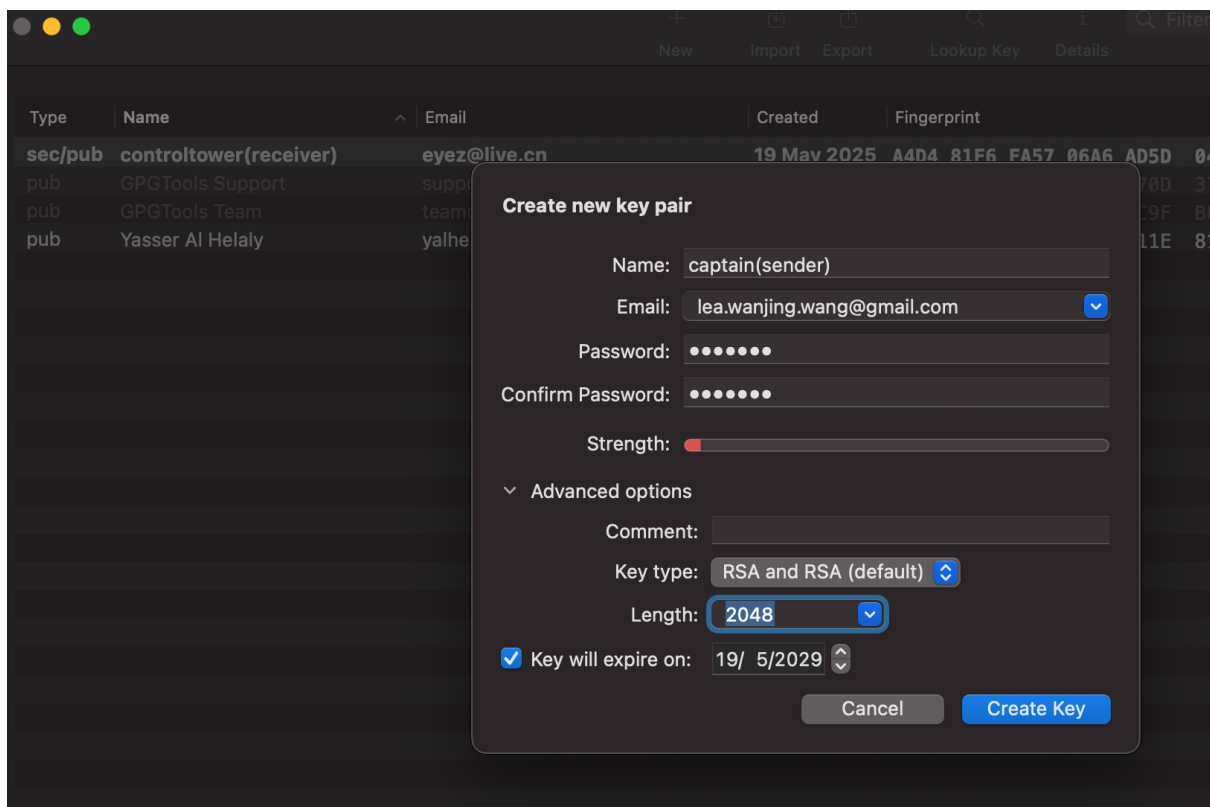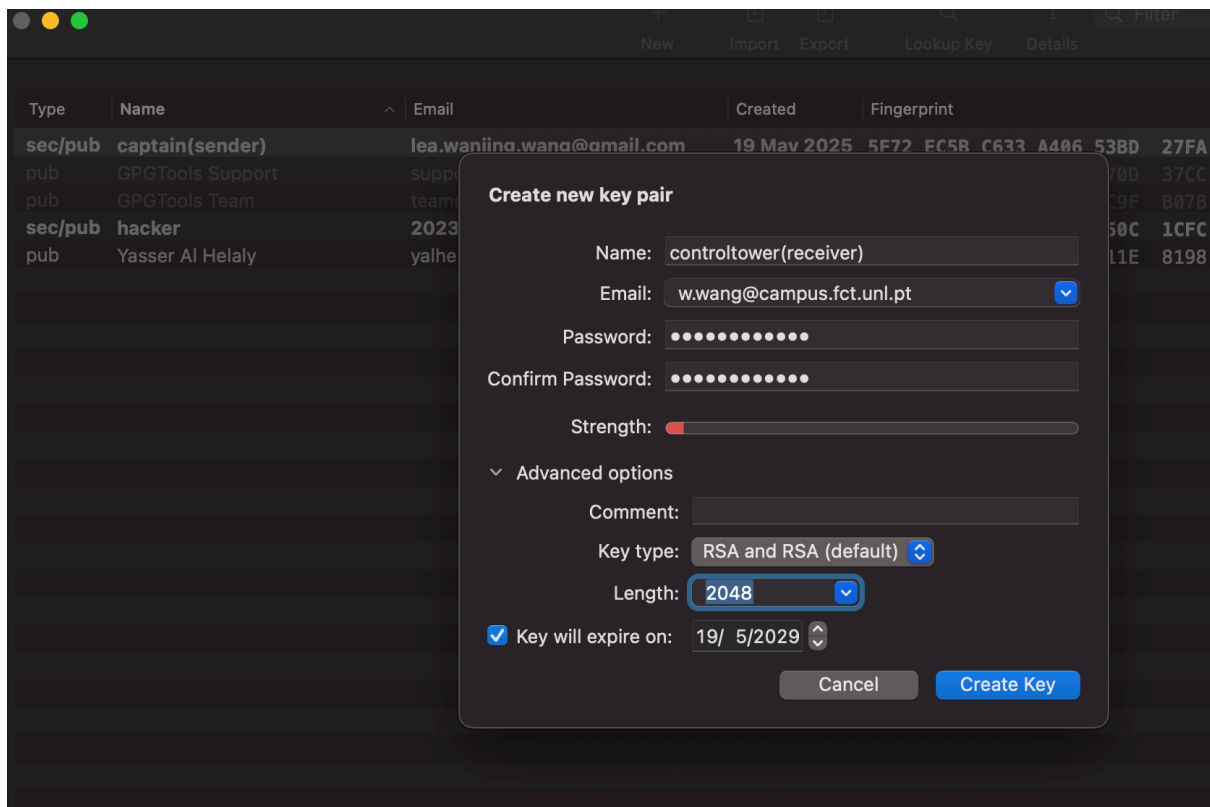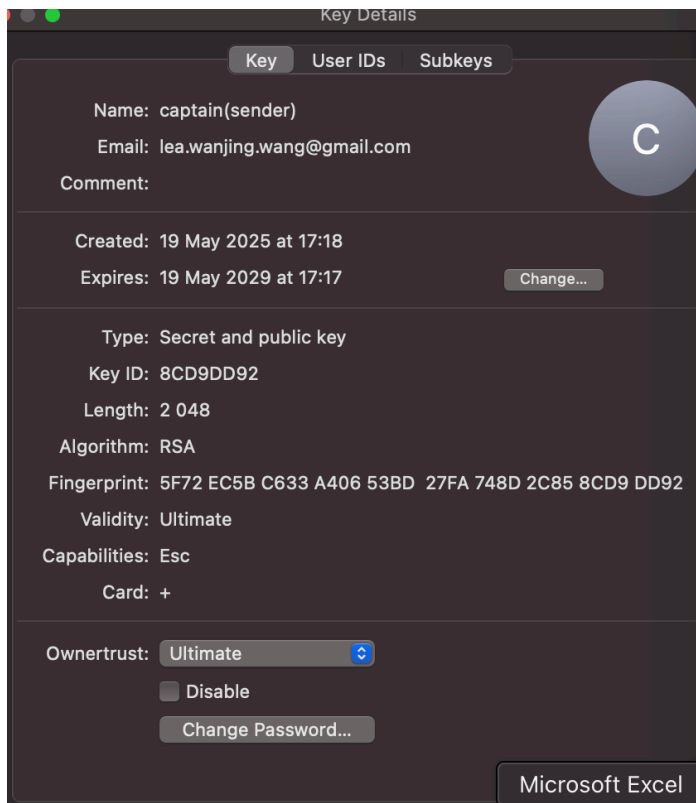## Key Pair Keyring

For checking out the full version of public key generated, right click 'copy', open an VS Code text file, and save onto it.

For checking out the full version of private key generated, open terminal (using command), input `gpg --list-secret-keys`.

e.g., to create role – captain(sender) // controltower(receiver) // hacker (using the same mailbox as sender in this case)

Key Details

Key | User IDs | Subkeys

Name: captain(sender)

Email: lea.wanjing.wang@gmail.com

Comment:

C

Created: 19 May 2025 at 17:18

Expires: 19 May 2029 at 17:17   Change...

Type: Secret and public key

Key ID: 8CD9DD92

Length: 2 048

Algorithm: RSA

Fingerprint: 5F72 EC5B C633 A406 53BD 27FA 748D 2C85 8CD9 DD92

Validity: Ultimate

Capabilities: Esc

Card: +

Ownertrust: Ultimate

☐ Disable

Change Password...

Microsoft Excel

New   Import   Export   Lookup Key   Details   Filter

Type	Name	Email	Created	Fingerprint
sec/pub	captain(sender)	lea.wanjing.wang@gmail.com	19 May 2025	5F72 EC5B C633 A406 53BD 27FA
pub	GPGTools Support	supp		70D 37CC
pub	GPGTools Team	team		C9F B07B
sec/pub	hacker	2023		50C 1CFC
pub	Yasser Al Helaly	yalhe		11E 8198

Create new key pair

Name: controltower(receiver)

Email: w.wang@campus.fct.unl.pt

Password: ••••••••••••

Confirm Password: ••••••••••••

Strength:

Advanced options

Comment:

Key type: RSA and RSA (default)

Length: 2048

☑ Key will expire on: 19/ 5/2029

Cancel   Create Key

```
Last login: Mon May 19 22:34:22 on ttys000
(base) wanjingwang@Mac ~ % gpg --list-secret-keys
/Users/wanjingwang/.gnupg/pubring.kbx
------------------------------------
sec    rsa2048 2025-05-19 [SC] [expires: 2029-05-19]
       5F72EC5BC633A40653BD27FA748D2C858CD9DD92
uid            [ultimate] captain(sender) () <lea.wanjing.wang@gmail.com>
ssb    rsa2048 2025-05-19 [E] [expires: 2029-05-19]

sec    rsa2048 2025-05-19 [SC] [expires: 2029-05-19]
       C46979630F709F2D2B13CEF5E63B16524BB7757C
uid            [ultimate] controltower(receiver) () <w.wang@campus.fct.unl.pt>
ssb    rsa2048 2025-05-19 [E] [expires: 2029-05-19]

sec    rsa2048 2025-05-19 [SC] [expires: 2029-05-19]
       1E76500D6C7E4360595D2E1D4B132C0867C796EB
uid            [ultimate] hacker <lea.wanjing.wang@gmail.com>
ssb    rsa2048 2025-05-19 [E] [expires: 2029-05-19]
```
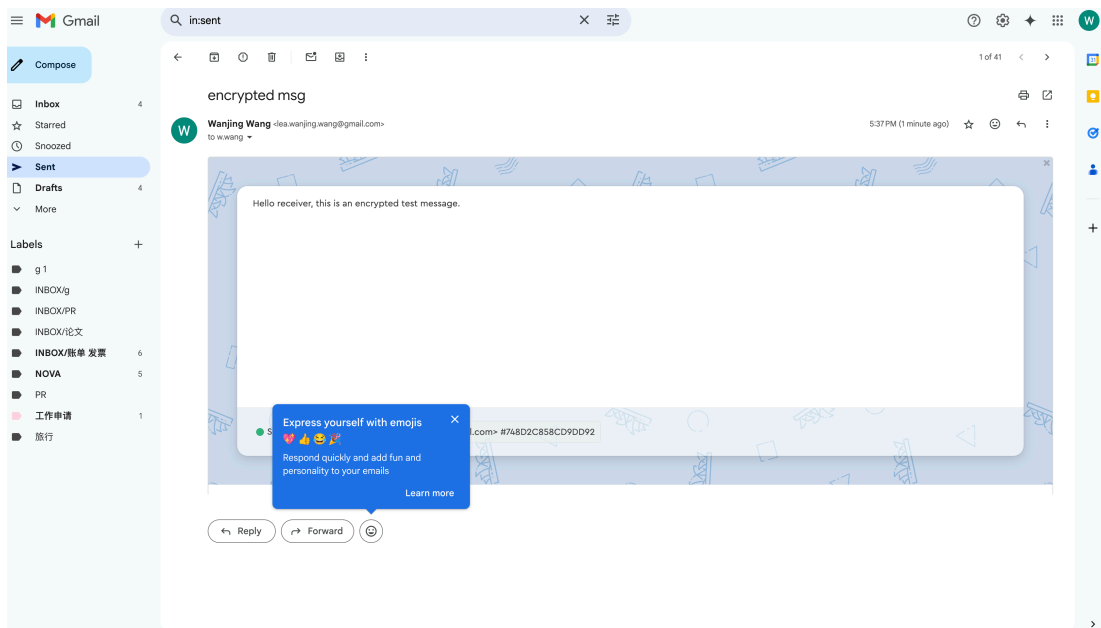
Email Encryption and Sending

- Composing the email and applying GPG encryption.

- The encrypted content as received by the receiver (before and after decryption).
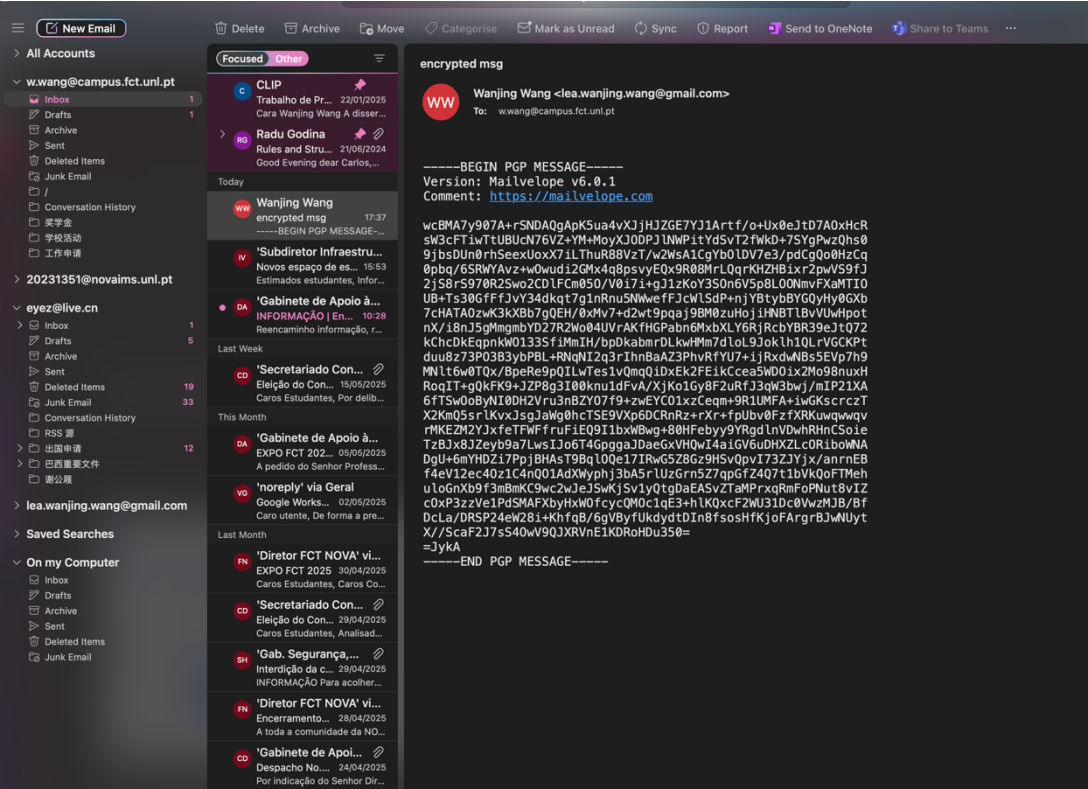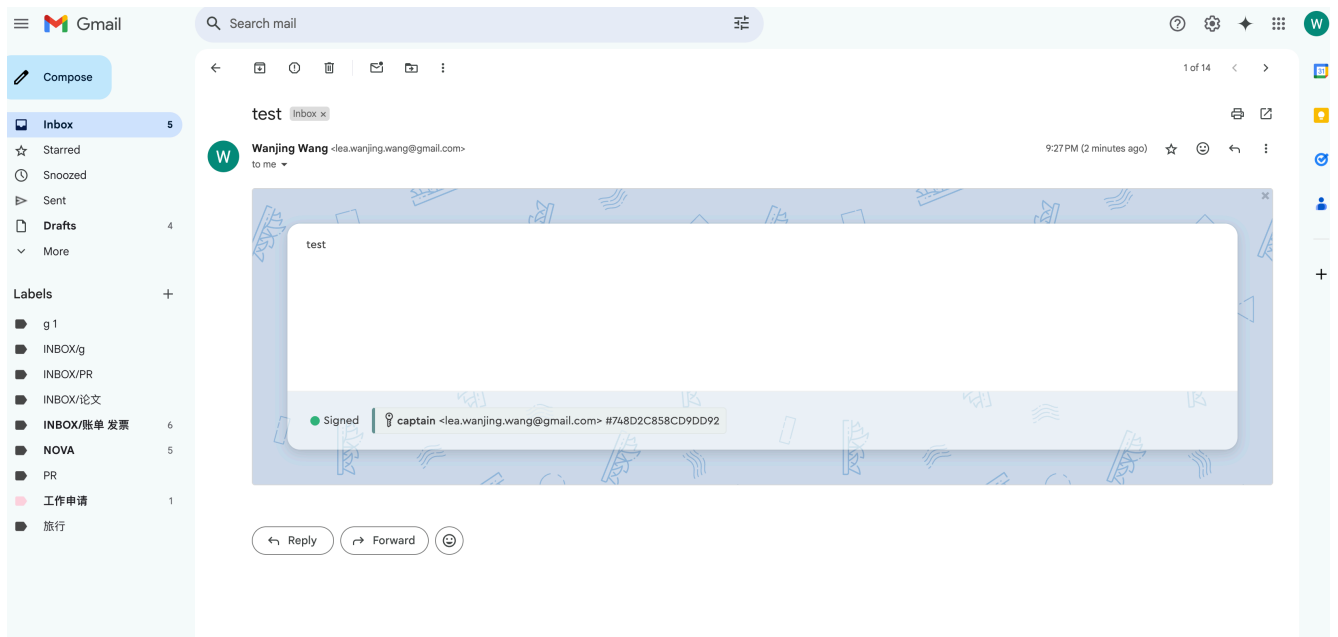

- The receiver decrypting the message.

- The public keys being imported and verified.

The Hacker's Interception Attempt

The provided screenshot contains the encrypted content from the fake inbox that the Hacker intercepts through email - copy & paste the encrypted massage received by the receiver and save it as a .txt file, in this case, named 'hacker'.

The hacker then try to decrypt the message using only the public key – the screenshot proves that decryption fails without the private key.