LAB04
S/MIME and OpenPGP

1. Write a brief report of what you have done. In the report, include your OpenPGP key ID and signature. (Your public key will be downloaded from http://pgp.mit.edu/ or https://keys.openpgp.org and checked for signatures.) Also, answer the question below: Can you send signed/encrypted emails using webmail such as Gmail? Why, or why not? What are the challenges?

The task was to do the encryption and signing of the email using S/MIME and OpenPGP while sending the emails. This is done to have a safe and secure communication.

Steps for S/MIME

1)Configure the name server on both client and server machines
2)Install evolution on the client machine then configure the exchange email using IU email.
3)Create PK12 certificate following the steps given
4) Now we can send email by selecting the required options

Steps for PGP

1)Install seahorse
2)Create a pgp key
3)Import certificate onto evolution and create .cer file
4)Sign and encrypt the file
Mail Accounts -> abkuma@iu -> Edit -> Security -> Now paste the key in OpenPGP Key ID tab : 3BB2344.....(Key to be copied)

5)Asked my friends to generate their asc key and send it to me
gpg --export --armor --output <key_name.asc> <email_id>

Also I sent my asc key to my friend. After that I send the PGP signed / encrypted email.

1)First import the friends key

gpg --import <.asc file>

It will say impoted

2)Second check the list of keys. It shows all the keys with respective emailId and Key

gpg --list-keys

3)Now sign this key of your friend

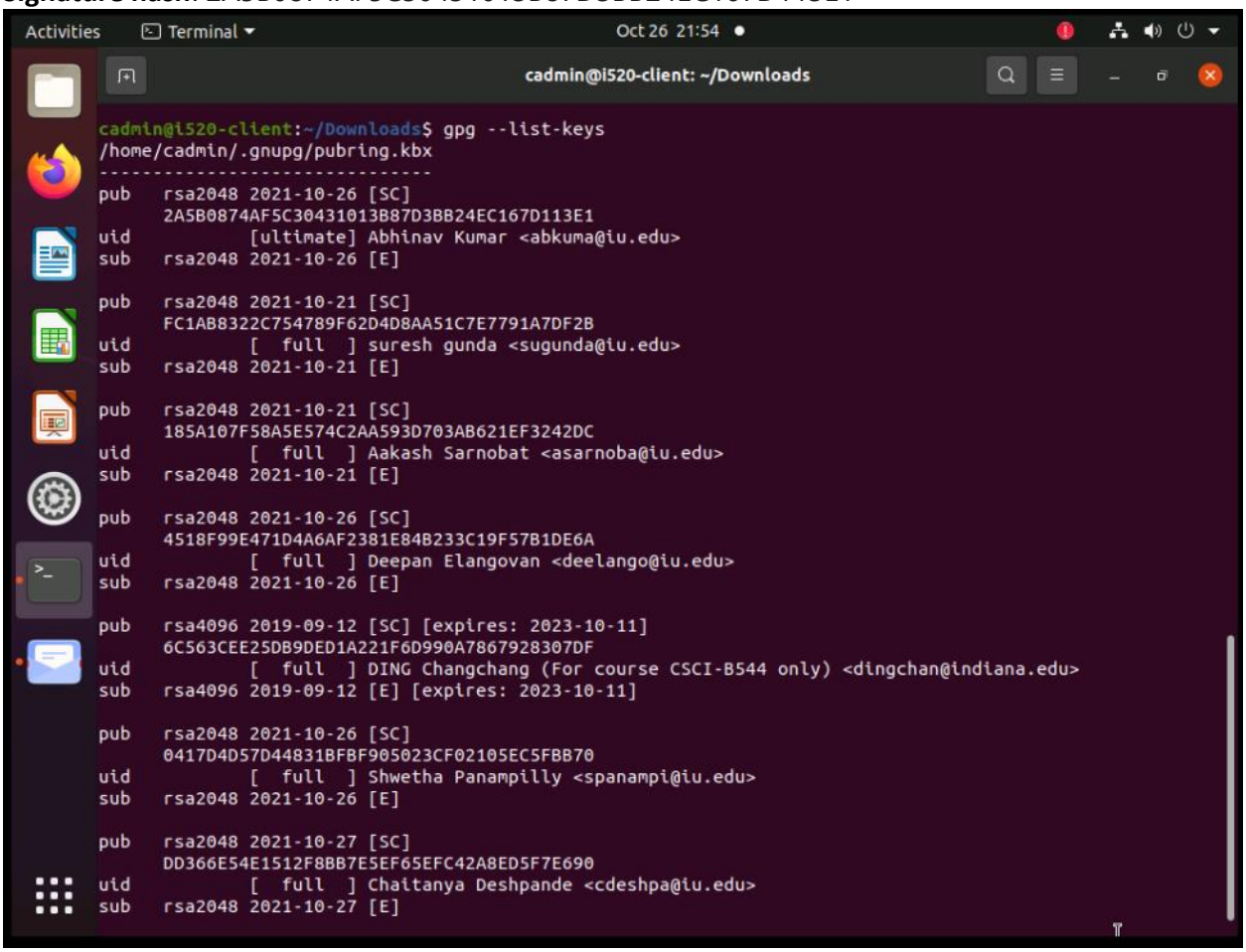
gpg --sign-key <KEYS COPY from the list>

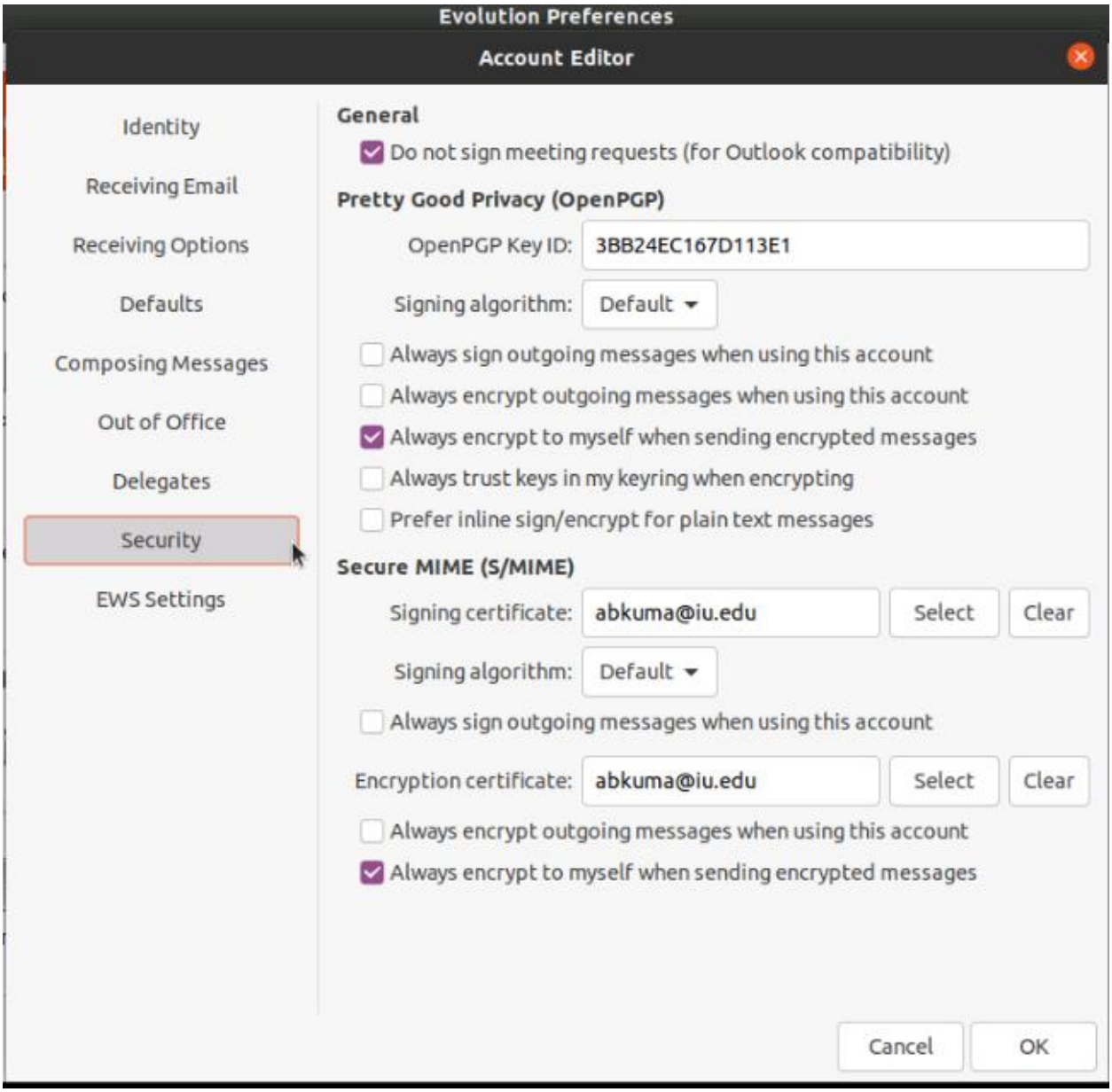
It will ask do u want to sign this key with your key?
Press y and enter

6) Download the AI key and do the same steps as done for friends.

OpenPGP Key ID: 3BB24EC167D113E1

Signature hash: 2A5B0874AF5C30431013B87D3BB24EC167D113E1





Can we do the same using Gmail?

Yes, we can send singed/encrypted email using Gmail but there is difficulty to tweak the required configuration. We need an enterprise account to sign and encrypt using S-MIME/ PGP.
As per the gnome evolution website, we can send signed and encrypted emails via Gmail, but we are required to buy the third-party certificates

2. Explain what the key fingerprint is (mentioned in 3.2.1) and why you are convinced that

this key is indeed Changchang's? Your argument should clearly indicate what properties of secure hash functions are important in making the decision.

Key Fingerprint: It is a short sequence of bytes used to identify a longer public key. Fingerprints are created by applying a hash or Key ID to identify the owner's identity.
I was able to verify the key's owner by checking the provided Hash and also, I have verified the email and the full name.

So, the unique mapping or collision resistance is one of the features of a secure hash function. Under which each fingerprint should be linked to just one public key. The fingerprint is unique for a public key. Therefore, it helps in verifying keys.

-