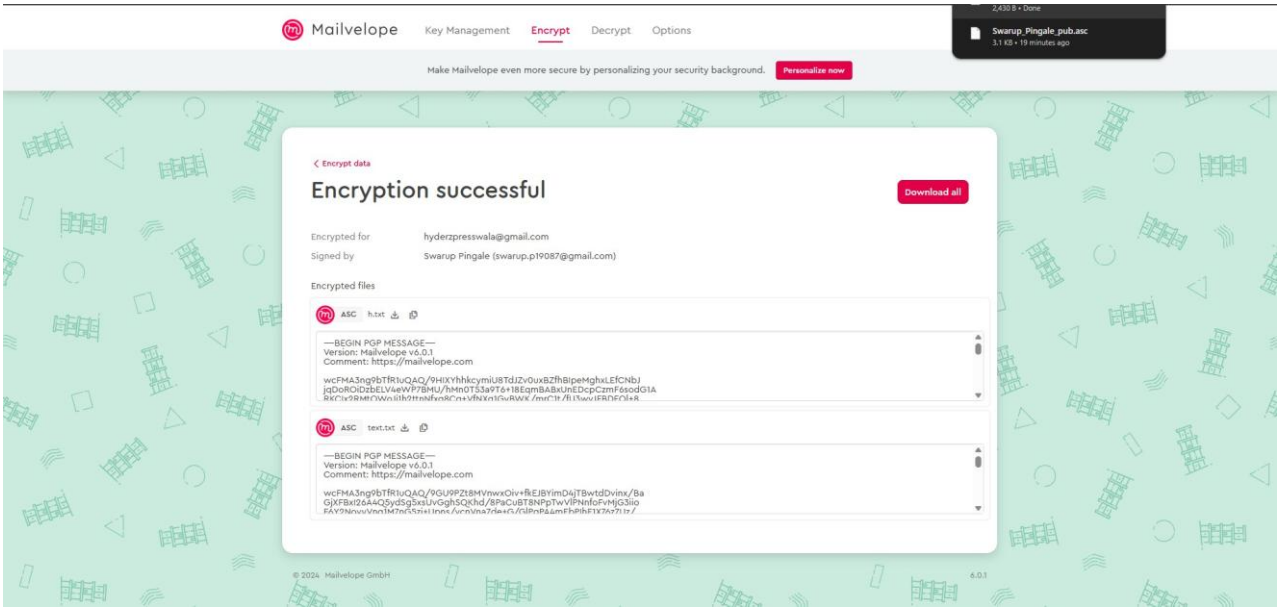


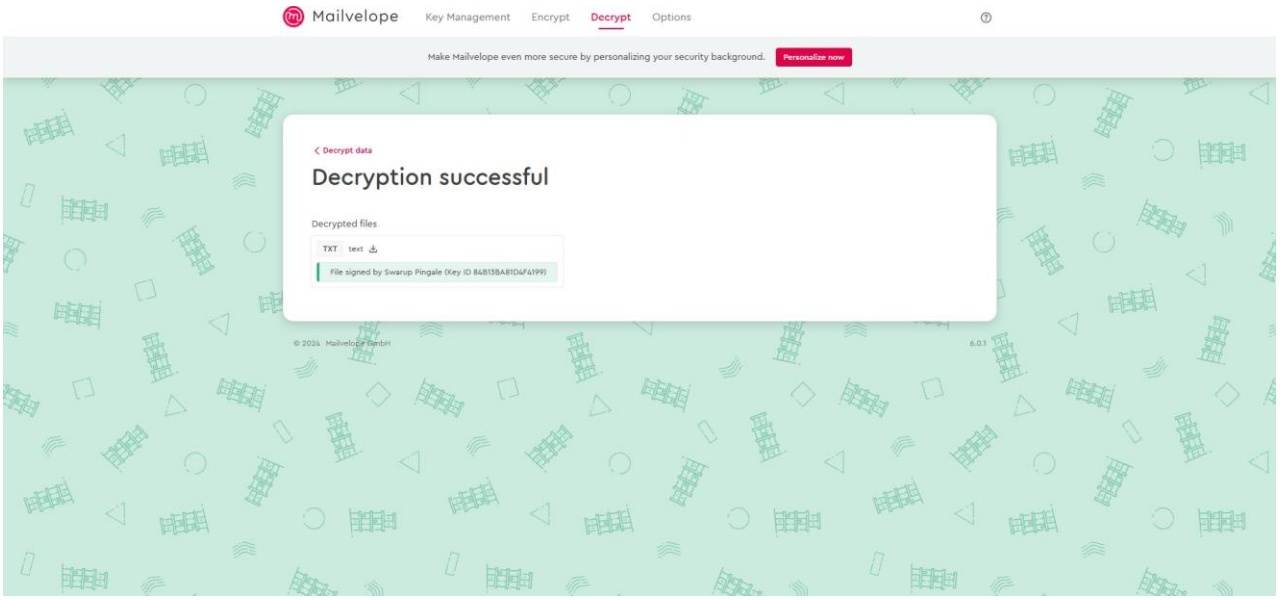


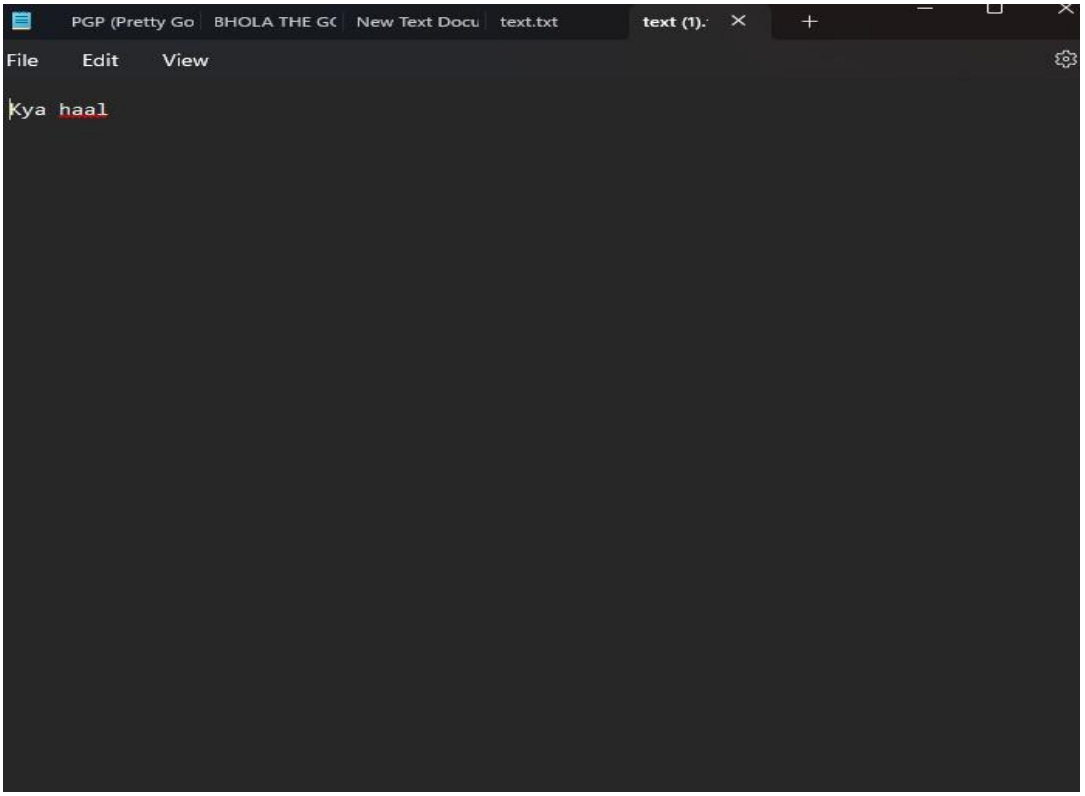

Mailvelope
Key Management
Encrypt
Decrypt
Options
Make Mailvelope even more secure by personalizing your security background.
Personalize now
Key Management
+ Generate
Import
Search
Export
Refresh
Filters:
All
Name
Email
Key ID
Created
Hyder Presswala
hyderzpresswala@gmail.com
2D67720156819 24E
03/13/2025
Swarup Pingale
Default
swarup.p19087@gmail.com
84B13BA81D4F4199
03/13/2025
© 2024 Mailvelope GmbH
6.0.1

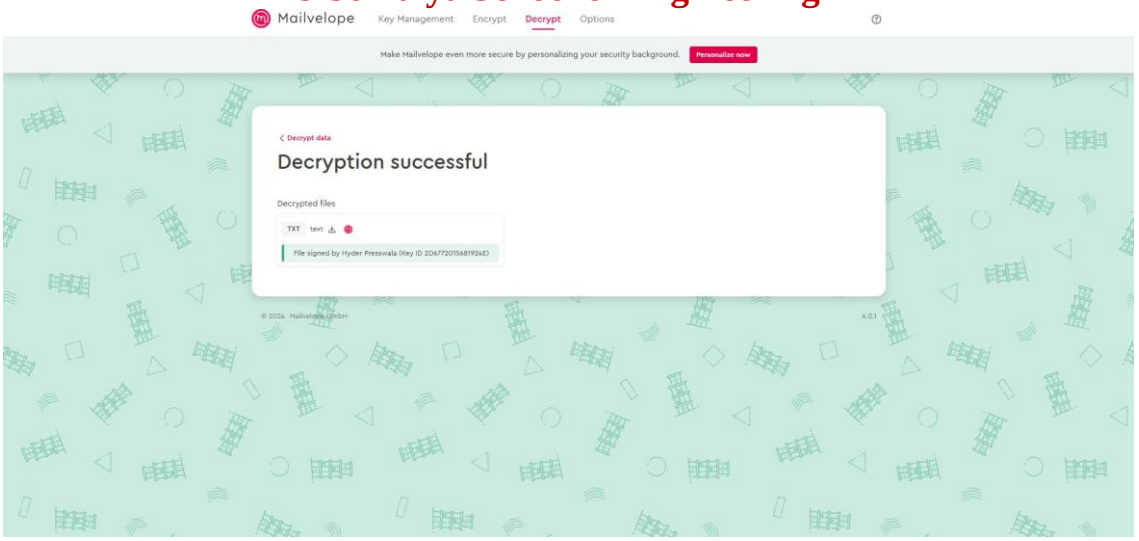

Mailvelope
Key Management
Encrypt
Decrypt
Options
Make Mailvelope even more secure by personalizing your security background.
Personalize now
Encrypt data
Encrypt
Recipient
hyderzpresswala@gmail.com
Encrypted data is signed with your key (swarup.p19087@gmail.com)
Change
Remove signature
Attachments
TXT h
Drag file to this window or
Add file
Message
Hello How are you
© 2024 Mailvelope GmbH
6.0.1

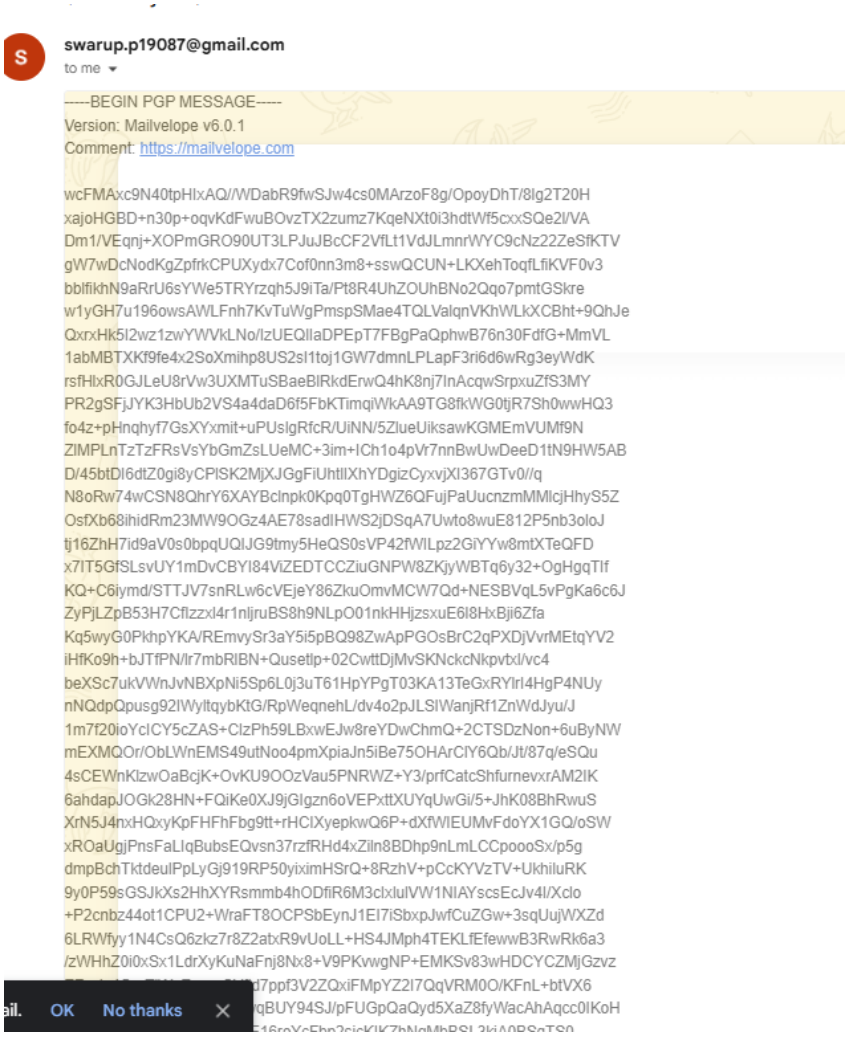

Mailvelope - Enter key password
Enter key password
Swarup Pingale <swarup.p19087@gmail.com>
84B13BA81D4F4199
Please enter your key password to sign this message.
Remember password temporarily
Cancel
OK

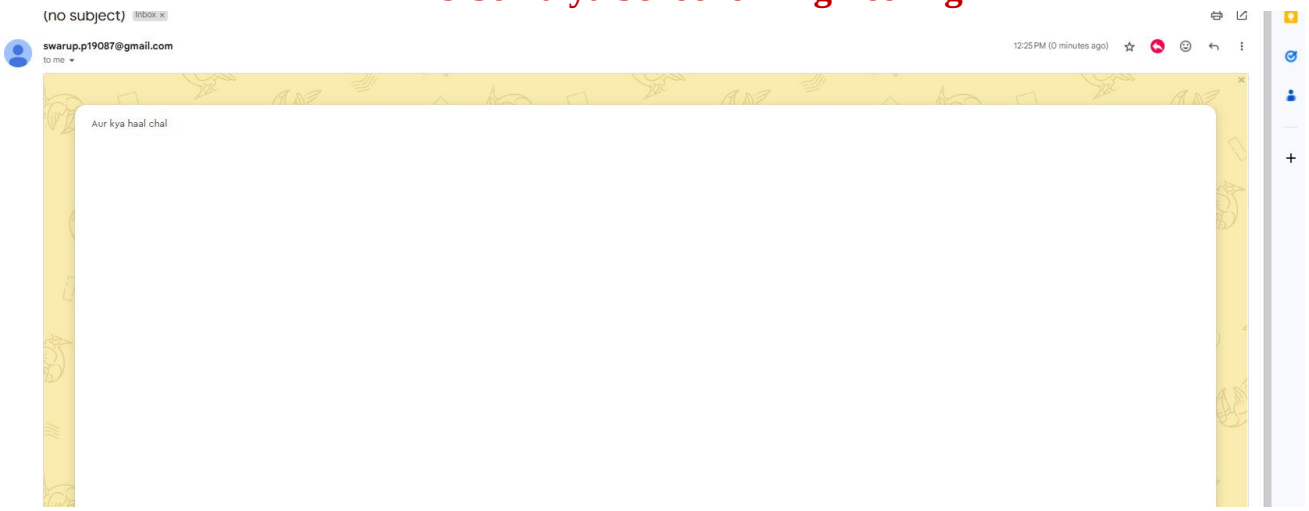

Mailvelope
Key Management
Encrypt
Decrypt
Options
Swarup_Pingale_pub.asc
Make Mailvelope even more secure by personalizing your security background.
Personalize now
Encrypt data
Encryption successful
Download all
Encrypted for
hyderzpresswala@gmail.com
Signed by
Swarup Pingale (swarup.p19087@gmail.com)
Encrypted files
—BEGIN PGP MESSAGE—
Version: Mailvelope v6.0.1
Comment: https://mailvelope.com
—BEGIN PGP MESSAGE—
Version: Mailvelope v6.0.1
Comment: https://mailvelope.com


Mailvelope
Key Management
Encrypt
Decrypt
Options
Make Mailvelope even more secure by personalizing your security background.
Personalize now
Decrypt data
Decryption successful
Decrypted files
TXT
text
File signed by Swarup Pingale (Key ID 84B13BA81DAF4199)


PGP (Pretty Go
BHOLA THE GC
New Text Docu
text.txt
text (1).
File
Edit
View
Kya haal


Mailvelope
Key Management
Encrypt
Decrypt
Options
Make Mailvelope even more secure by personalizing your security background.
Personalize now
Decrypt data
Decryption successful
Decrypted files
TXT
text
File signed by Hyder Presswala (Key ID 2D67720156819241)


swarup.p19087@gmail.com
to me
-----BEGIN PGP MESSAGE-----
Version: Mailvelope v6.0.1
Comment: https://mailvelope.com
wcFMAxc9N40tpHIxAQ//WDabR9fwSJw4cs0MArzoF8g/OpoyDhT/8Ig2T20H
xajoHGBD+n30p+oqvKdFwuBOvzTX2zumz7KqeNXt0i3hdtWf5cxxSQe2l/VA
Dm1/VEqnj+XOPmGRO90UT3LPJuJBcCF2VfLt1VdJLmnrWYC9cNz22ZeSfKTV
gW7wDcNodKgZpfrkCPUXydx7Cof0nn3m8+sswQCUN+LKXehToqfLfiKVF0v3
bblfikhN9aRrU6sYWe5TRYrzqh5J9iTa/Pt8R4UhZOUhBNo2Qqo7pmtGSkre
w1yGH7u196owsAWLFnh7KvTuWgPmspSMae4TQLValqnVKhWLkXCBht+9QhJe
QxrxHk5l2wz1zwYWVkLNo/lzUEQIlaDPEpT7FBgPaQphwB76n30FdfG+MmVL
1abMBTXKf9fe4x2SoXmihp8US2sI1toj1GW7dmnLPLapF3ri6d6wRg3eyWdK
rsfHlxR0GJLeU8rVw3UXMTuSBaeBlRkdErwQ4hK8nj7InAcqwSrpxuZfS3MY
PR2gSFjJYK3HbUb2VS4a4daD6f5FbKTimqiWkAA9TG8fkWG0tjR7Sh0wwHQ3
fo4z+pHnqhyf7GsXYxmit+uPUsIgRfcR/UiNN/5ZlueUiksawKGMEmVUMf9N
ZIMPLnTzTzFRsVsYbGmZsLUeMC+3im+ICh1o4pVr7nnBwUwDeeD1tN9HW5AB
D/45btDl6dtZ0gi8yCPlSK2MjXJGgFiUhtlIXhYDgizCyxvjXI367GTv0//q
N8oRw74wCSN8QhrY6XAYBclnpk0Kpq0TgHWZ6QFujPaUucnzmMMlcjHhyS5Z
OsfXb68ihidRm23MW9OGz4AE78sadlHWS2jDSqA7Uwto8wuE812P5nb3oloJ
tj16ZhH7id9aV0s0bpqUQlJG9tmy5HeQS0sVP42fWILpz2GiYYw8mtXTeQFD
x7IT5GfSLsvUY1mDvCBYI84ViZEDTCCZiuGNPW8ZKjyWBTq6y32+OgHgqTlf
KQ+C6iymd/STTJV7snRLw6cVEjeY86ZkuOmvMCW7Qd+NESBVqL5vPgKa6c6J
ZyPjLZpB53H7Cflzzxl4r1nljruBS8h9NLpO01nkHHjzsxuE6l8HxBji6Zfa
Kq5wyG0PkhpYKA/REmvySr3aY5i5pBQ98ZwApPGOsBrC2qPXDjVvrMEtqYV2
iHfKo9h+bJTfPN/lr7mbRlBN+QusetIp+02CwttDjMvSKNckcNkpvtxl/vc4
beXSc7ukVWnJvNBXpNi5Sp6L0j3uT61HpYPgT03KA13TeGxRYlrl4HgP4NUy
nNQdpQpusg92lWyltqybKtG/RpWeqnehL/dv4o2pJLSlWanjRf1ZnWdJyu/J
1m7f20ioYcICY5cZAS+ClzPh59LBxwEJw8reYDwChmQ+2CTSDzNon+6uByNW
mEXMQOr/ObLWnEMS49utNoo4pmXpiaJn5iBe75OHArClY6Qb/Jt/87q/eSQu
4sCEWnKlzwOaBcjK+OvKU9OOzVau5PNRWZ+Y3/prfCatcShfurnevxrAM2IK
6ahdapJOGk28HN+FQiKe0XJ9jGlgzn6oVEPxttXUYqUwGi/5+JhK08BhRwuS
XrN5J4nxHQxyKpFHFhFbg9tt+rHClXyepkwQ6P+dXfWIEUMvFdoYX1GQ/oSW
xROaUgjPnsFaLIqBubsEQvsn37rzfRHd4xZiln8BDhp9nLmLCCpoooSx/p5g
dmpBchTktdeulPpLyGj919RP50yixImHSrQ+8RzhV+pCcKYVzTV+UkhiluRK
9y0P59sGSJkXs2HhXYRsmmb4hODfiR6M3clxlulVW1NlAYscsEcJv4l/Xclo
+P2cnbz44ot1CPU2+WraFT8OCPSbEynJ1EI7iSbxpJwfCuZGw+3sqUujWXZd
6LRWfyy1N4CsQ6zkz7r8Z2atxR9vUoLL+HS4JMph4TEKLfEfewwB3RwRk6a3
/zWHhZ0i0xSx1LdrXyKuNaFnj8Nx8+V9PKvwgNP+EMKSv83wHDCYCZMjGzvz
OK
No thanks



Conclusion:
PGP (Pretty Good Privacy) provides a robust and effective solution for securing email communications through public key cryptography, digital signatures, and key management. By ensuring confidentiality, authenticity, and integrity, it protects sensitive information from unauthorized access and tampering. PGP's decentralized trust model and efficient encryption methods make it a vital tool for maintaining privacy in today's digital communication.

6.1 In PGP, explain how Bob and Alice exchange the secret key for encrypting the messages?

In PGP, Bob and Alice exchange the secret key using a combination of asymmetric and symmetric encryption. First, Alice generates a random secret key (session key) for encrypting the message. She then encrypts this session key with Bob's public key (asymmetric encryption). Bob, using his private key, decrypts the session key. Once the session key is exchanged securely, both Alice and Bob use it to encrypt and decrypt the message using symmetric encryption, which is faster.

6.2 List the types of algorithms used in PGP.

PGP uses three types of algorithms:

1. Asymmetric Encryption Algorithms (e.g., RSA, DSA): Used for encrypting the session key and for digital signatures.

2. Symmetric Encryption Algorithms (e.g., AES, IDEA): Used to encrypt the actual message content.
3. Hash Functions (e.g., SHA-1, MD5): Used to create message digests for ensuring data integrity and creating digital signatures.

6.3 Explain the significance of key rings in PGP.

In PGP, a key ring is a collection of public and private keys stored locally on a user's system. The public key ring holds the public keys of others for encrypting messages, while the private key ring stores the user's private key for decryption and signing messages. Key rings are essential for managing multiple keys, keeping track of trusted keys, and ensuring secure communication.

6.4 Distinguish between PGP and S/MIME.

PGP (Pretty Good Privacy):

- A decentralized, open-source encryption standard.
- Uses a web of trust for key validation.
- Primarily focused on email encryption and digital signatures.

S/MIME (Secure/Multipurpose Internet Mail Extensions):

- A more centralized, standards-based encryption protocol.
- Uses a public key infrastructure (PKI) for key management and validation via trusted Certificate Authorities (CAs).
- Designed for securing emails and other MIME-based data formats, commonly used in enterprise environments.