

Nama : Asyrof Hafizh Maulana

CRYPTOGRAPHY

1. Memanfaatkan tools Cryptography dalam menerapkan prinsip privacy, confidentiality dan Integrity menggunakan Tandatangan digital PGP pada Email menggunakan Mail Client Thunderbird dengan Plugin PGP (GnuPG), Anda diharapkan dapat

- Membuat pasangan kunci PGP (Public Key dan Private Key)
- Mengupload Publik Key ke Public Key Server (<https://keys.openpgp.org/>)
- Mengirim dan Menerima Email Bertandatangan Digital
- Mengirim dan Menerima Email dengan Pesan terenkripsi menggunakan PGP
- Mengirim dan Menerima Email dengan Attachment Terenkripsi menggunakan PGP

Anda dapat mengirim email contoh kepada teman anda, atau email anda yang lain atau ke email josh@ugm.ac.id (Cari kunci public email tersebut di <https://keys.openpgp.org/> dan download/simpan/import ke PGP Manager anda) agar Anda dapat mengirimkan email terenkripsi ke email tersebut.

Tunjukkan hasil melalui screenshoot dan jelaskan syarat masing masing proses pengiriman email pada tugas c, d, e diatas agar berhasil.

A:

- Install Thunderbird
- Setup email :


- Pilih configurations :


✓ Configuration found in Mozilla ISP database.


Available configurations

☐ IMAP
Keep your folders and emails synced on your server

☒ POP3
Keep your folders and emails on your computer

 Incoming **POP3** **SSL/TLS**
pop.gmail.com

 Outgoing **SMTP** **SSL/TLS**
smtp.gmail.com

 Username
asyrof.hafzh@students.utdi.ac.id

[Configure manually](#) Cancel Done

- ⓘ Thunderbird is free and open source software, built by a community of thousands from all over the world.

- Selanjutnya ke End-To-End Encryption lalu add key :

ⓘ **If you have an existing personal key** for this email address, you should import it.
Otherwise you will not have access to your archives of encrypted emails, nor be able to read incoming encrypted emails from people who are still using your existing key. [Learn more](#)

☒ Create a new OpenPGP Key

☐ Import an existing OpenPGP Key

Continue Cancel

➤ Generate OpenPGP Key :

Generate OpenPGP Key

Identity Asyrof Hafizh Maulana <asyrofhafizhmaulana@gmail.com> - asyrofhafizhmaulana@gmail.com

Key expiry

Define the expiration time of your newly generated key. You can later control the date to extend it if necessary.

- ☒ Key expires in years
- ☐ Key does not expire

Advanced settings

Control the advanced settings of your OpenPGP Key.

Key type:

Key size:

Generate key

Go back

Cancel

➤ Konfirmasi :

i Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.

Generate public and secret key for Asyrof Hafizh Maulana "**asyrofhafizhmaulana@gmail.com**"?


Cancel

Confirm

- OpenPGP Key sudah dibuat :


OpenPGP

Thunderbird found 1 personal
OpenPGP key associated with

**asyrofhafizhmaulana@gmail.com**

✓ Your current configuration uses
key ID **0xAF5B778B414F6B7B**

[Learn more](#)

 Add Key...

✓ OpenPGP Key created successfully!

☐ **None**

Do not use OpenPGP for this identity.

☒ **0xAF5B778B414F6B7B** 

Expires on: 10/12/2027

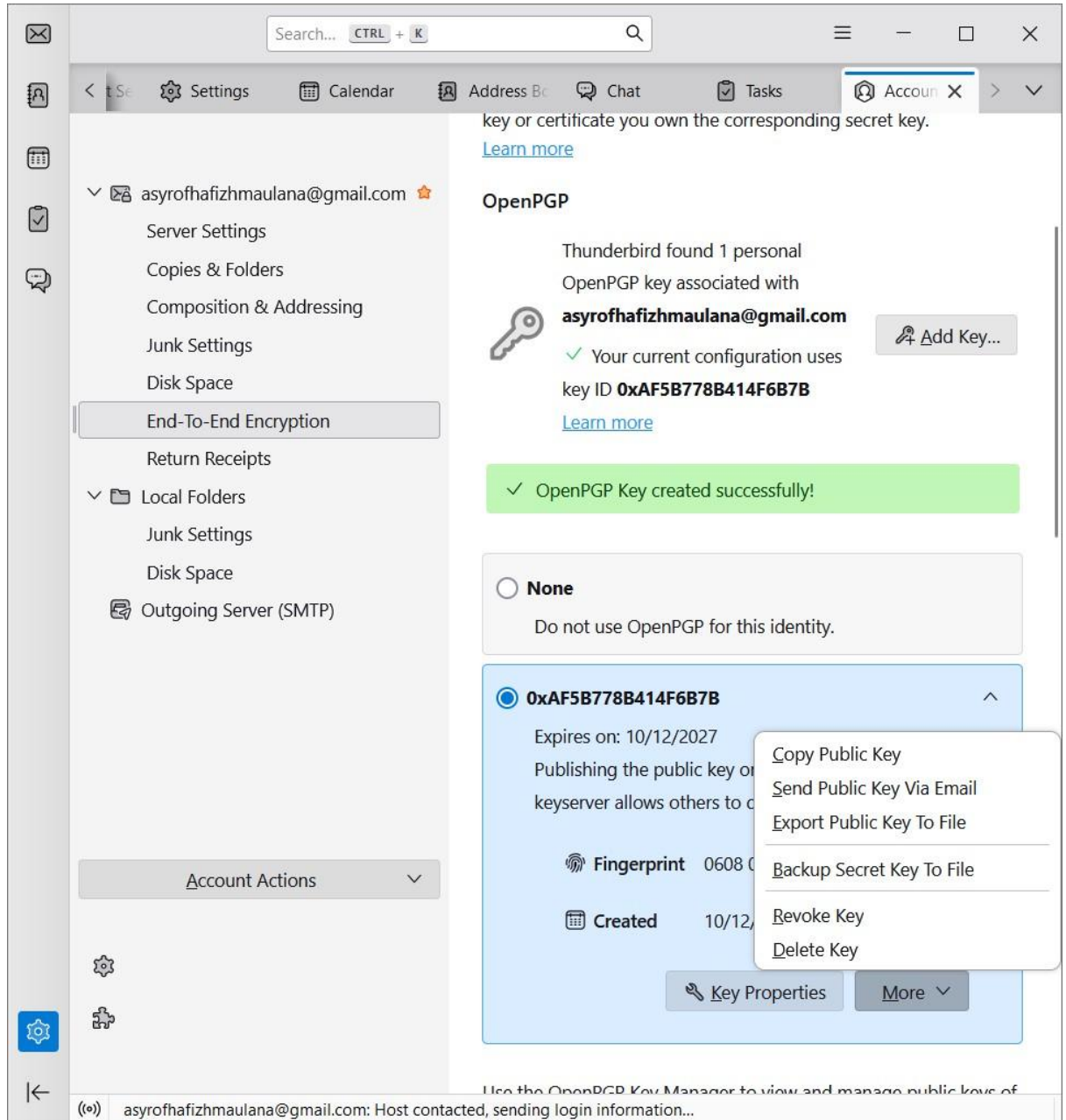
Publishing the public key on a
keyserver allows others to discover it.

Publish

Use the OpenPGP Key Manager to view and manage public keys of
your correspondents and all other keys not listed above.

OpenPGP Key Manager

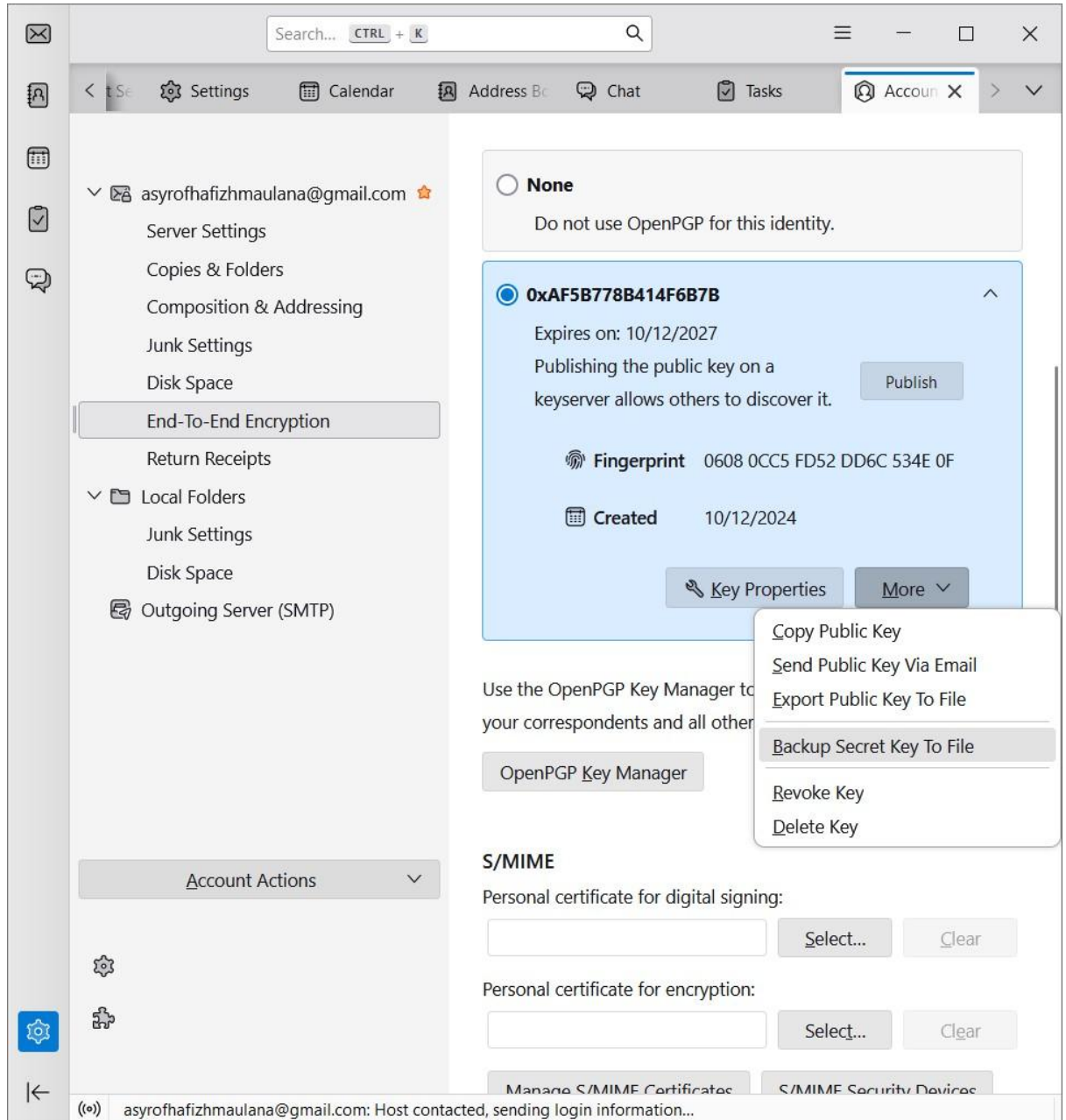
- Setelah itu klik more dan pilih export public key :



- Pembuatan public key berhasil :

File name:	Asyrof Hafizh Maulana_asyrofahfizhmaulana@gmail.com-0xAF5B778B414F6B7B-pub
Save as type:	ASCII Armored Files (*.asc)

- Setelah itu export lagi untuk secret key nya :



- Masukkan password untuk secret key :

Choose a password to backup your OpenPGP Key

The password you set here protects the OpenPGP secret key backup file that you are about to create. You must set this password to proceed with the backup.

Choose a Password

Secret Key backup password:

Secret Key backup password (again):



Password quality meter

Important! If you forget your secret key backup password, you will not be able to restore this backup later. Please record it in a safe location.

OK

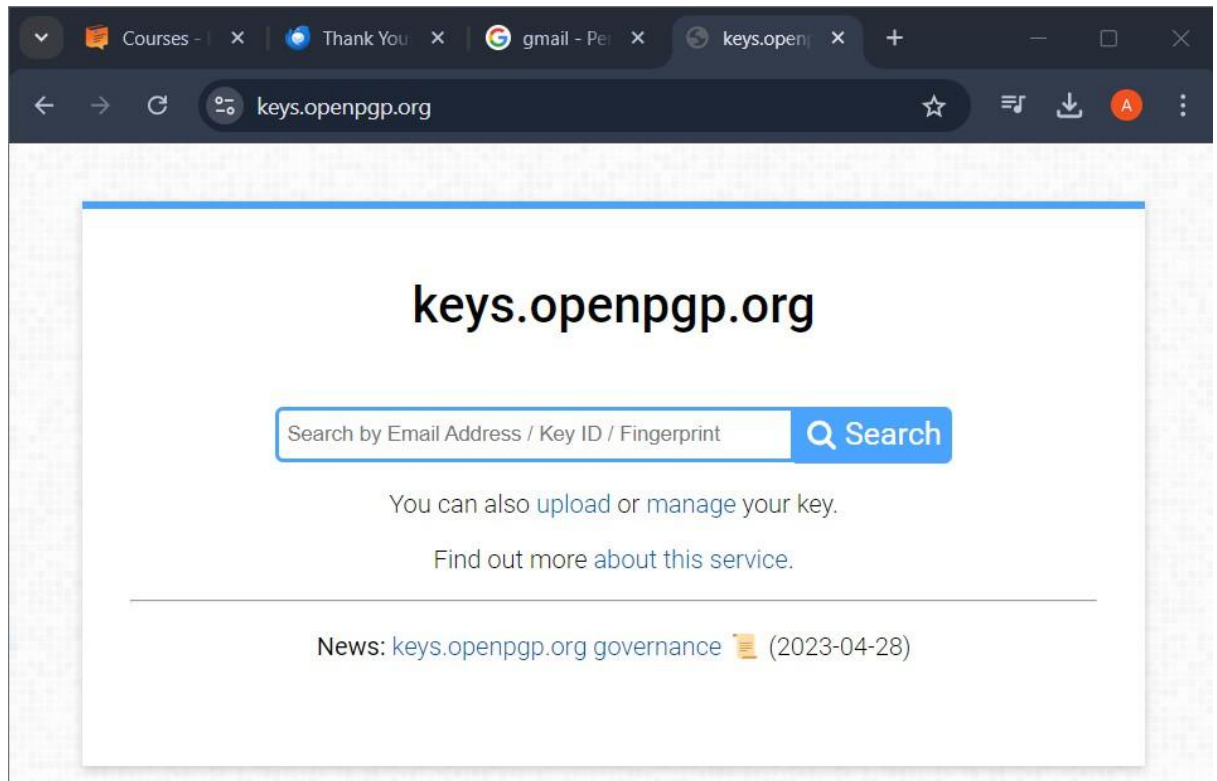
Cancel

- Pembuatan public key dan secret key sudah berhasil :

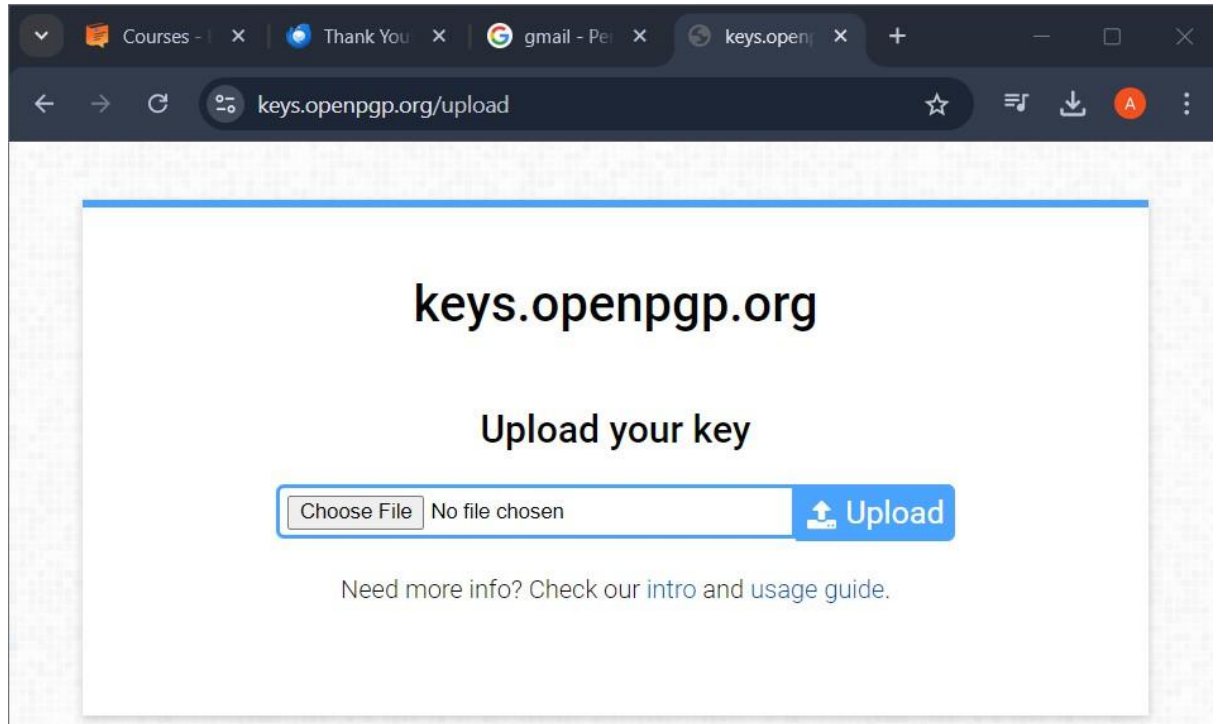
 Asyrof Hafizh Maulana_asyrofhafizhmaulana@gmail.com-0xAF5B778B414F6B7B-pub.asc	12/10/2024 22:09	ASC File	3 KB
 Asyrof Hafizh Maulana_asyrofhafizhmaulana@gmail.com-0xAF5B778B414F6B7B-secret.asc	12/10/2024 22:16	ASC File	6 KB

B:

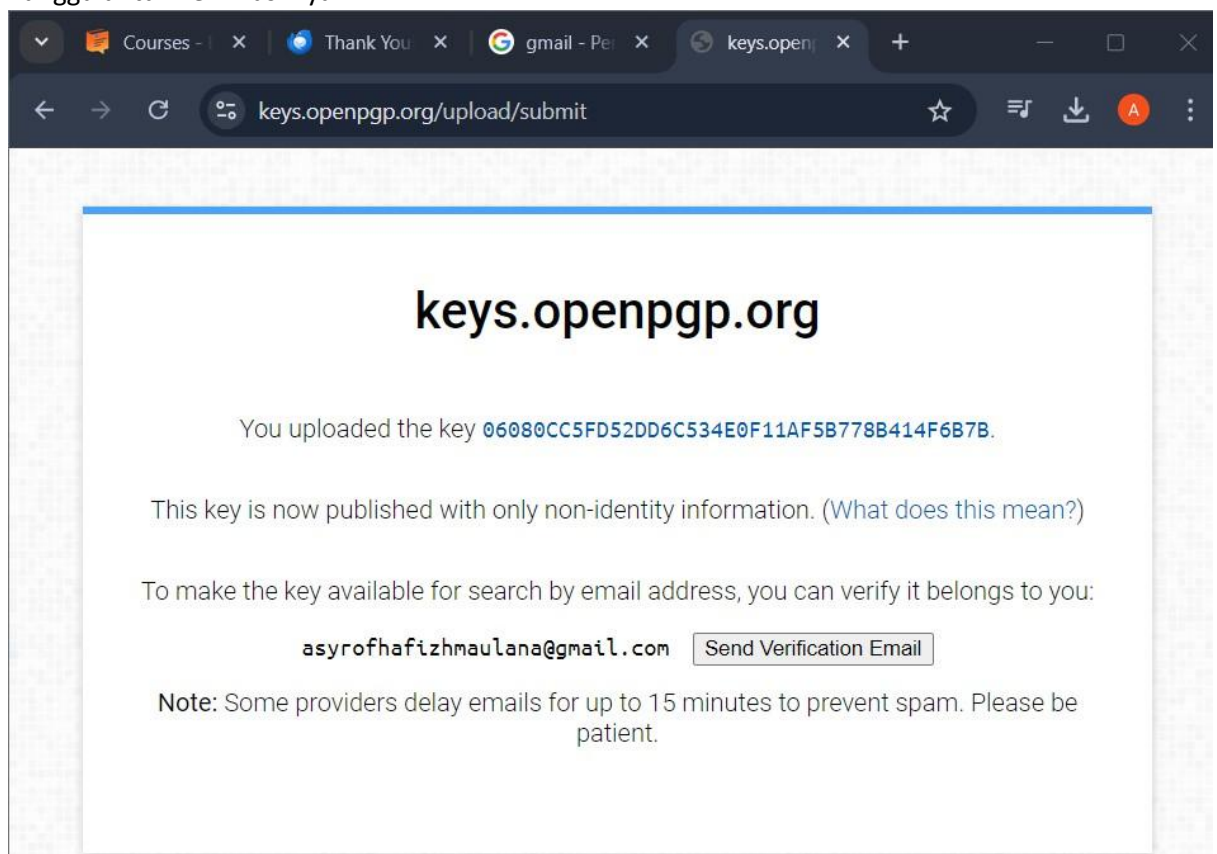
- Upload file :



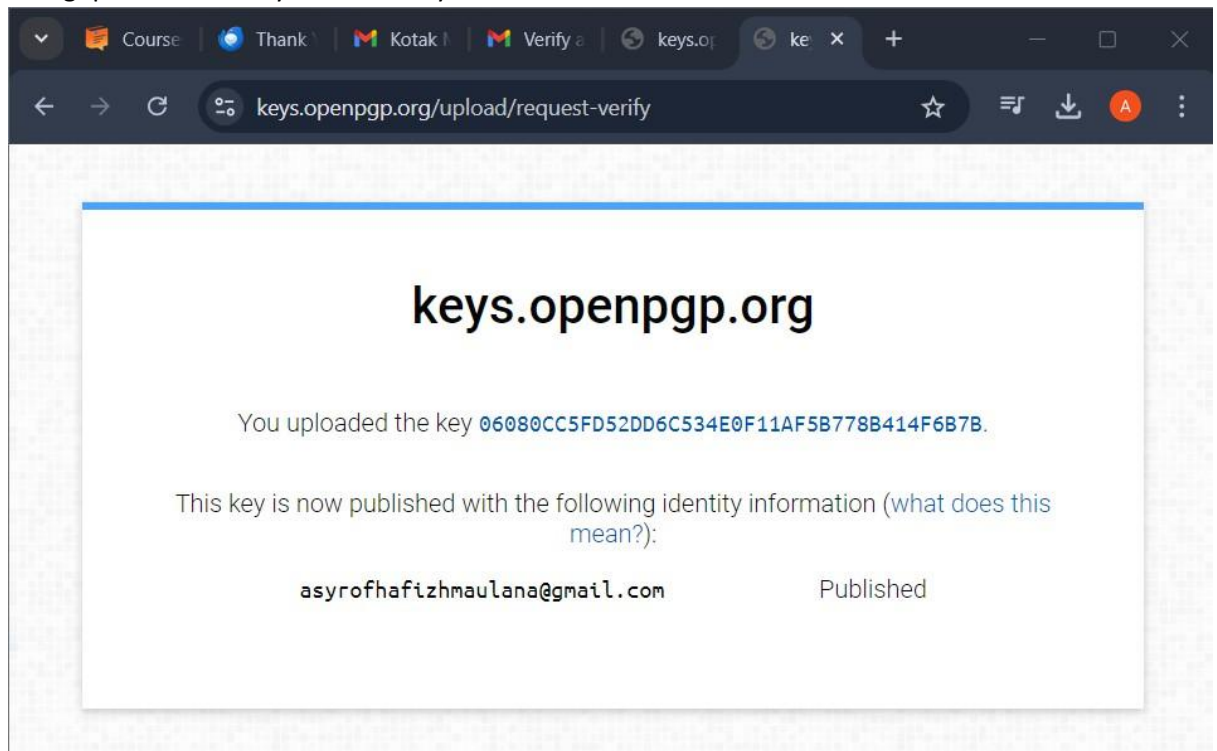
- Pilih file yang akan di upload :



- Tunggu untuk verifikasi nya :

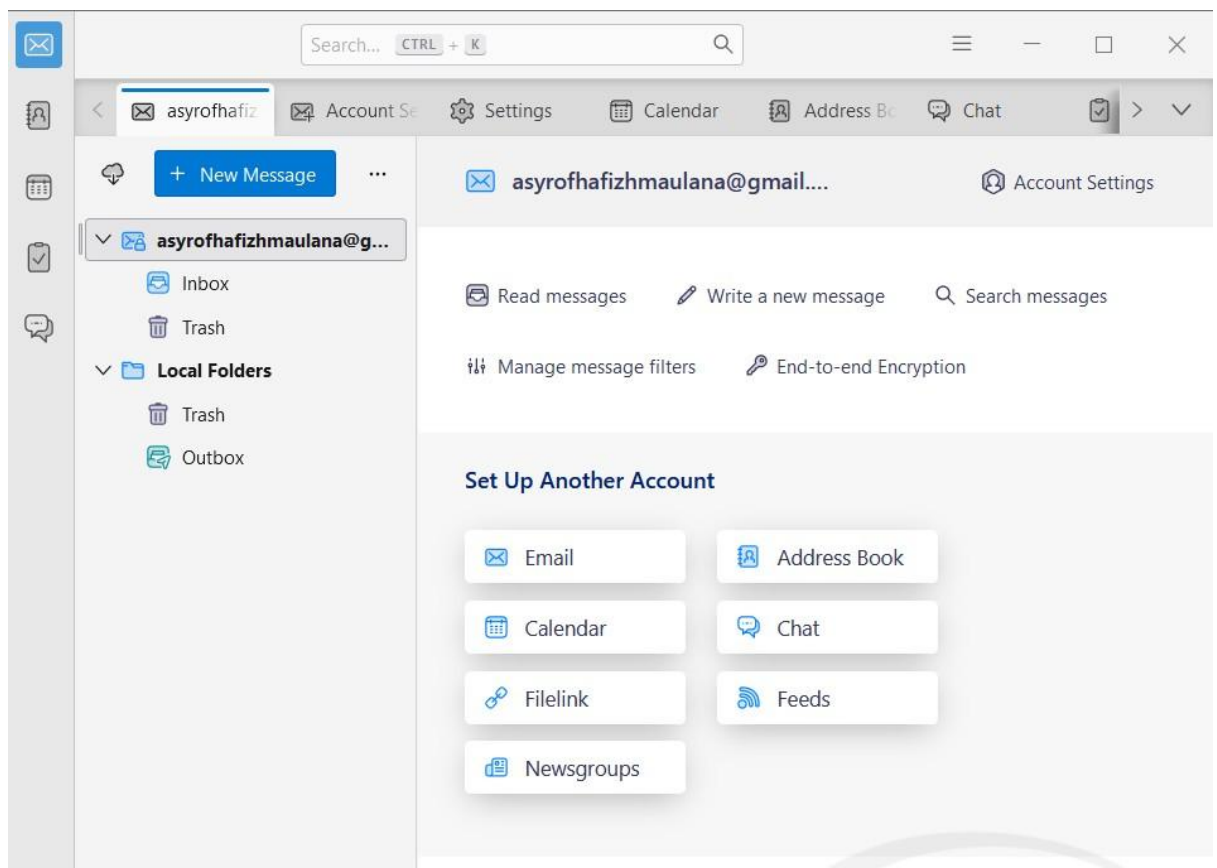


- Mengupload Publik Key ke Public Key Server berhasil :

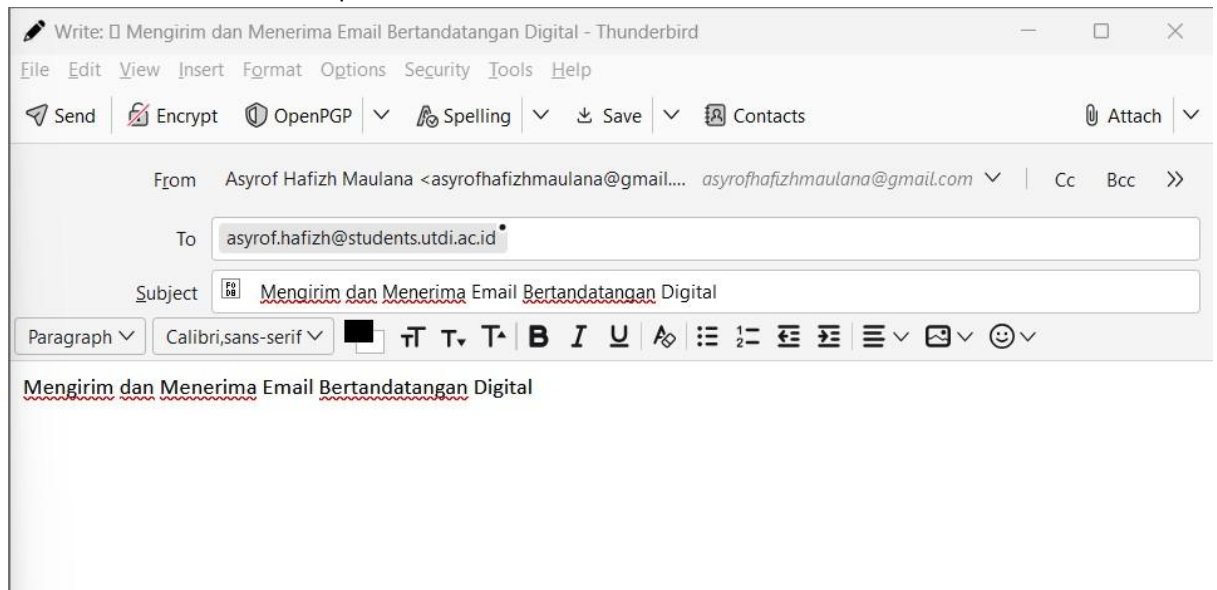


C:

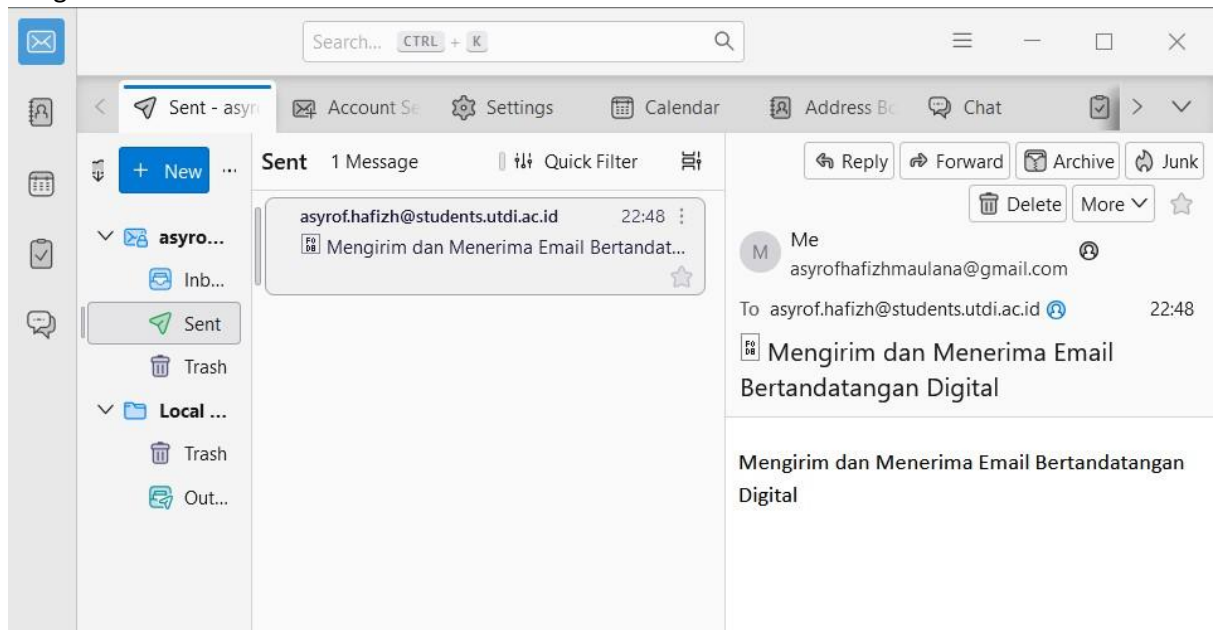
- Mengirim dan Menerima Email Bertandatangan Digital dengan cara klik message :



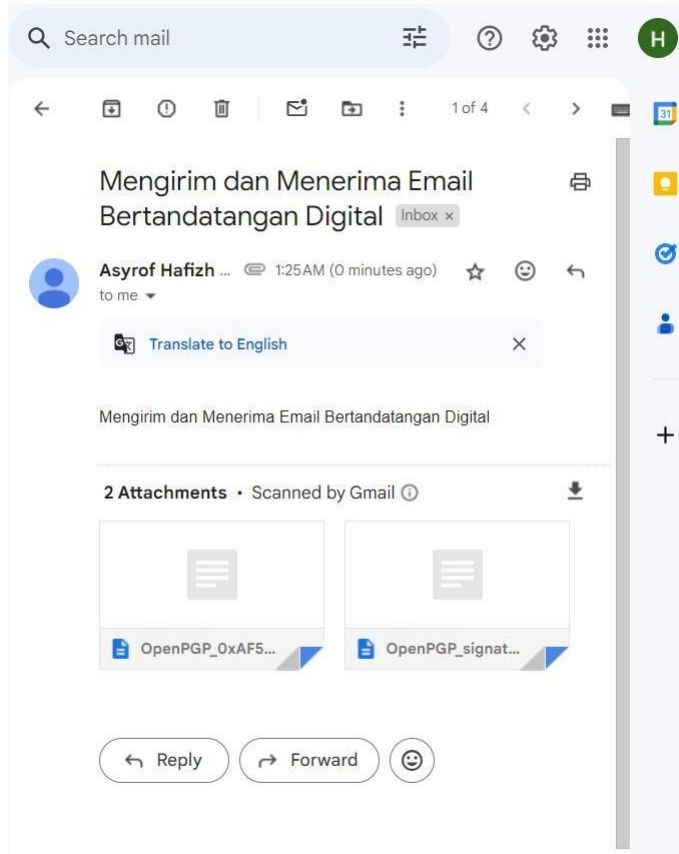
- Setelah itu masukkan email penerima dll :



- Pengiriman email selesai :



➤ Menerima email :

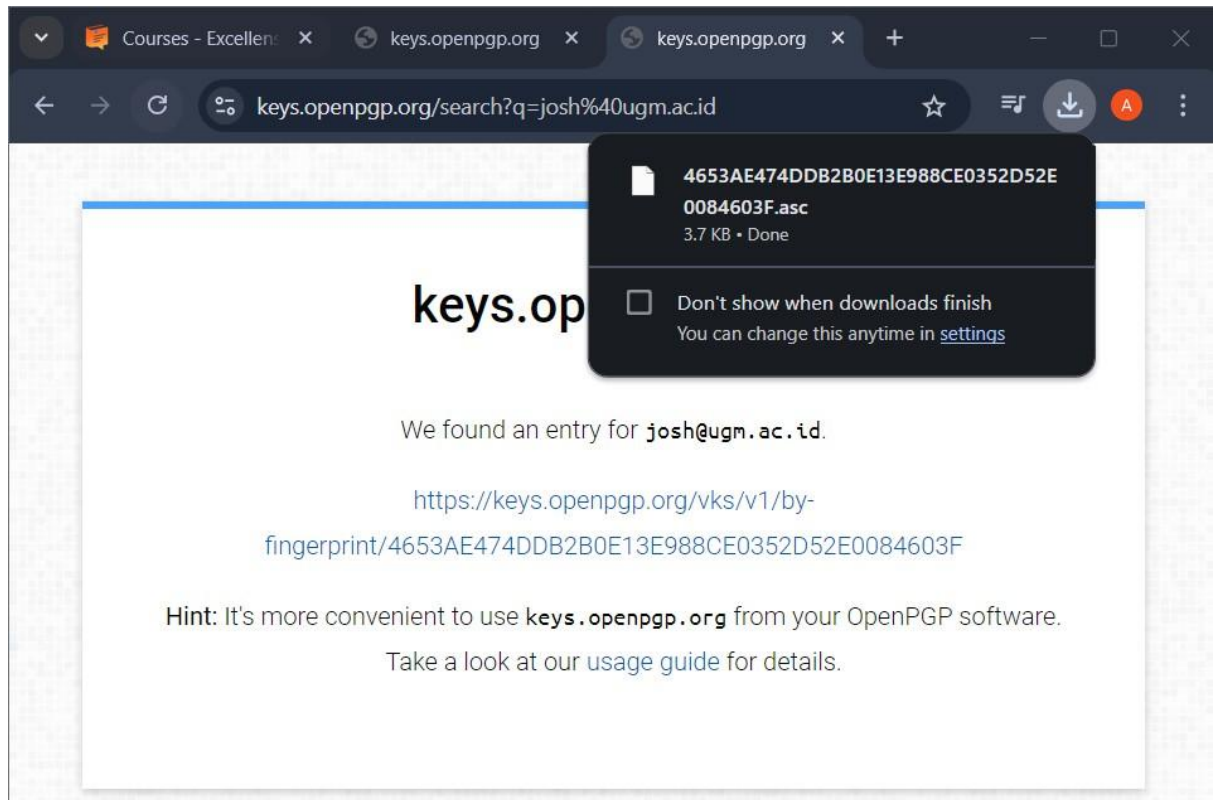


Syarat:

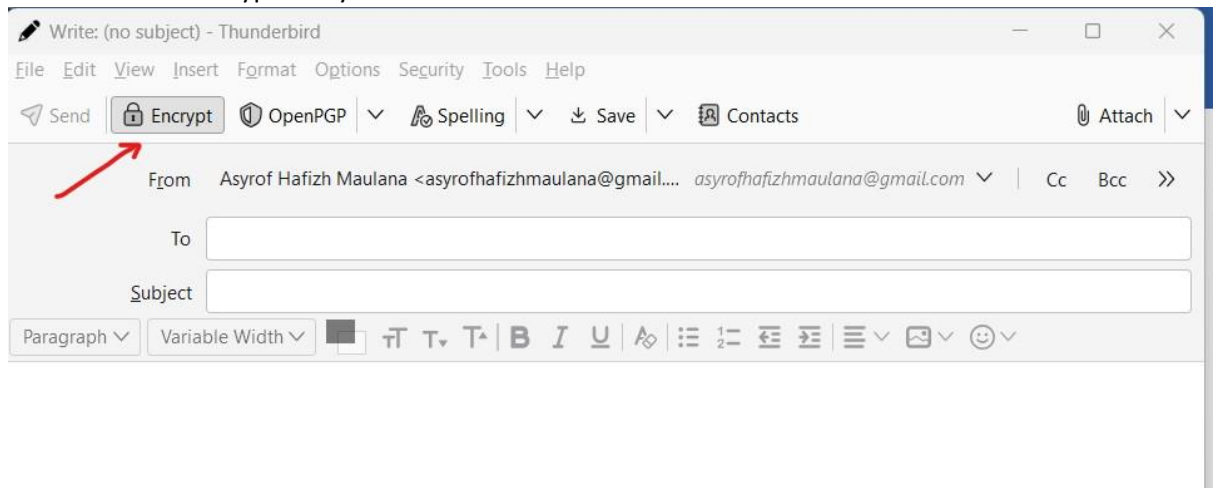
- Menggunakan Sertifikat Digital: harus memiliki sertifikat digital dari otoritas sertifikasi (CA) yang tepercaya untuk menandatangani email.
- Aplikasi Email yang Mendukung: Gunakan aplikasi email yang mendukung tanda tangan digital, seperti Thunderbird dengan plugin Enigmail atau Evolution.
- Kunci Privat: Kunci privat harus disimpan di komputer, dan ini digunakan untuk menandatangani pesan.

D :

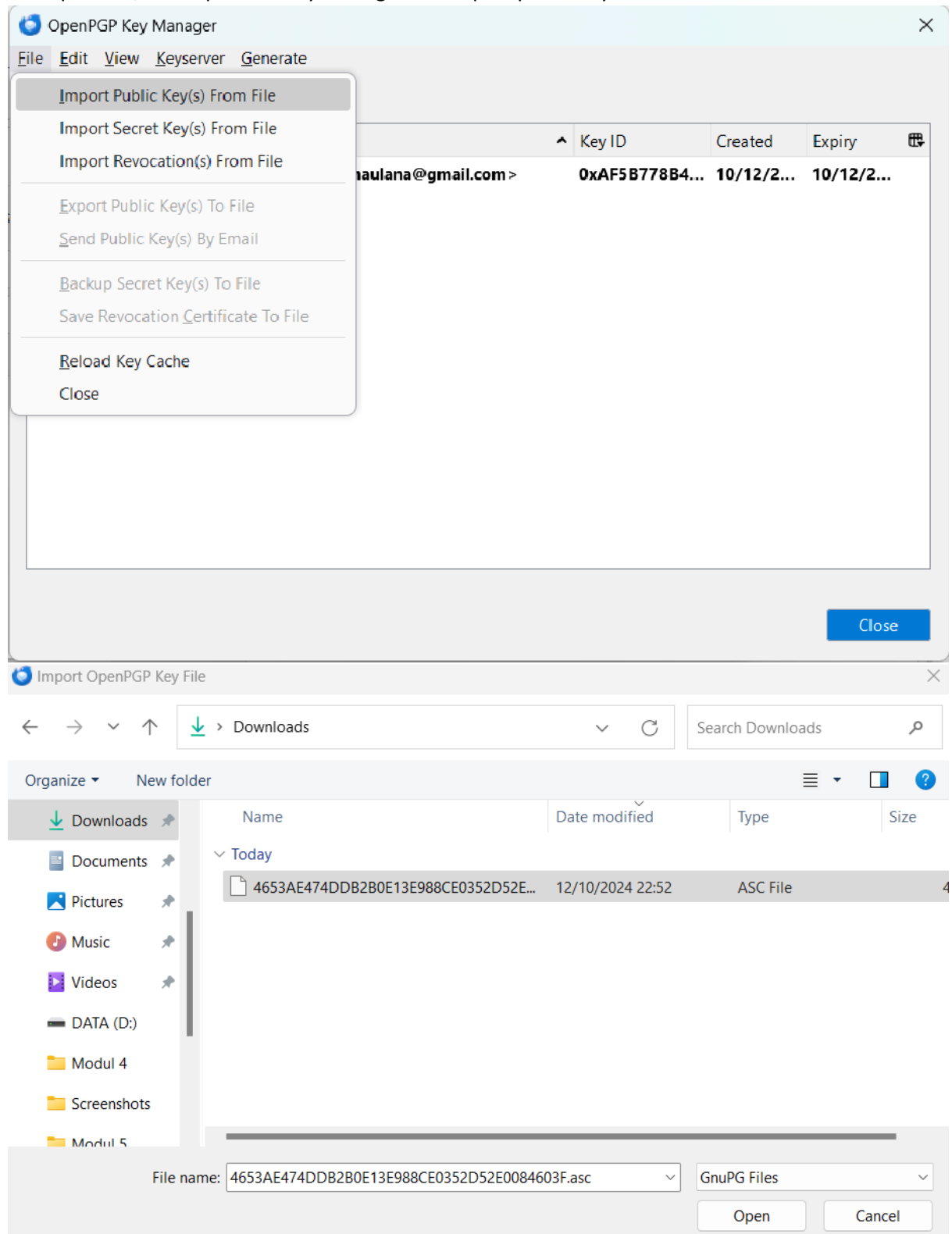
- Download public key dari pak josua :

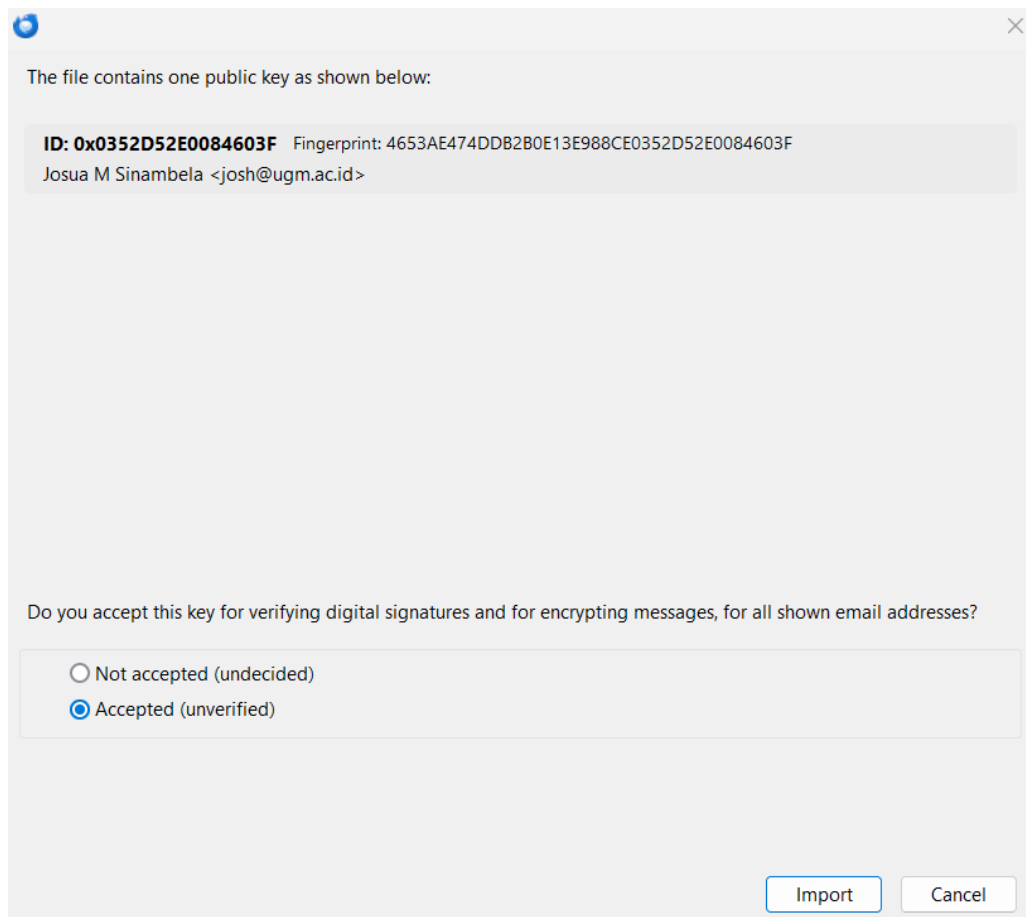


- Setelah itu klik encryption nya :

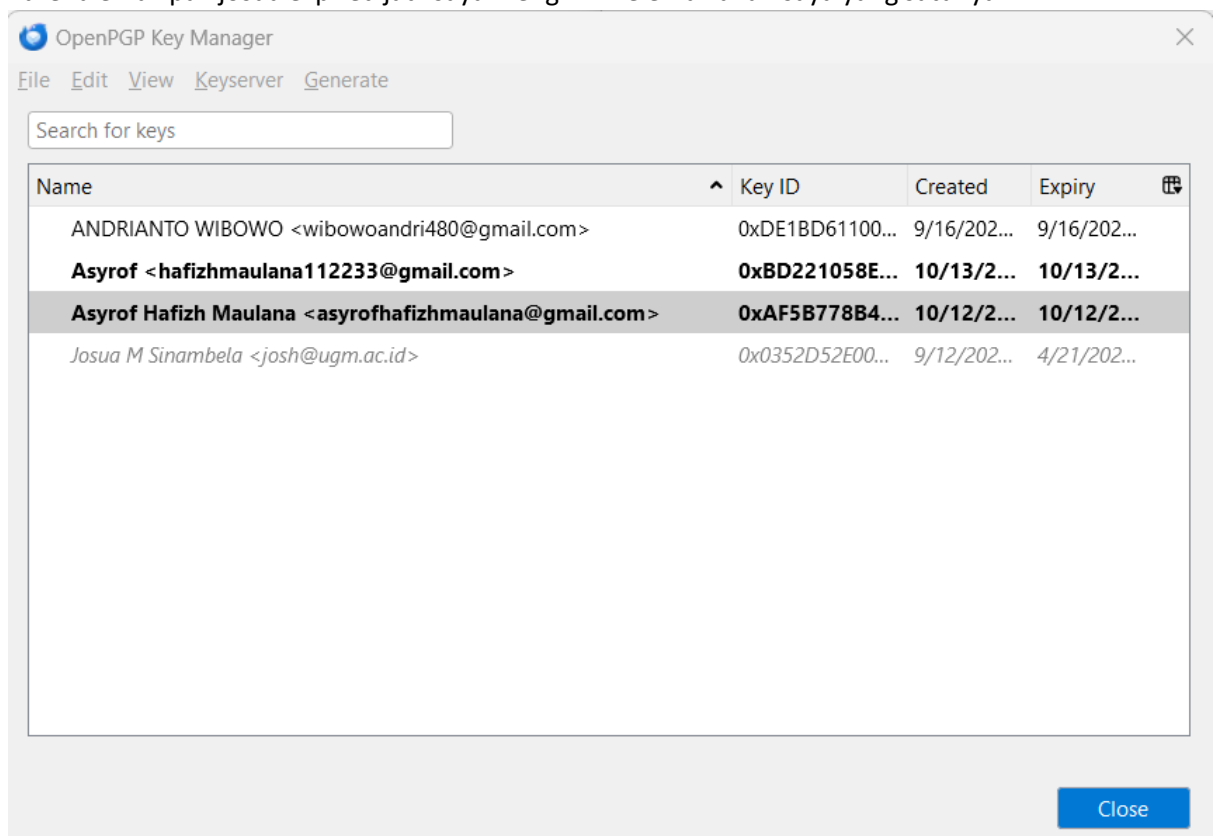


- Klik OpenPGP, buka OpenPGP Key Manager lalu import public key :

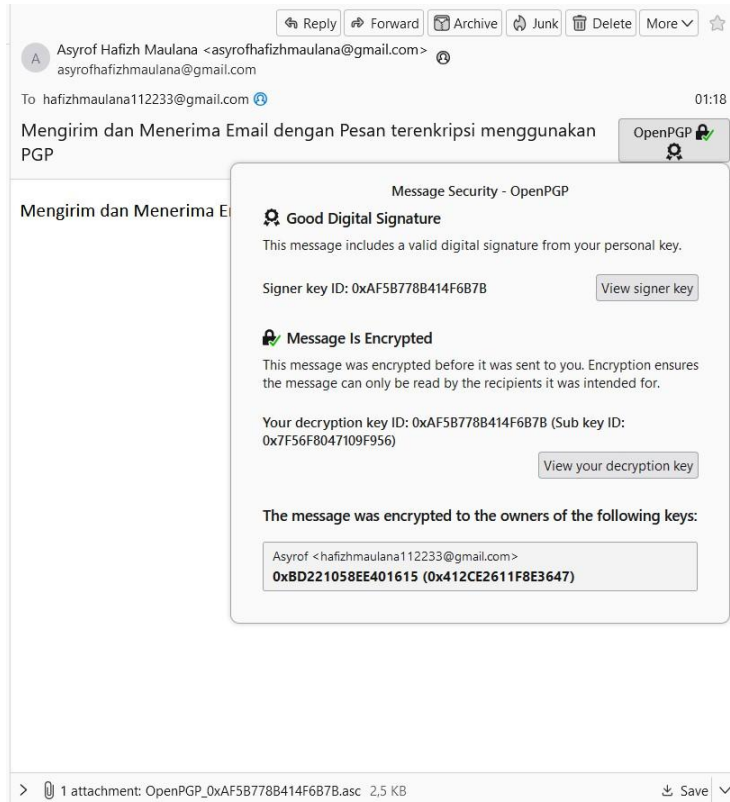




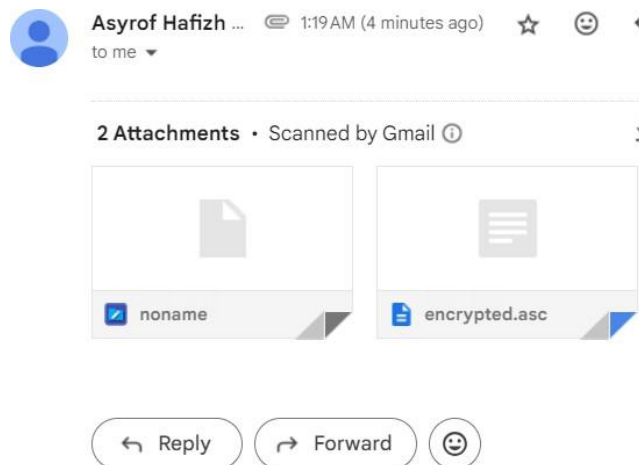
- Karena email pak josua expired jadi saya mengirim ke email akun saya yang satunya :



➤ Pengiriman email dengan Pesan terenkripsi menggunakan PGP selesai :



➤ Menerima email :

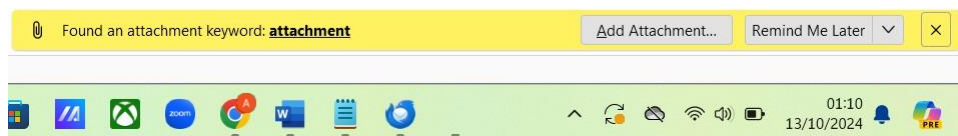
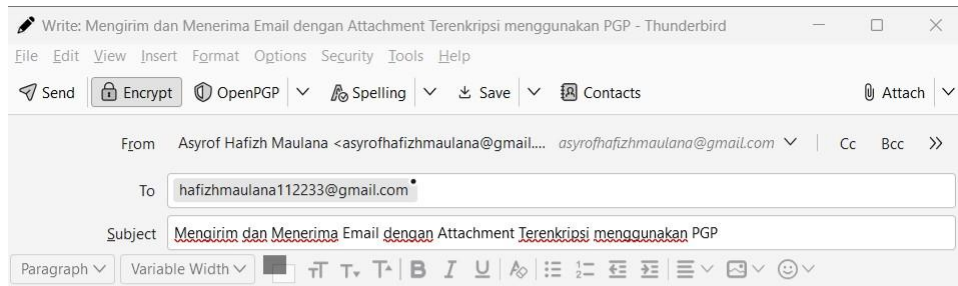


Syarat:

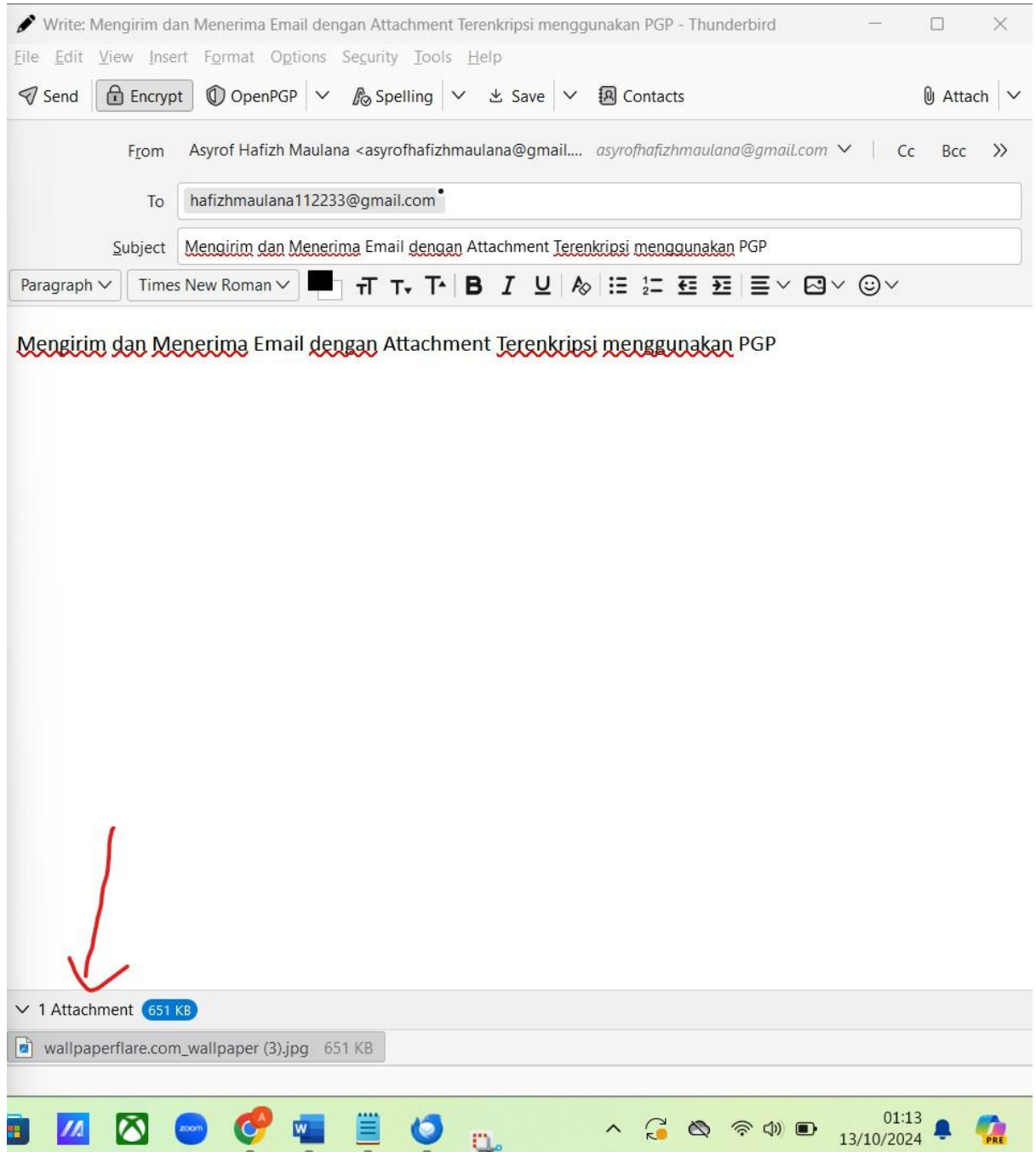
- Memiliki Kunci Publik Penerima: Untuk mengirimkan email terenkripsi, memerlukan kunci publik penerima. Kunci publik ini dapat diunduh dari server kunci seperti keys.openpgp.org.
- Kunci Privat : harus memiliki kunci privat untuk mendekripsi pesan yang diterima.
- Aplikasi Email yang Mendukung PGP: Gunakan aplikasi seperti Thunderbird dengan plugin Enigmail atau aplikasi lain yang mendukung PGP.

E:

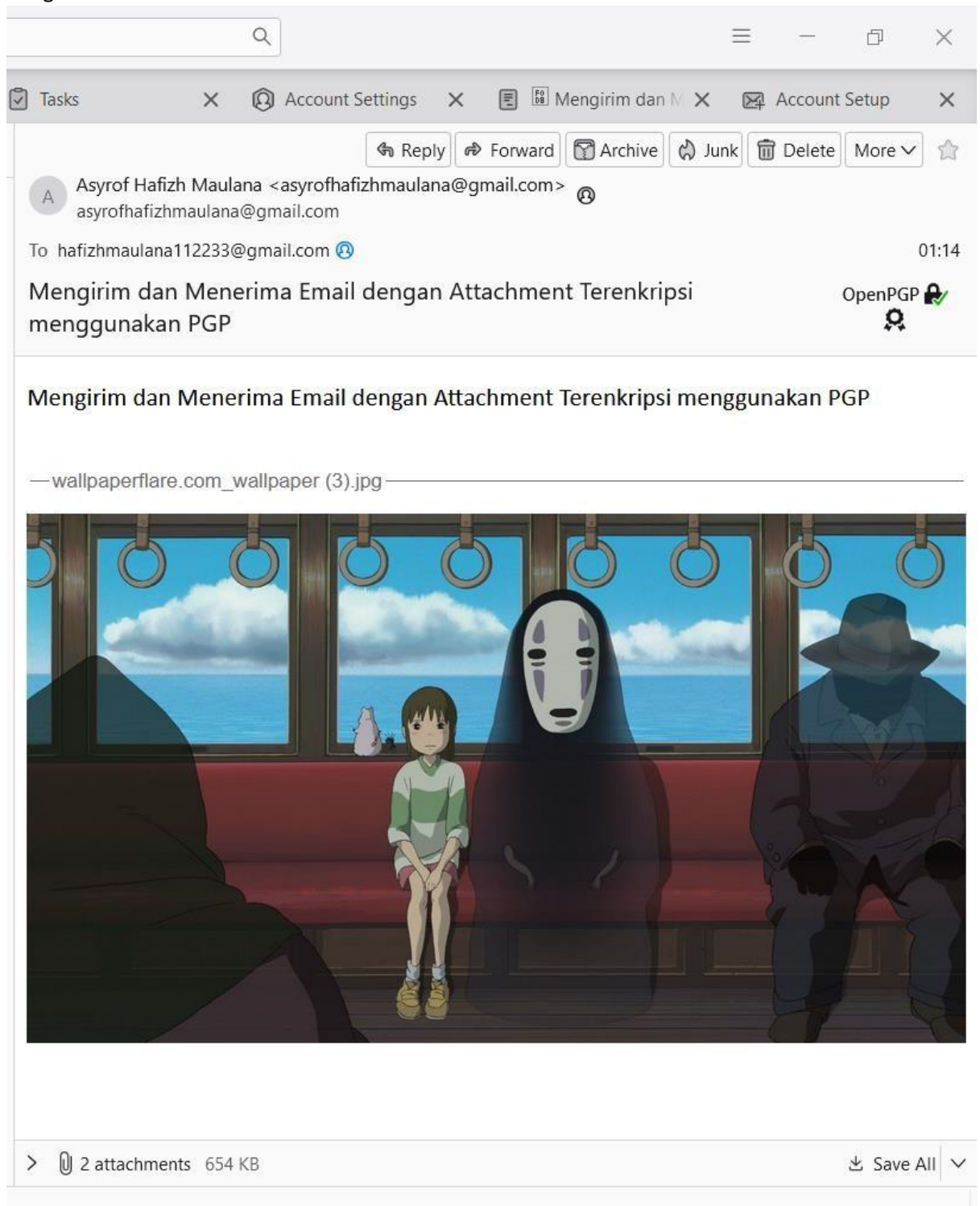
- Sama seperti sebelumnya,atur penerima email dll :



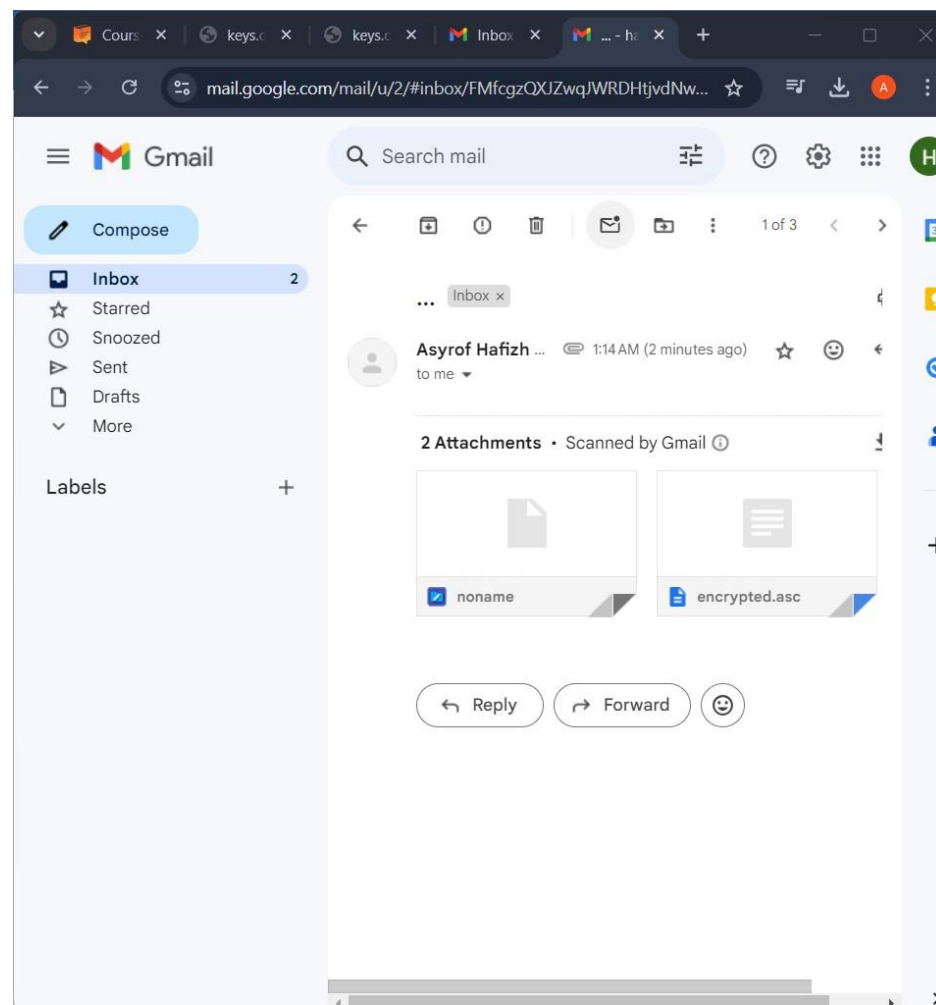
- Pilih gambar yang akan dikirim :



➤ Pengiriman email selesai :



➤ menerima email :



Syarat:

- Memiliki Kunci Publik Penerima: Sama seperti tugas d, memerlukan kunci publik penerima untuk mendekripsi lampiran.
- Kunci Privat : Kunci privat akan digunakan untuk mendekripsi lampiran yang diterima.
- Aplikasi Email yang Mendukung: Gunakan aplikasi email yang mendukung PGP untuk mengenkripsi lampiran, seperti Thunderbird.