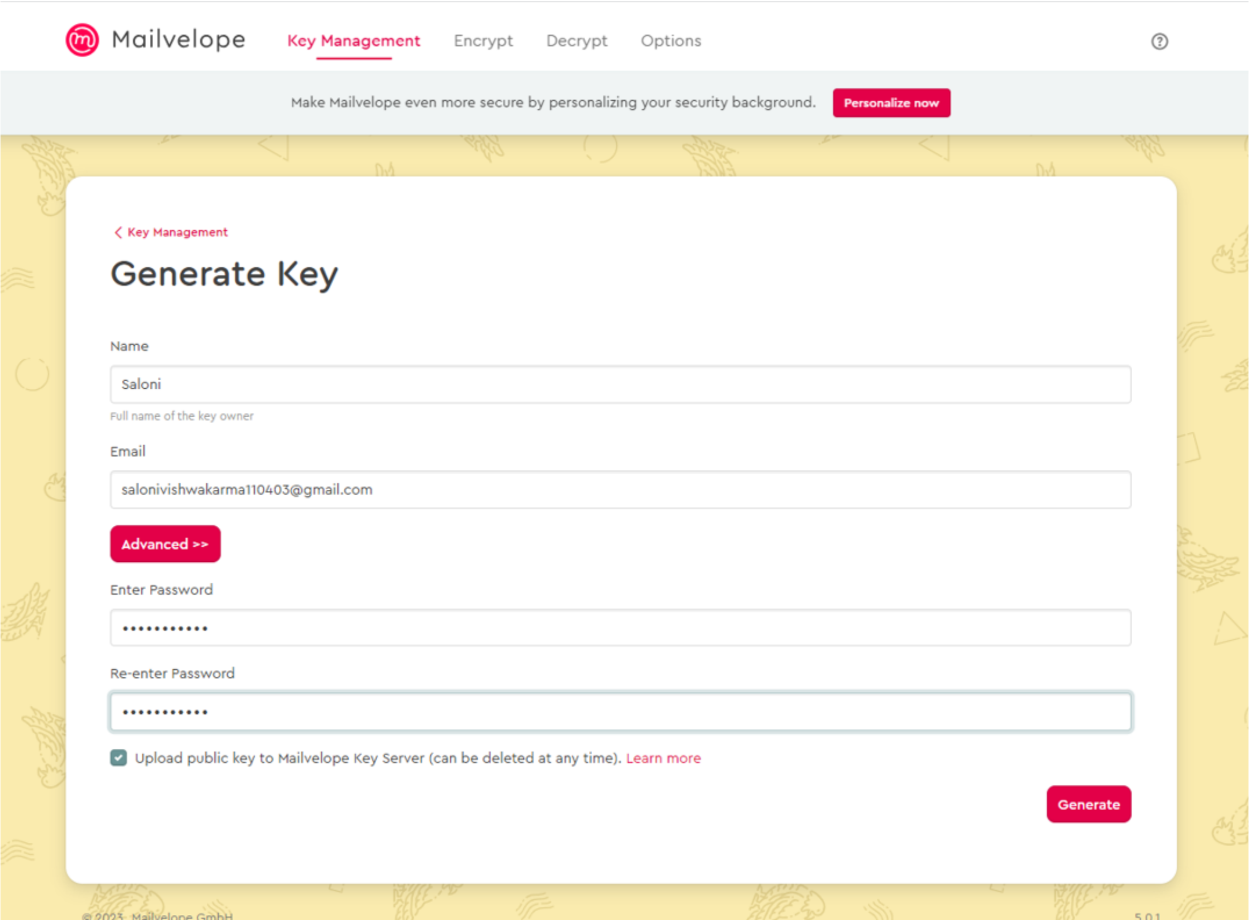
Practical no: 8

Name: Saloni Vishwakarma
Batch-Roll no: C1-13
Subject: Cryptography Lab
Date of execution: 8 July 2023

Aim:

1. Understand the working of PGP
2. Demo of encryption and decryption using Mailvelope (web-based email clients) PGP software.
3. CASE STUDY: Recent attacks, its effects and its counter- measures

Demo of Mailvelope



Make Mailvelope even more secure by personalizing your security background.

Generate Key

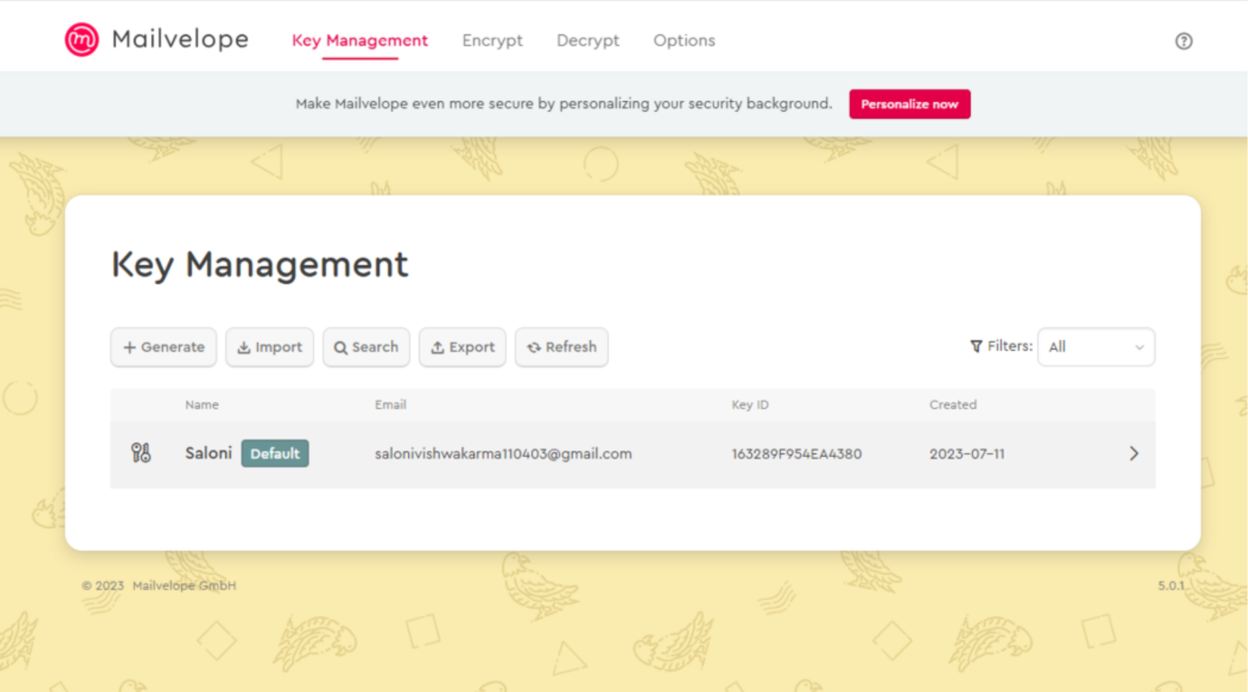
Name: Saloni
Full name of the key owner

Email: salonivishwakarma110403@gmail.com

Enter Password: •••••••••••

Re-enter Password: •••••••••••

☑ Upload public key to Mailvelope Key Server (can be deleted at any time). Learn more



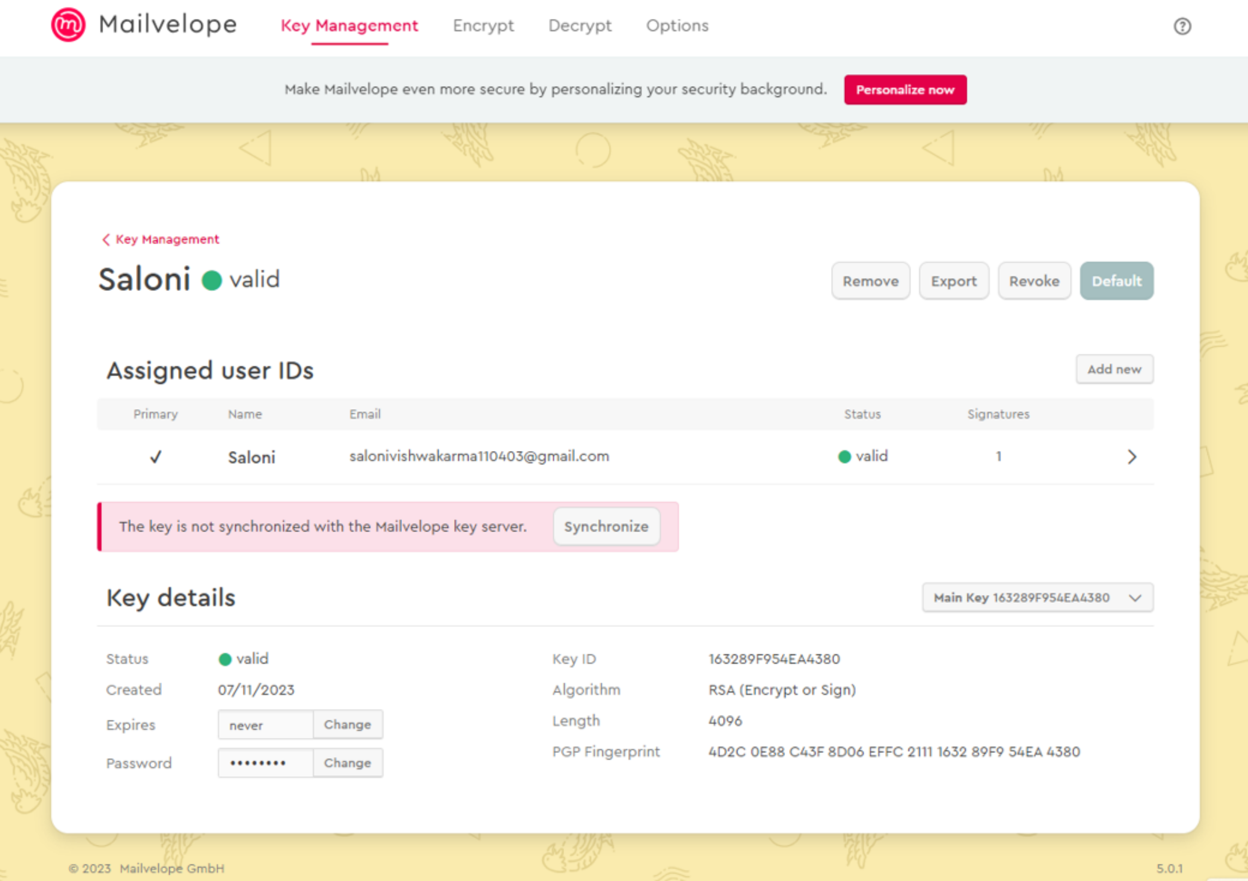
Make Mailvelope even more secure by personalizing your security background.

Key Management

	Name	Email	Key ID	Created
	Saloni Default	salonivishwakarma110403@gmail.com	163289F954EA4380	2023-07-11

© 2023 Mailvelope GmbH

5.0.1



Make Mailvelope even more secure by personalizing your security background.

Saloni ● valid

Assigned user IDs

Primary	Name	Email	Status	Signatures
✓	Saloni	salonivishwakarma110403@gmail.com	● valid	1

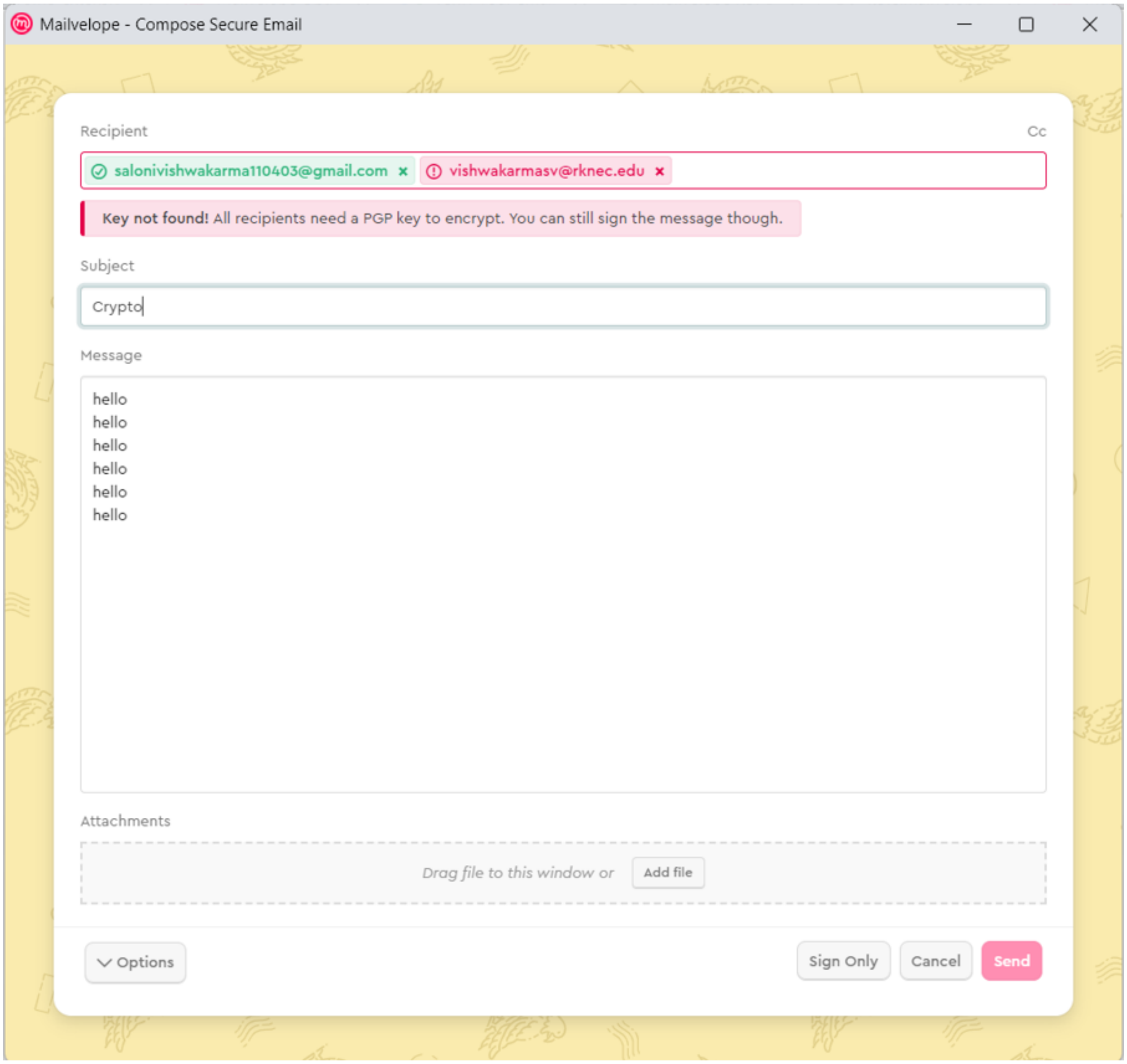
The key is not synchronized with the Mailvelope key server.

Key details

Status	● valid	Key ID	163289F954EA4380
Created	07/11/2023	Algorithm	RSA (Encrypt or Sign)
Expires	never	Length	4096
Password	••••••••	PGP Fingerprint	4D2C 0E88 C43F 8D06 EFFC 2111 1632 89F9 54EA 4380

© 2023 Mailvelope GmbH

5.0.1



Mailvelope - Compose Secure Email

salonivishwakarma110403@gmail.com ×

vishwakarmasv@rknec.edu ×

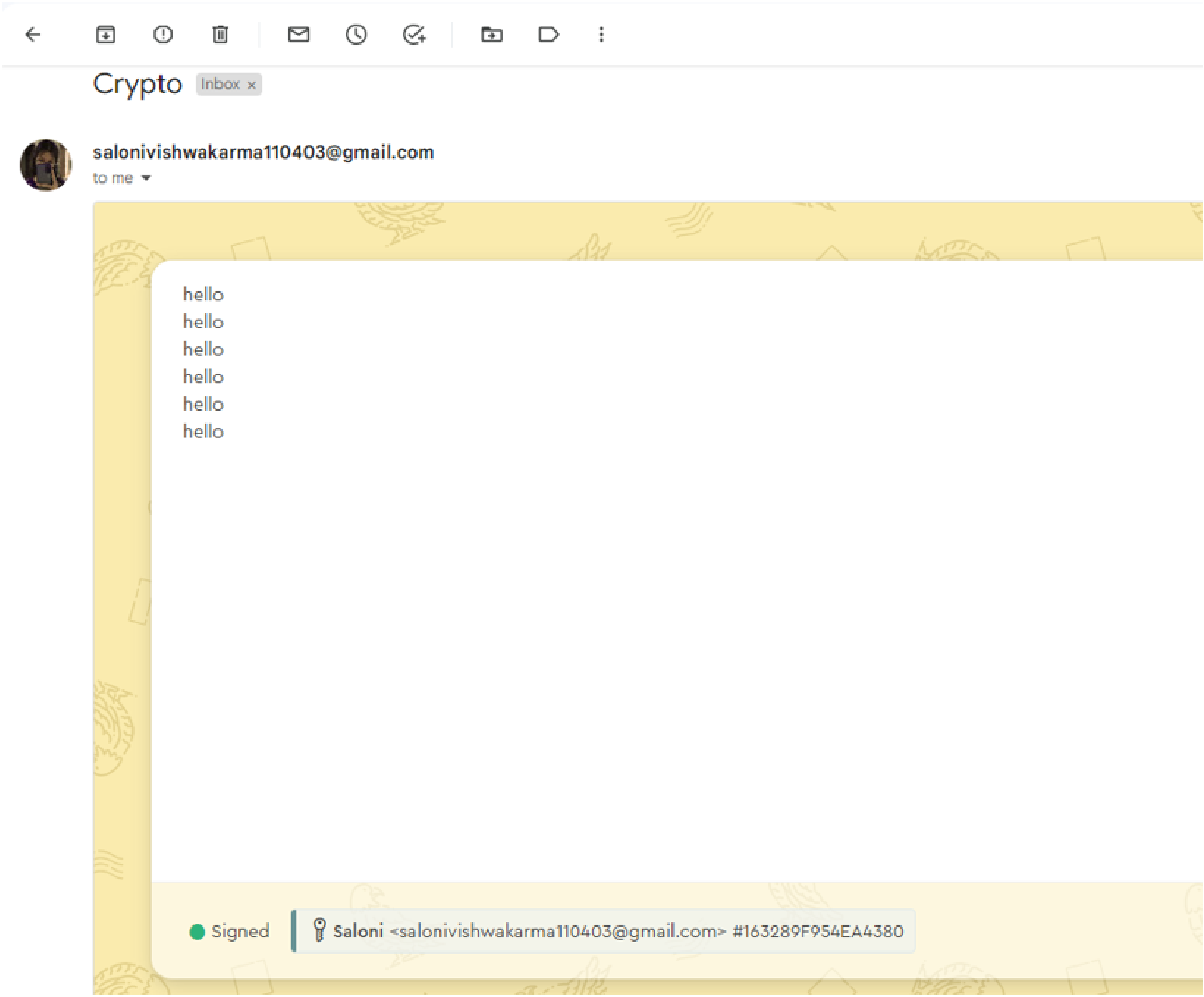
Key not found! All recipients need a PGP key to encrypt. You can still sign the message though.

Subject: Crypto

Message:

hello
hello
hello
hello
hello
hello

Drag file to this window or Add file



Crypto

salonivishwakarma110403@gmail.com

hello
hello
hello
hello
hello
hello

● Signed

Saloni <salonivishwakarma110403@gmail.com> #163289F954EA4380

Case Study:

SolarWinds Supply Chain Attack (2020): The SolarWinds cyberattack, discovered in December 2020, was one of the most significant cyberattacks in recent years. This highly sophisticated attack targeted the software supply chain, compromising the SolarWinds Orion platform used by numerous organizations, including government agencies and Fortune 500 companies. The attack had far-reaching implications and raised concerns about the security of supply chain systems.
The attack involved compromising the software build process of the SolarWinds Orion platform. Threat actors inserted a malicious code, known as Sunburst or Solorigate, into legitimate software updates. When these updates were distributed to SolarWinds customers and installed on their systems, the attackers gained unauthorized access to their networks.

Effects of SolarWinds Supply Chain Attack : The effects of the SolarWinds Supply Chain Attack were significant and widespread. It compromised approximately 18,000 organizations, including government agencies and major corporations, leading to unauthorized access to networks and potential data exfiltration. The attack raised concerns about national security as government systems were compromised, potentially exposing sensitive intelligence and defense information.

Trust in software supply chains was shaken, prompting increased scrutiny and investment in supply chain security. Financially, the incident resulted in substantial losses for affected organizations due to remediation costs and potential legal actions. The attack served as a wake-up call, heightening awareness of supply chain vulnerabilities and emphasizing the need for enhanced cybersecurity measures and information sharing to combat such sophisticated attacks in the future.

Counter measures and Prevention techniques: To prevent and mitigate the impact of a supply chain attack like the SolarWinds incident, organizations can implement several countermeasures and prevention techniques.

These include rigorous vendor management processes to vet and assess software suppliers, ensuring code integrity through secure development practices and regular code review, implementing network segmentation to limit lateral movement within the network, keeping software and systems up to date with timely patch management, educating employees about common attack vectors, implementing multi-factor authentication to enhance access controls, developing and regularly testing incident response plans, and collaborating with industry peers to share threat intelligence.

By adopting these measures, organizations can strengthen their supply chain security, detect and respond to attacks more effectively, and reduce the risk of falling victim to similar supply chain attacks in the future.

Reference: [ChatGPT (openai.com)]

Conclusion: We have successfully understood the working of PGP using the Mailvelope, the PGP software. We have successfully demonstrated the working of the PGP software. We saw how cyber attacks can happen and what we can do in counter to that attack through a Case study.