

Name : Shriram Karpoora Sundara Pandian

Course : CSEC 600 Introduction to Cyber Security

Title : Cryptography

Lab : 2

Chapter : 6

Spell and Grammar Checker is used “ Quillbot Grammar Checker “

Exercise : 6. 01

Apple and FBI case :

In this case, there is a point of view for both parties, and both parties need their goals to be achieved. If the privacy of the iPhone is breached by their own OS, their market share will eventually fall, and they will lose customer trust. At the same time, unlocking the phone of Syed Farook is crucial for the FBI to proceed with other investigations into any attacks or any clues to catch their group, their next plan, the origin of their team, etc. I find this case, as usual, where the debates between tech giants and the government on privacy and keeping the users data safe are apples to apples, but sometimes the government asks Facebook if it knows and monitors the users data and location regularly and how it becomes a privacy issue for users. In the case of Apple, it is known for its privacy, and some people argue it is more secure than Android, and I think Apple wants to save its reputation that it has built for years. From would say point of view of both parties, I would not siding with any one side. Because the FBI wants to know the details, which are crucial for the safety of the public, whereas Apple wants to keep privacy, which is also crucial for the safety of customers.

I also think people debate sometimes in a biased way or with temporary emotion rather than thinking for the future. For example, people who debated or said Apple should unlock the device may not have thought of the consequences of doing so and how it may affect iPhone users later. The FBI wanted Apple to create GovOS, which may completely destroy the privacy and reputation Apple has built over the years if somebody gets access and uses it maliciously. In this case, I think in this way, which always happens in the Android world and all Android users may not be aware of

sometimes, which is Vault apps and other rooted apps, Android gives you a lot of flexibility, and these vault apps make it possible for users to utilize YouTube and YouTube Music, Spotify, and other paid apps for free. But who knows what happened in the back of the code? To make the app free, developers should crack the application and remove the subscription feature or make it unlimited, but there is also a possibility that developers may include backdoors or add some malicious code, which may cause or have a passive attack on users using the application, so flexibility always comes with a price. IOS keeps their apps strict and paid, and I support Apple in this case as they wanted to protect their reputation and their users privacy, which is best for both. Anyway, the FBI cracked the phone, which is good news too. As the FBI reported, they opened the phone with the help of Israeli firm Cellebrite, and the company did not say anything about whether they did or not. I think sometimes it is premature for the FBI to say that they don't need the help of Apple anymore.

Exercise : 6. 02

Australia rules and claims :

Terrorists and other illegal activities need covert channels for communicating, so WhatsApp and many social media platforms give end-to-end encryption, which uses public key encryption, and only end-point devices are able to encrypt the data I got information from Google." I would say it depends. For example, if we have a knife, "we can use it for cutting vegetables," which is a good thing, "we can also threaten others using that." So using the technology responsibly is key. But what manufacturers of knives can do for their job is sharpen it; they can't modify it for different people. Same it goes, and I think if Australia wants to pass those laws and thinks the law of Australia is a law it follows ", they should act like China and other countries that have their own social media and not allow Google or Facebook into

their country. That's the right approach if they want something they need, especially based on a network to track down criminals or other activities. Companies can't break their policy of protecting customers from encryption. Because it's just a move that will breach the whole network of Apple or Facebook if they try to create an access or backdoor, especially for the government, which will later affect the whole crowd. I find a similar case in blockchain, or I would say it is the origin of everything that started. For example, the Tor network and the blockchain network were created for users rights to privacy and anonymity; some people called it Web 3.0, which offers privacy. But it became the best tool for illegal contracts and money transfers; even terrorists use those networks. Designing something special to have control over anything helps sometimes, and that should be the research others or tech developers do. At least I will try to do research about it, and it will become my favorite topic to keep privacy, and at the same time, it is true that we should have a government to stop those illegal and dangerous activities. We can't blame anything other than technology. So even though technology offers privacy and other things to the common user, It should be responsible enough to protect others too. That is my take on these cases, both the Apple debate with the US government and the laws being passed by Australia to keep a check on activities that happen online. As technology is getting developed day by day, at the same time, it should have some checks on activities that are not under its control. The brands like Apple and Facebook sell their services in the name of privacy, which may later be exploited by bad guys. So I feel it's a story of acting responsibly and making use of it properly. This is how I conclude this by studying those articles from my point of view.

Exercise : 6. 03

To serve man :

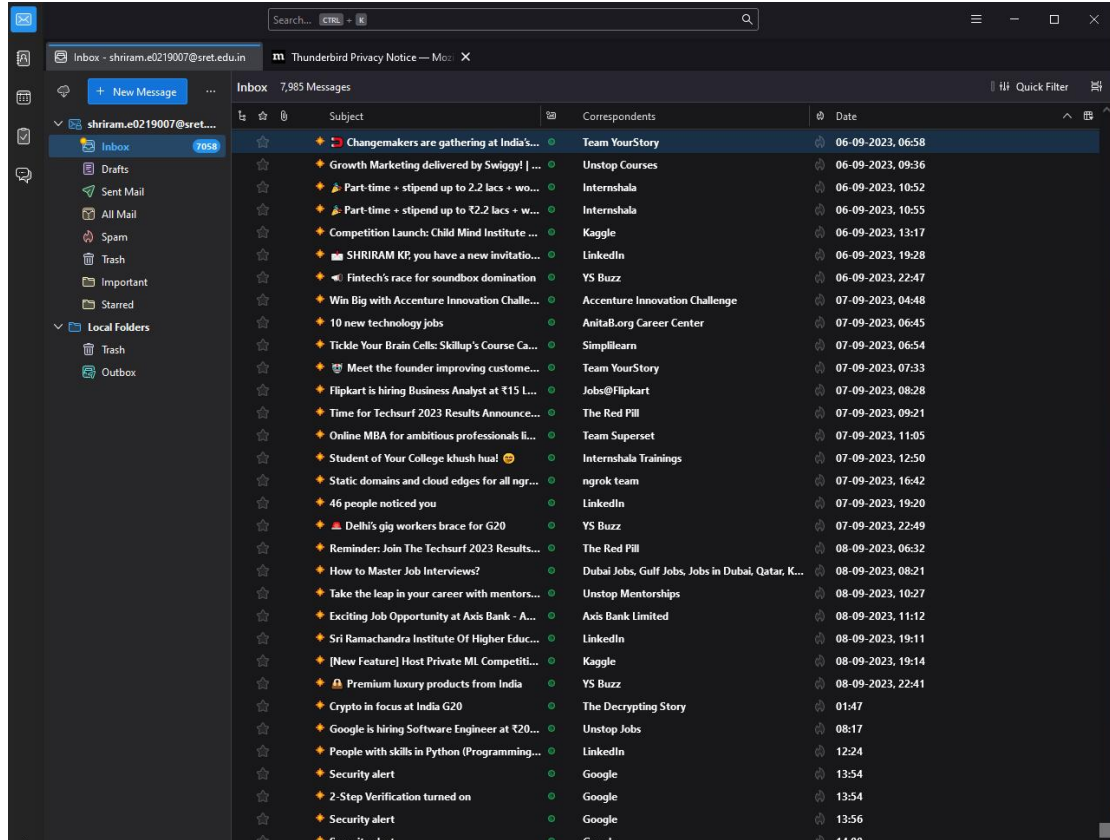
It is great knowing that these kinds of series and sci-fi existed in the 1900s, and the direction was very good knowing it was filmed 60 years ago. In my point of view, the theme of cryptography exists in the essence of the story of this episode specifically. When kanamites arrived on earth and wanted to help humans by helping them fight famine and stop wars so they could save humans, they gained the trust of humans that this was their true intention, which happens in cryptography too. We try to trust the cryptography algorithm and its key because it offers better protection for our data. Then aliens gave us the book called "To Serve Man, which we fellow humans thought was their way of serving us, which was clearly not the case when this book got decoded. What this meant was that the book is a cookbook, which eventually relates to cryptography in that the message we see is not original and has another hidden meaning to it; we see ciphertext as the original message, but the original message is something else. This way of looking at it fascinates me because the day-to-day things we see and try to understand are not the way they are and are not true either. I got reminded of this thought: Witnessing something may be wrong, and what you hear might be wrong too; analyze it deeply and look for other reasons that may establish the real truth, which is a strong foundation of cryptography, I think. In cryptography, if we want to test the strength of the algorithm or add more protection to it, we need to open it to the public and get rigorous testing to determine whether it withstands the attack or real-time compromises. Like when suddenly aliens arrived on earth and showed a lot of kindness, instead of taking it as a benefit or help, people should have felt suspicious and looked more into it to ask questions like why they chose earth. Why suddenly should they help, and what benefits do they get from helping us? Is it

really that they want to help and so much more, which will give us a clear understanding and the idea that they came with a particular intention and that they want us as a meal? That is why they are trying to protect us and feed us so that they can eat well. Therefore, we should analyze the situation with a series of questions to understand it well, just like algorithms go through a series of tests and simulation attacks to know whether they can withstand them or not. As we saw in the above articles, technology and cryptography can be used to protect us but also have the ability to go against us, which is how aliens can develop us or either eat us entirely. So each situation has different meanings and sides.

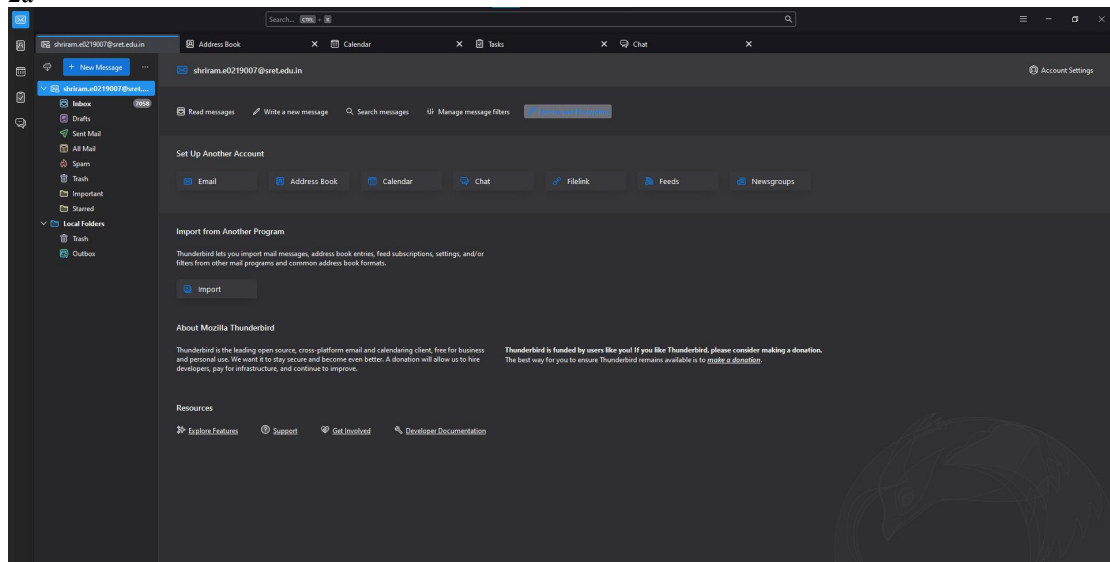
Exercise : 6. 04

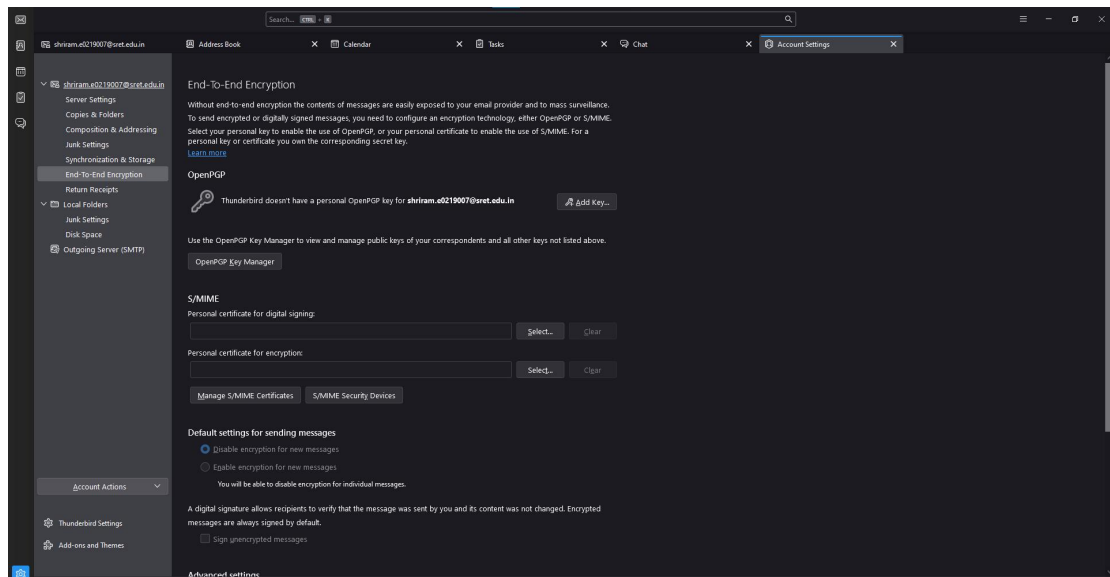
6. 04 Thunderbird assignment screenshots :

1j



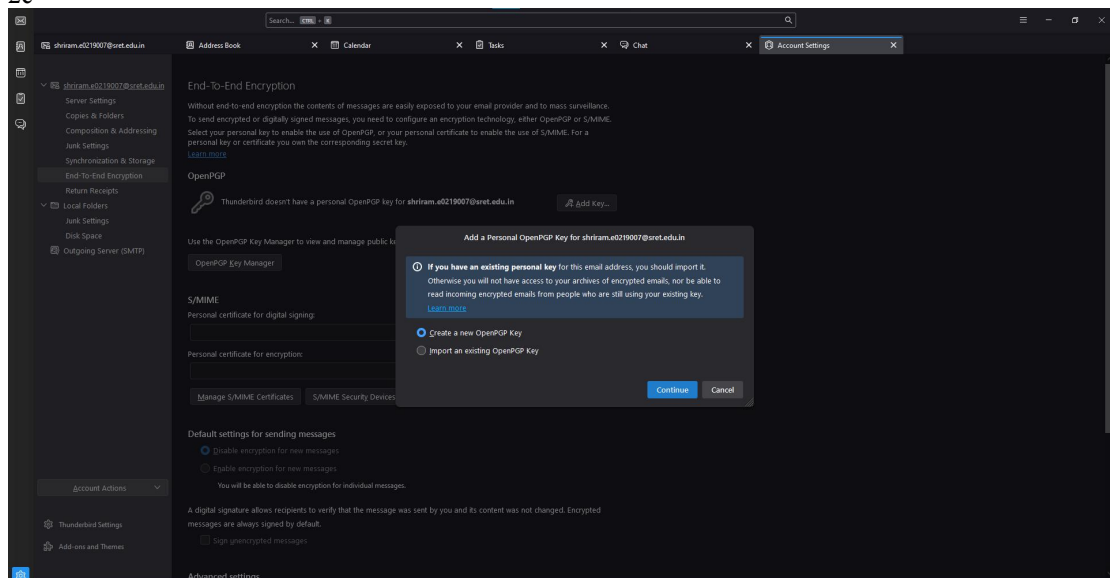
2a

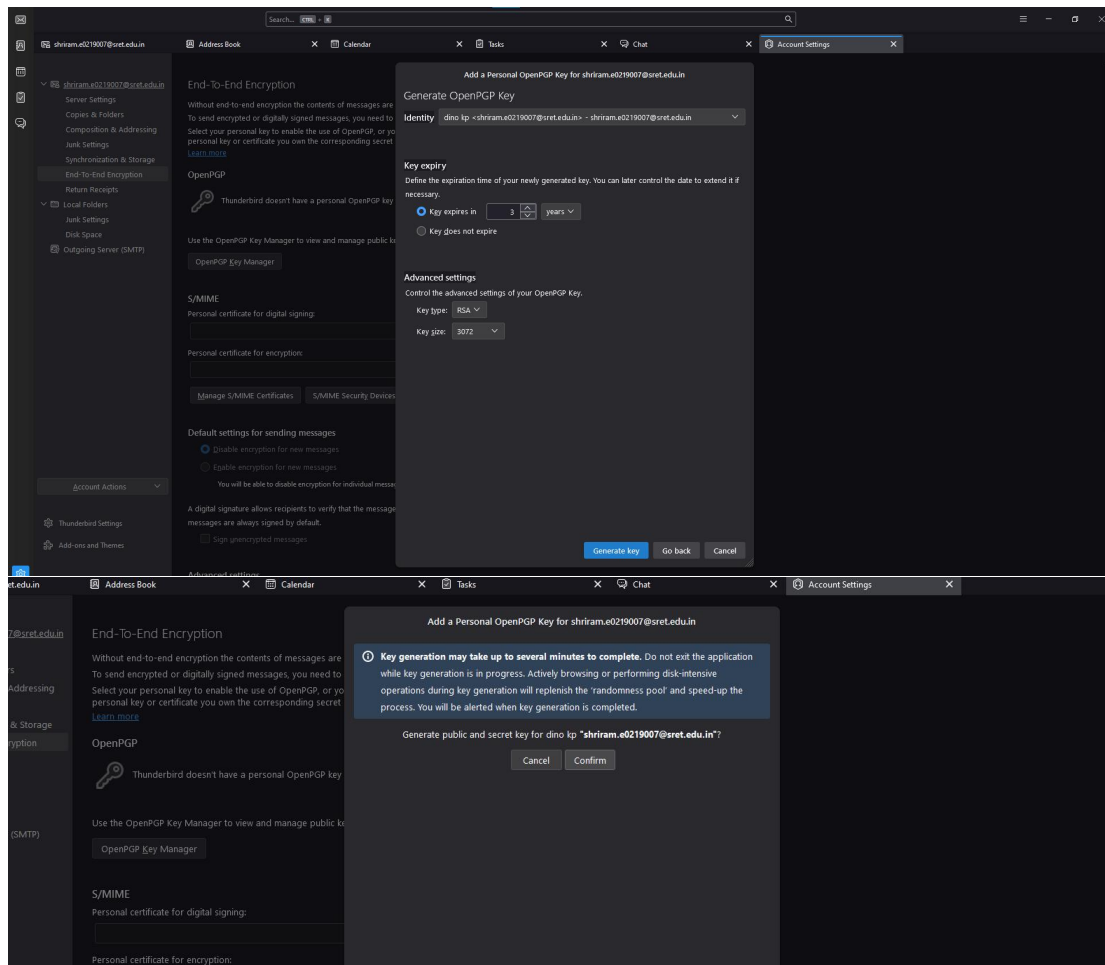




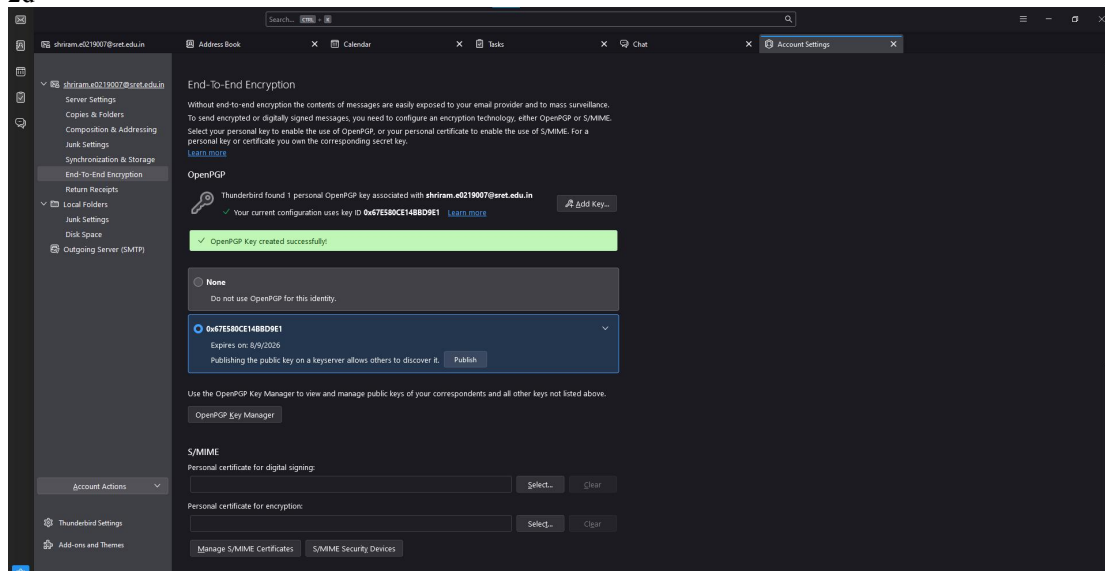
2b

2c





2d



2e

Key Properties

Claimed Key Owner

dino kp <shriram.e0219007@sret.edu.in>

Type

key pair (secret key and public key)

Key ID

0x67E580CE148BD9E1

Fingerprint

B827 2E24 8526 D32E 7F8C DD2F 67E5 80CE 148B D9E1

Created

9/9/2023

Expiry

8/9/2026

Refresh Online

Change Expiration Date

Your Acceptance

Certifications

Structure

For this key, you have both the public and the secret part. You may use it as a personal key. If this key was given to you by someone else, then don't use it as a personal key.

☐ No, don't use it as my personal key.
 ☒ Yes, treat this key as a personal key.

OK Cancel

Change Key Expiration

ⓘ

After a key expires, it's no longer possible to use it for encryption or digital signing.

This key is currently configured to expire on 8/9/2026.

To use this key for a longer period of time, change its expiration date, and then share the public key with your conversation partners again.

☒ Do not change the expiry date
 ☐ Key will expire in:

in 3 years

☐ Key will never expire

OK Cancel

2f

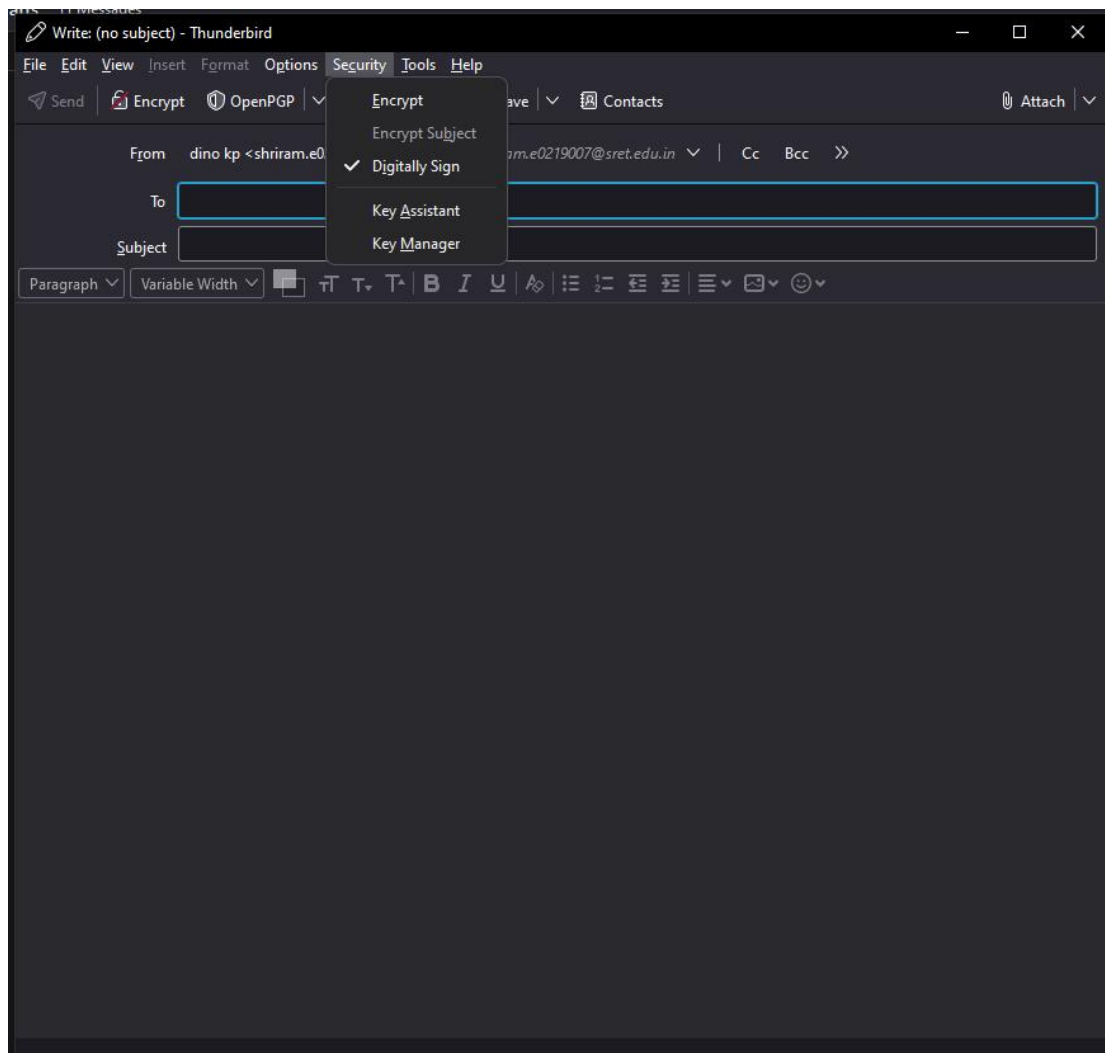
Default settings for sending messages

☒ Disable encryption for new messages
 ☐ Enable encryption for new messages

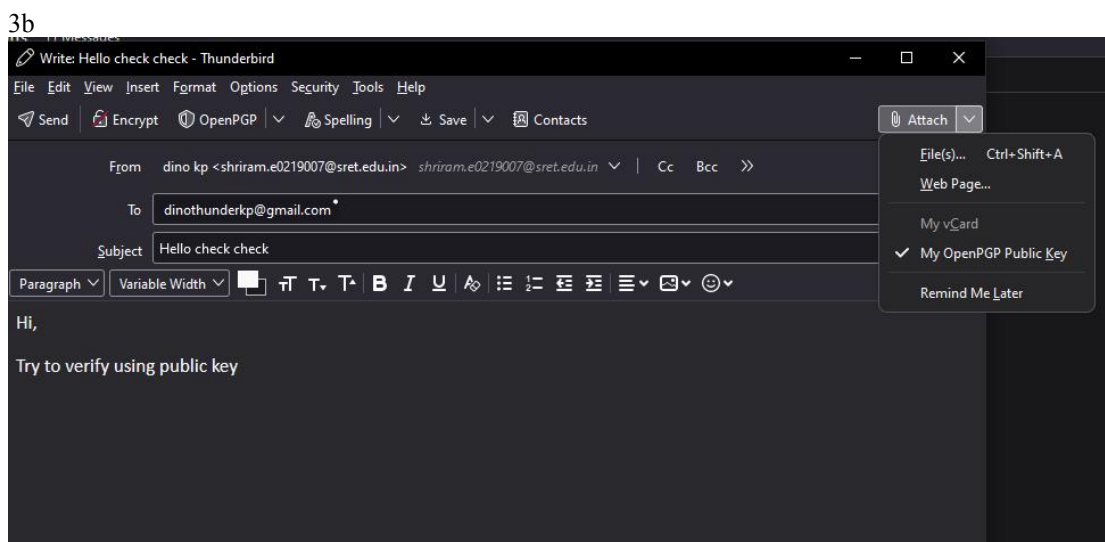
You will be able to disable encryption for individual messages.

A digital signature allows recipients to verify that the message was sent by you and its content was not changed. Encrypted messages are always signed by default.

☐ Sign unencrypted messages



3a



3b

4a



Seathy Ragupathy

seathy.r0119023@set.edu.in

Reply

Forward

Archive

Junk

Delete

More

14:30

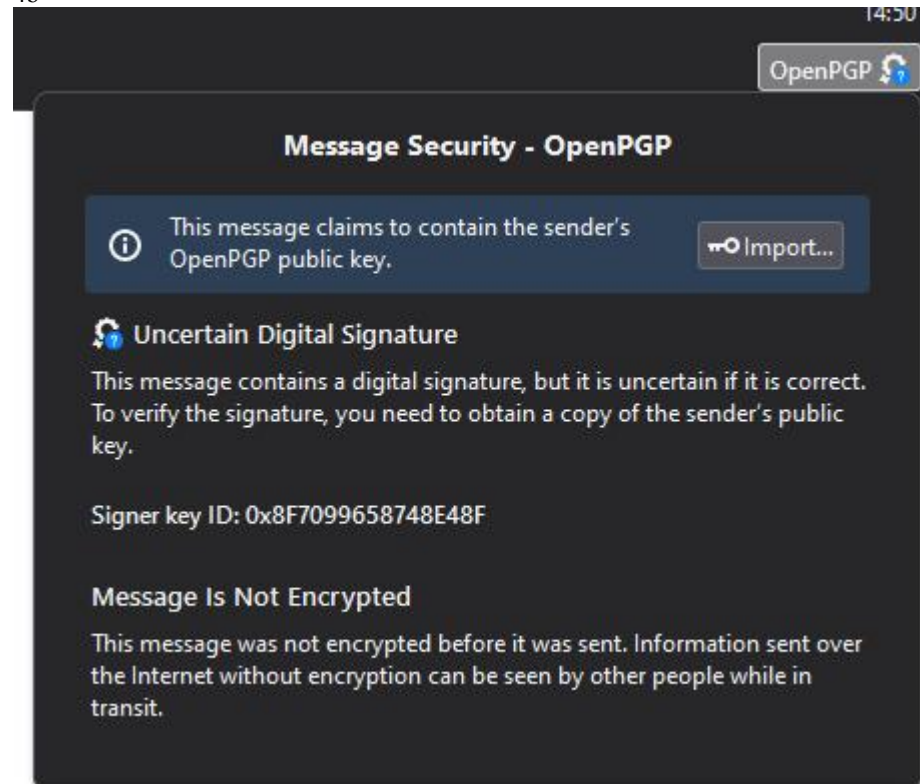
To: Me

check

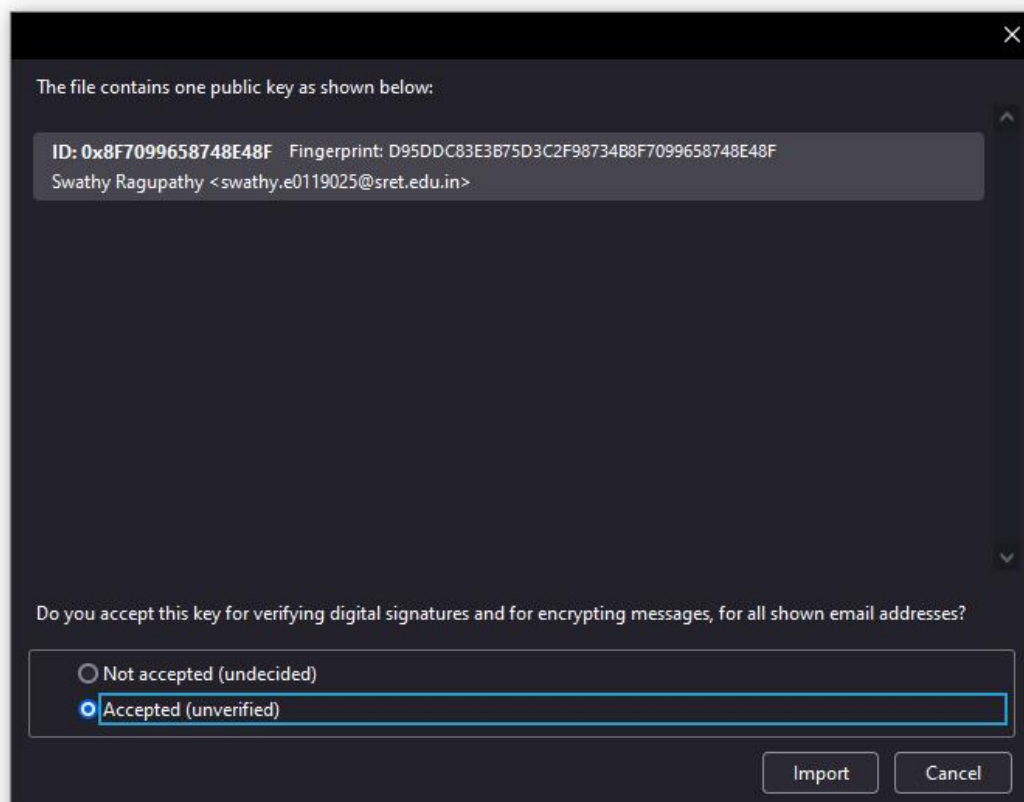
OpenPGP

hi.....

4b



4c



4d

Key Properties

Claimed Key OwnerSwathy Ragupathy <swathy.e0119025@sret.edu.in>

Typepublic key

Key ID0x8F7099658748E48F

FingerprintD95D DC83 E3B7 5D3C 2F98 734B 8F70 9965 8748 E48F

Created9/9/2023

Expiry8/9/2026

Refresh Online

Your Acceptance

Certifications

Structure

Do you accept this key for verifying digital signatures and for encrypting messages?

☐ No, reject this key.

☐ Not yet, maybe later.

☒ Yes, but I have not verified that it is the correct key.

☐ Yes, I've verified in person this key has the correct fingerprint.

Verify the fingerprint of the key using a secure communication channel other than email to make sure that it's really the key of swathy.e0119025@sret.edu.in.

OK

Cancel

4e

14:50

OpenPGP

Message Security - OpenPGP

Good Digital Signature - Signed on 09-09-2023, 14:50

This message includes a valid digital signature from a key that you have already accepted. However, you have not yet verified that the key is really owned by the sender.

Signer key ID: 0x8F7099658748E48F

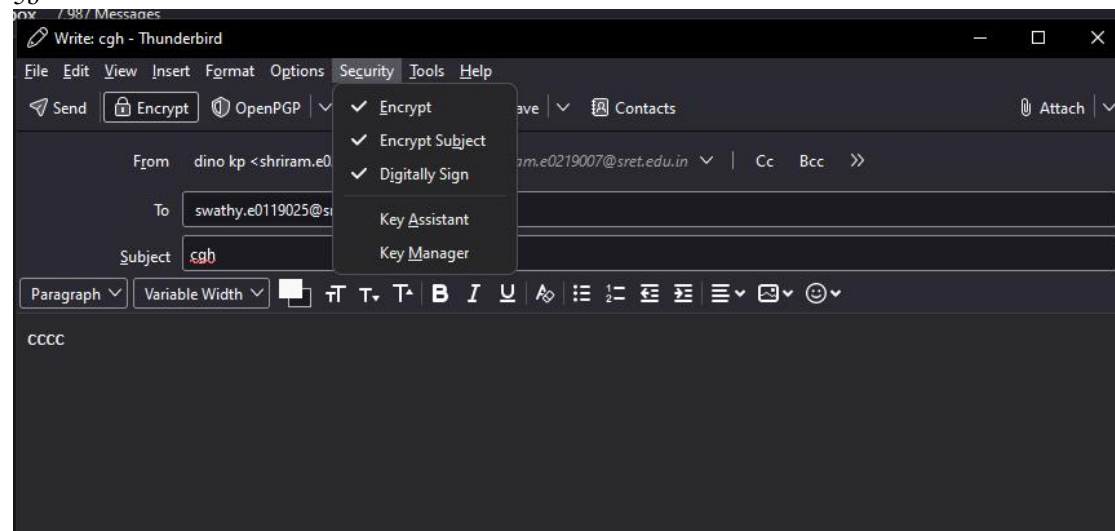
View signer key

Message Is Not Encrypted

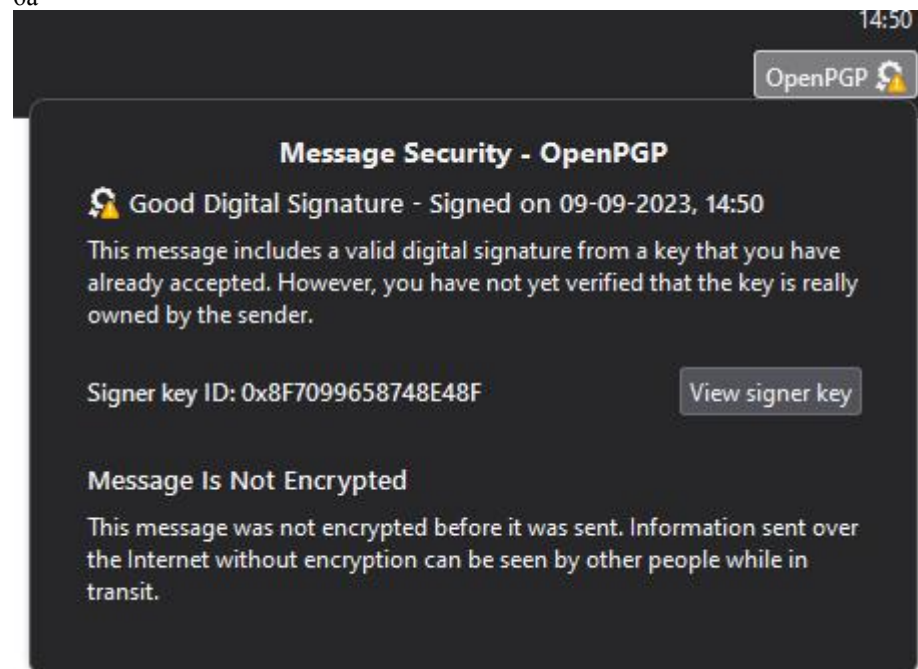
This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

5a

5b



6a




6b


15:03

OpenPGP

Message Security - OpenPGP

 **Good Digital Signature**
This message includes a valid digital signature from your personal key.

Signer key ID: 0x67E580CE14BBD9E1 [View signer key](#)

 **Message Is Encrypted**
This message was encrypted before it was sent to you. Encryption ensures the message can only be read by the recipients it was intended for.

Your decryption key ID: 0x67E580CE14BBD9E1 (Sub key ID: 0x95882034753162DC) [View your decryption key](#)

The message was encrypted to the owners of the following keys:

Swathy Ragupathy <swathy.e0119025@sret.edu.in>
0x8F7099658748E48F (0xFE39857FEB35AB4)

6c

 **Swathy Ragupathy**
to me ▾

2 Attachments • Scanned by Gmail ⓘ

[↩ Reply](#)[➦ Forward](#)

7.

a. Viewing the email is better in thunderbird which has unique design and shows all the content well. One thing i noticed that the public key and digital signature is shown at gmail whereas the signature and other signing process happens automatically here.

b. I am encrypted my email using the session key which is generated by the thunderbird

c. My session key will be encrypted using public key of my partner and i will send the session key to partner and he or she decrypt the session key using their private key.

d. After decrypting the session key using private key, they will decrypt the email using session key.

e. The session key is decrypted by the private key of the partner.

f. To ensure the security, also in my opinion as the symmetric is fast and asymmetric is slow, the message is encrypted and decrypted by symmetric and key is using asymmetric which will also increase the protection.

g. I signed using the private key

h. My parter used by public key to verify it.

i. It is achieved by using both asymmetric and symmetric encryption.

j. Using digital signatures concept we ensured integrity.

k. As we are using digital signatures we can confirm and ensure the non repudiation.

Lab analysis

1. My takeaway is that apple cant compromise their security for keeping their users safe and ensuring privacy whereas government got what they wanted, but government cant modify policy as they wish for.

2. I think the law passed by Australia is long debate and if they want their needs they should setup their own channel and networks like china and turkey, rather than implying and trying to access other organization data through backdoors.

3. Always decrypt the message and look for the answer rather than looking into cyphertext which is "To serve man" is not helping humans, is helping them gain weight and later become meal for aliens.

4. Sure i will use encrypted mail for sending confidential documents and personnel moments, not necessary to use for all the emails, as following through steps, some people may find time consuming and unnecessary protection. So security and convenience should be balanced.

Key term Quiz

1. Encrypt
2. Backdoor
3. decrypt
4. Hash