



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

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.goanywhere.com/blog/everything-you-need-to-know-about-pgp-encryption>



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

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.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Implementation

Mailvelope **Key Management** Encrypt Decrypt Options ⓘ

Make Mailvelope even more secure by personalizing your security background. [Personalize now](#)

< Key Management

Pargat Singh Dhanjal ● valid [Remove](#) [Export](#) [Revoke](#) [Default](#)

Assigned user IDs [Add new](#)

Primary	Name	Email	Status	Signatures
✓	Pargat Singh Dhanjal	pargat@gmail.com	● valid	1

The key is not synchronized with the Mailvelope key server. [Synchronize](#)


Key details [Main Key D84CAF439C1F9F0E](#)


Status	● valid	Key ID	D84CAF439C1F9F0E
Created	13/03/2024	Algorithm	RSA (Encrypt or Sign)
Expires	<input type="text" value="never"/> Change	Length	4096
Password	<input type="text" value="*****"/> Change	PGP Fingerprint	93F0 F275 31FA D324 433B 8FEF D84C AF43 9C1F 9F0E




Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

(no subject) Inbox x 🖨️ 🔗

 **Vishrut Deshmukh**
to MEET, me ▾ 📧 12:08 PM (3 minutes ago) ★ 🔒 ↩️ ⋮


Show message

One attachment • Scanned by Gmail ⓘ 🔗

 Mailvelope Key Manager Make Mailvelope Realize now

Using the Gmail API ✕

Using the Gmail API extends the functionality of Mailvelope with Gmail and simplifies sending and reading encrypted emails and attachments. [Learn more](#)


Please note: This feature is freely available for Gmail accounts. If you are part of a G Suite (gsuite.google.com) organization, it is necessary to purchase a license on the [Mailvelope product page](#).

In order to use the Gmail integration for pargatsingh.d@somaiya.edu, the following permissions must be granted to Mailvelope:

- read email
- send email

If you click on the sign in button, a Google authorization window opens. Select your Gmail account for the email address pargatsingh.d@somaiya.edu and follow the instructions.

Please read our [Privacy Policy](#)

Close  Sign in with Google

General

Authorized Domains

Security

Security Background

Gmail API ▶

Security Log

Key Directories

Analytics

© 2024 Mailvelope GmbH 512



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Mailvelope Key Management Encrypt Decrypt Options

Make Mailvelope even more secure by personalizing your security background. [Personalize now](#)

General
Authorized Domains
Security
Security Background
Gmail API
Security Log
Key Directories
Analytics

Gmail API

☒ Gmail API Integration

Important! Mailvelope requires additional permissions to access the Gmail API. As soon as you use the encryption functions of Mailvelope in Gmail, you are guided through an authorization process. This requires you to sign in to your Google account. [Learn more](#)

Google API Authorizations

Email	Authorizations	
pargatsingh.d@somaiya.edu	send email, read email	Cancel authorization

Mailvelope License

Email	Enabled	
pargatsingh.d@somaiya.edu	<input checked="" type="checkbox"/>	Refresh

Licenses for the use of the Gmail-API integration when using the G Suite ([gsuite.google.com](#)) can be purchased on the [Mailvelope product page](#).

Mailvelope

Confirm key to import

After confirmation, this key is transferred to the local keyring:

Key ID	Name	Email	PGP Fingerprint
B92788DEDOFE1ECD	Vishrut Deshmukh	Vishrut.deshmukh@somaiya.edu	AB55 AEAF 2B3A 0B00 3428 8076 B927 88DE DOFE 1ECD

[Cancel](#) [Confirm](#)

You can add keys either as file or as text from the clipboard.

Select files

ASC keyring_pub X


Drag file to this window or [Add file](#)

[Import key from clipboard](#)

[Import keys](#)



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

 Mailvelope

Key ManagementEncryptDecryptOptions

Make Mailvelope even more secure by personalizing your security background. [Personalize now](#)

Encrypt data

Recipient

Vishrut.deshmukh@somaiya.edu

Encrypted data is signed with your key (pargat@gmail.com) [Change](#) [Remove signature](#)

Attachments

PNG Ethindia

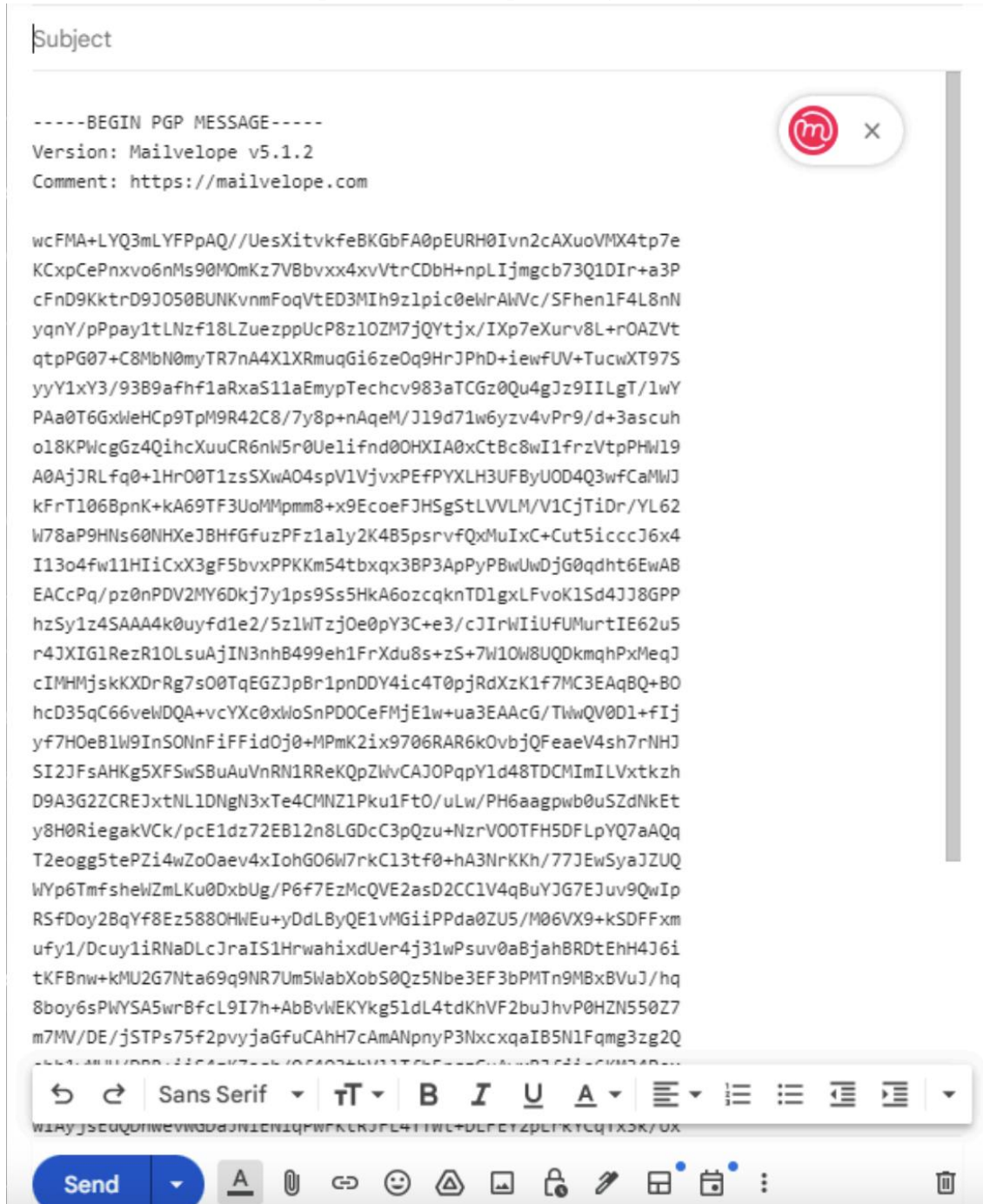
Drag file to this window or [Add file](#)

Message

Hello There!



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering



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



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

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.