**Batch: B1 Roll No.: 16010121045**

**Experiment No. 5**

|  |
| --- |
| **Title:**  Email security using PGP implementation (Pretty Good Privacy) |

**Objective:** To make use of the Mailvelope extension to implement PGP encryption for

cryptographic privacy and authentication for data communication.

**Expected Outcome of Experiment: To implement Cryptanalysis Tools .**

|  |  |
| --- | --- |
| **CO** | **Outcome** |
| **CO3** | Illustrate Secure software design principles and apply them for secure software development |

**Books/ Journals/ Websites referred:**

[**https://www.varonis.com/blog/pgp-encryption**](https://www.varonis.com/blog/pgp-encryption)

[**https://www.goanywhere.com/blog/everything-you-need-to-know-about-pgp-encryption**](https://www.goanywhere.com/blog/everything-you-need-to-know-about-pgp-encryption)

**Abstract**:-

PGP, or Pretty Good Privacy, is a widely-used encryption program that provides cryptographic privacy and authentication for data communication. It utilizes a combination of symmetric-key cryptography and public-key cryptography to secure messages, ensuring confidentiality, integrity, and authenticity.

**Related Theory: -**

**How PGP Works:**

PGP employs a hybrid encryption scheme that combines symmetric and asymmetric encryption. Here's a simplified overview:

1. **Key Generation**: Each user generates a pair of cryptographic keys - a public key and a private key. The public key is shared with others, while the private key is kept secret.
2. **Encryption**:
   * **Symmetric Encryption**: A random session key is generated for each message. The message is encrypted using this session key.
   * **Asymmetric Encryption**: The session key is then encrypted using the recipient's public key.
3. **Decryption**:
   * The recipient uses their private key to decrypt the session key.
   * The session key is then used to decrypt the message.

**Security Goals Achieved by PGP:**

1. **Confidentiality**: Messages can only be read by the intended recipient.
2. **Integrity**: Any tampering with the message can be detected.
3. **Authentication**: Ensures that the sender is who they claim to be.
4. **Non-repudiation**: Prevents the sender from denying that they sent a message.

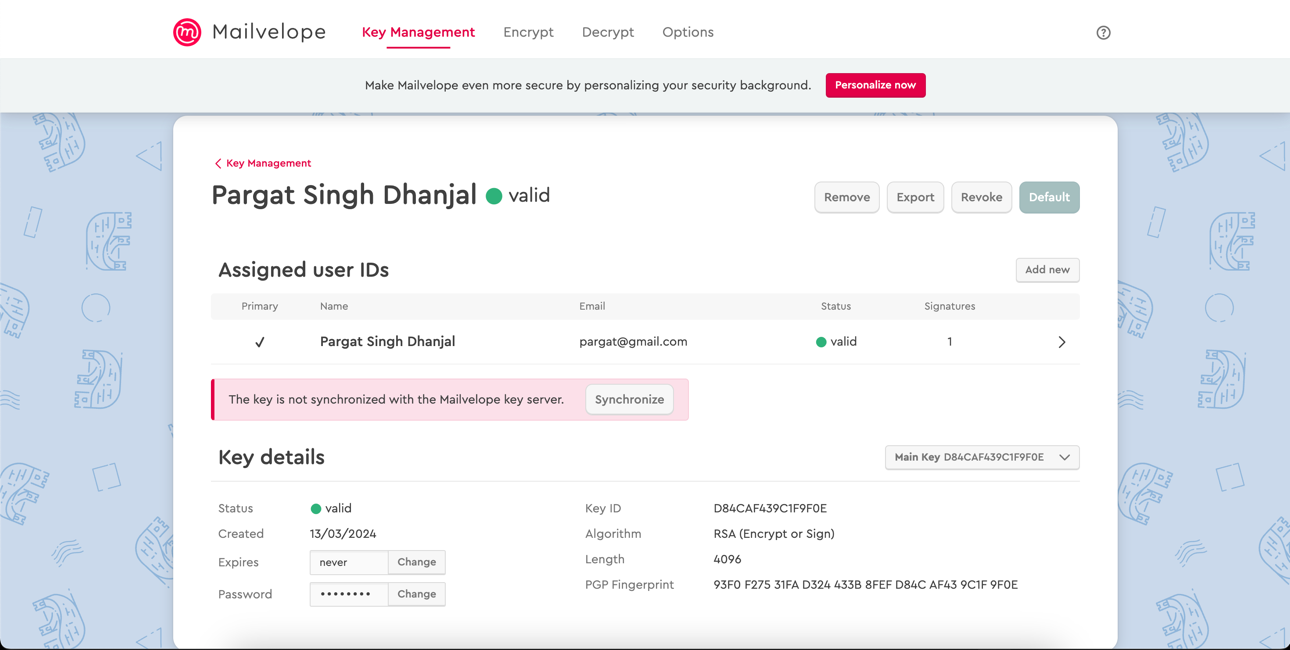
**Real-Life Applications of PGP:**

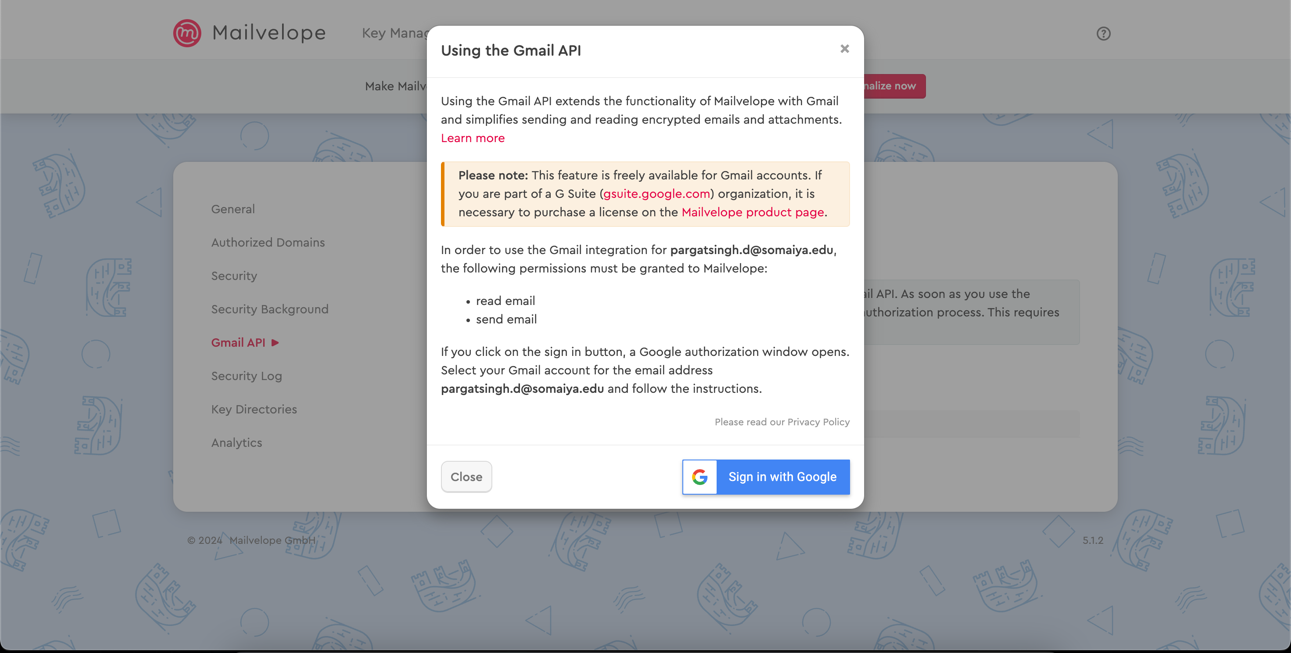
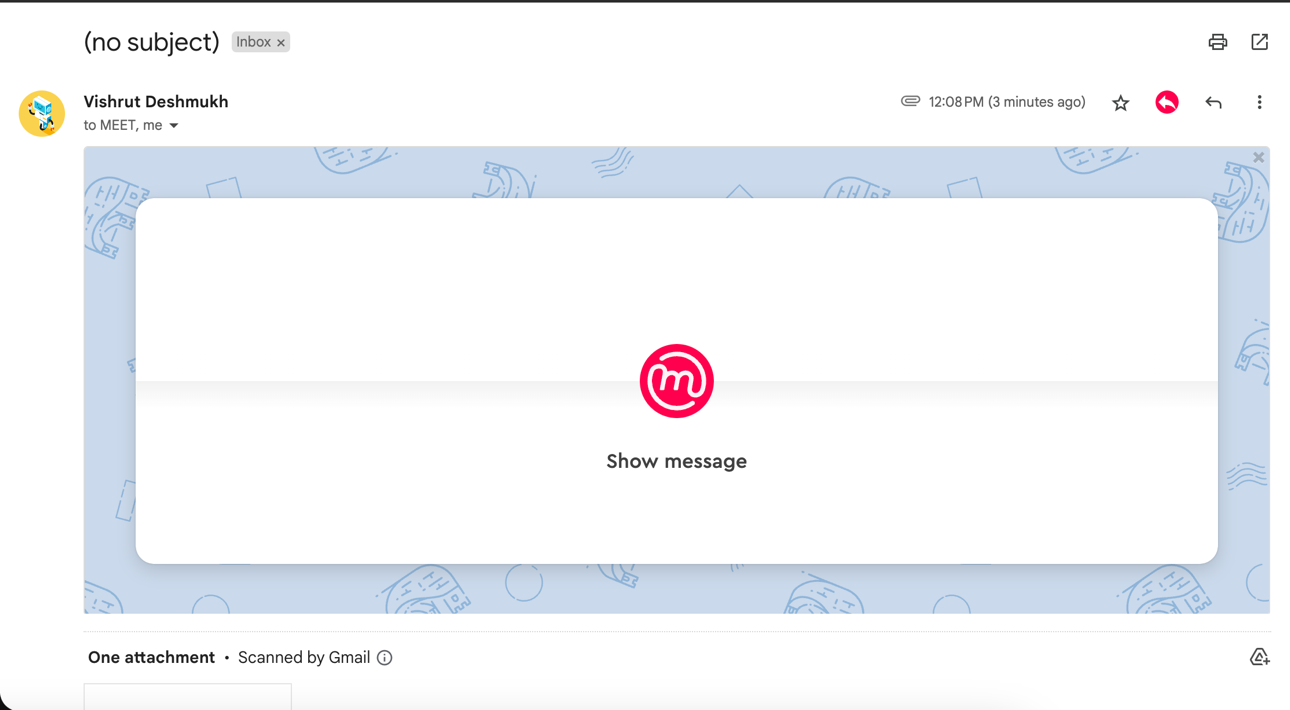
1. Secure Email Communication
2. File Encryption
3. Digital Signatures
4. Secure Messaging Platforms

**Limitations of PGP:**

1. **Key Management**: Handling key distribution and verification can be complex.
2. **Trust Model**: Users must verify the authenticity of public keys manually.
3. **Backdoors**: Vulnerabilities in implementation can compromise security.
4. **Limited Adoption**: Not all email clients support PGP, limiting its widespread use.

**Implementation**

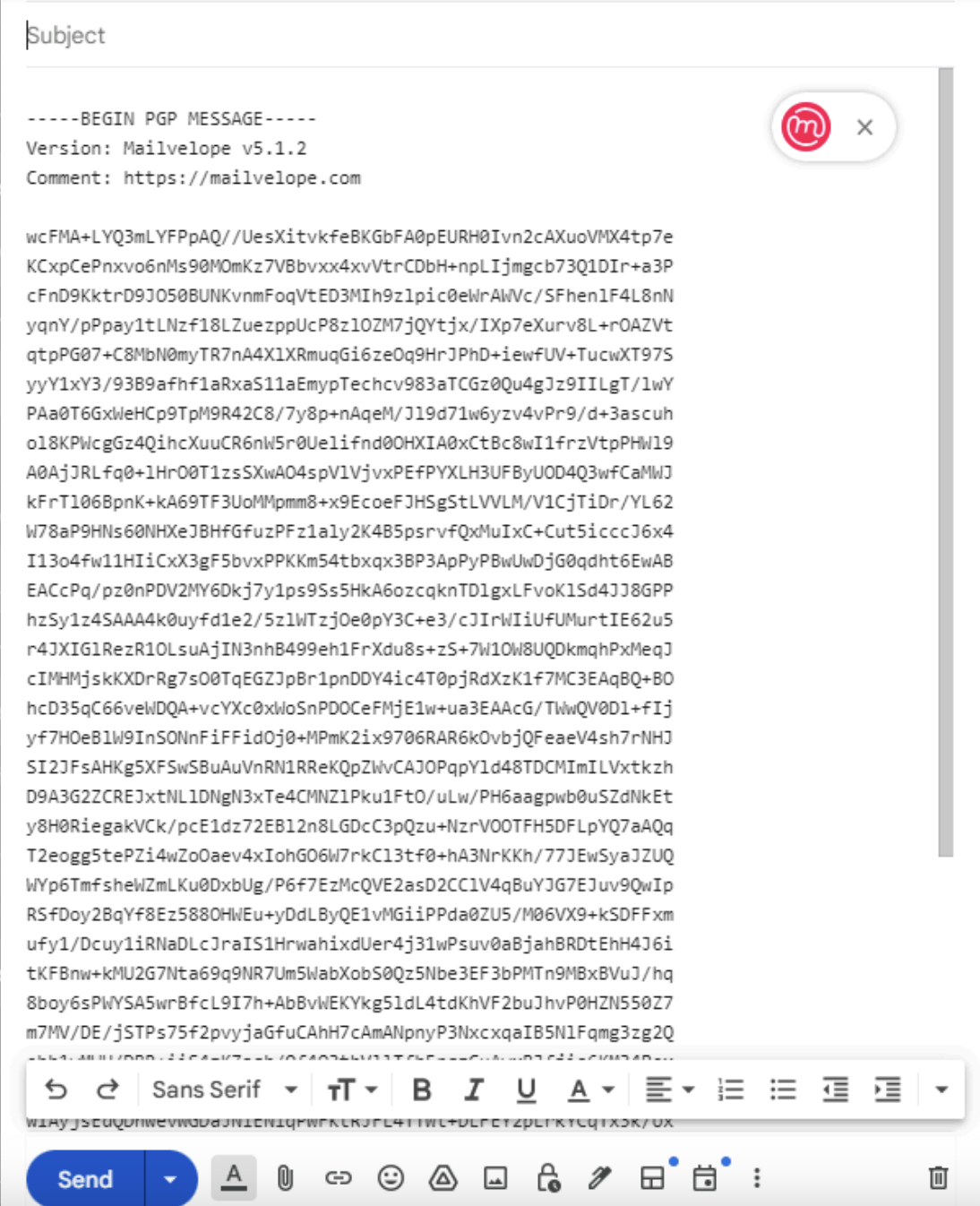
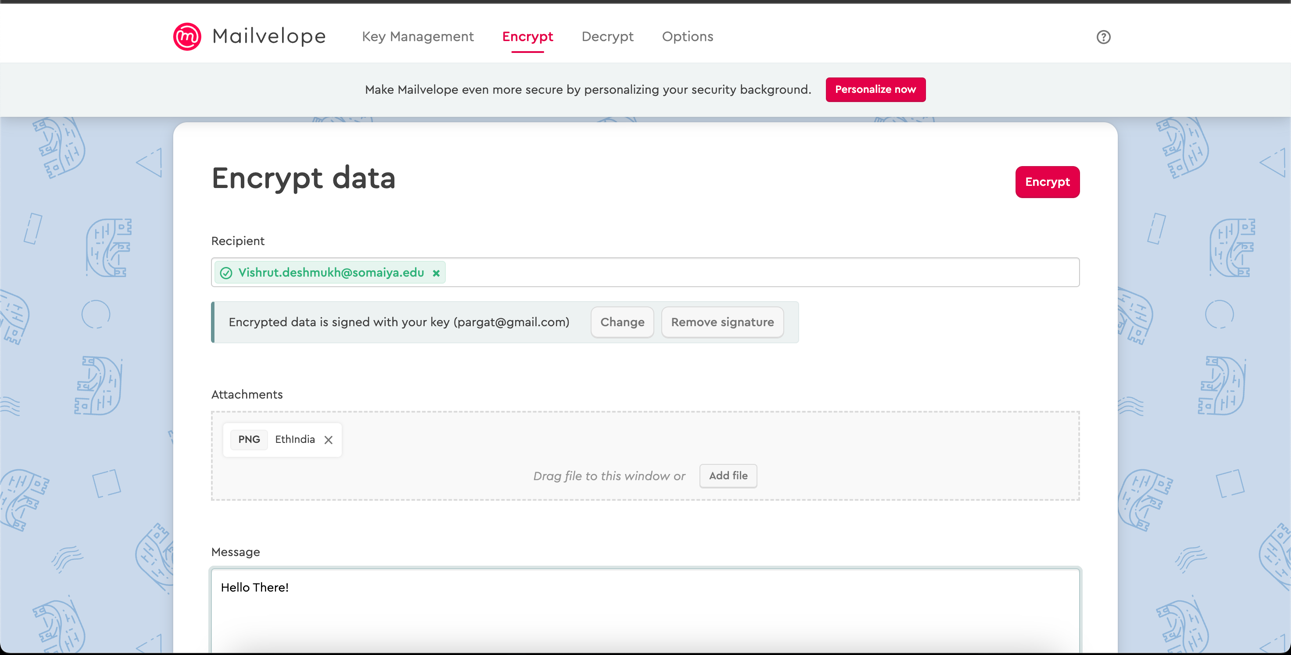
****

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

****

**Conclusion:-** Hence, we understood and implemented email security using PGP.

**Postlab Questions:**

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

Bob and Alice exchange messages using PGP through a process called key exchange. They share their public keys with each other through a secure channel (e.g., in person, via a trusted intermediary, or through a secure online platform). Once each party has the other's public key, they can encrypt messages using the recipient's public key. The recipient then uses their private key to decrypt the message.

6.2 **List the types of algorithms used in PGP.**

PGP uses various cryptographic algorithms including:

* RSA for asymmetric encryption and digital signatures
* AES (Advanced Encryption Standard) for symmetric encryption
* SHA (Secure Hash Algorithm) for hashing
* IDEA or Triple DES for older versions

6.3 **Explain the significance of key rings in PGP.**

Key rings in PGP store the user's public and private keys. They serve as a repository for managing keys, including storing, importing, exporting, and revoking keys. Key rings are crucial for encryption, decryption, and digital signature processes within PGP.

6.4 **Distinguish between PGP and S/MIME.**

* **PGP (Pretty Good Privacy)**: It is a program used for data encryption and decryption. PGP uses a combination of symmetric-key cryptography and public-key cryptography. It provides confidentiality, integrity, authentication, and non-repudiation. PGP is widely used for secure email communication, file encryption, and digital signatures.
* **S/MIME (Secure/Multipurpose Internet Mail Extensions)**: It is a standard for public key encryption and signing of MIME data (email messages and attachments). S/MIME is based on X.509 certificates and is widely used for securing email communication. S/MIME provides similar security features as PGP but operates within the MIME framework for email.

Top of Form

Bottom of Form