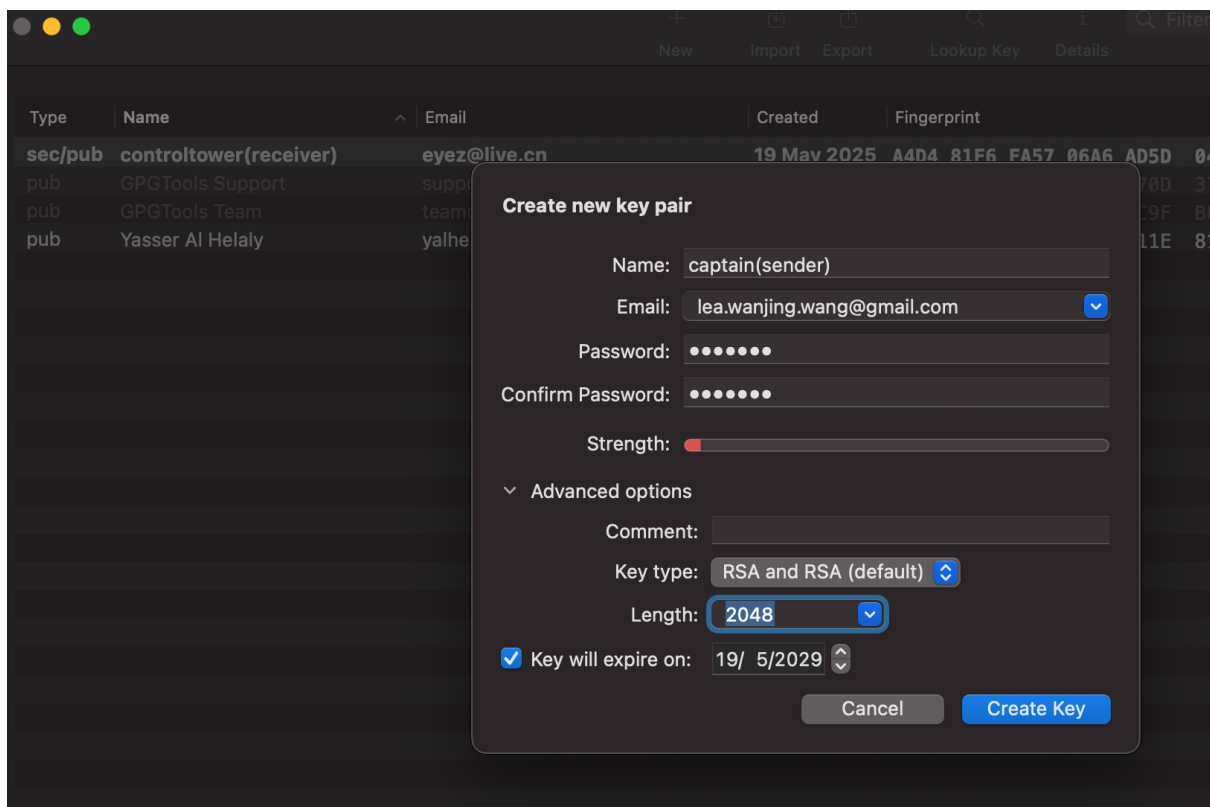


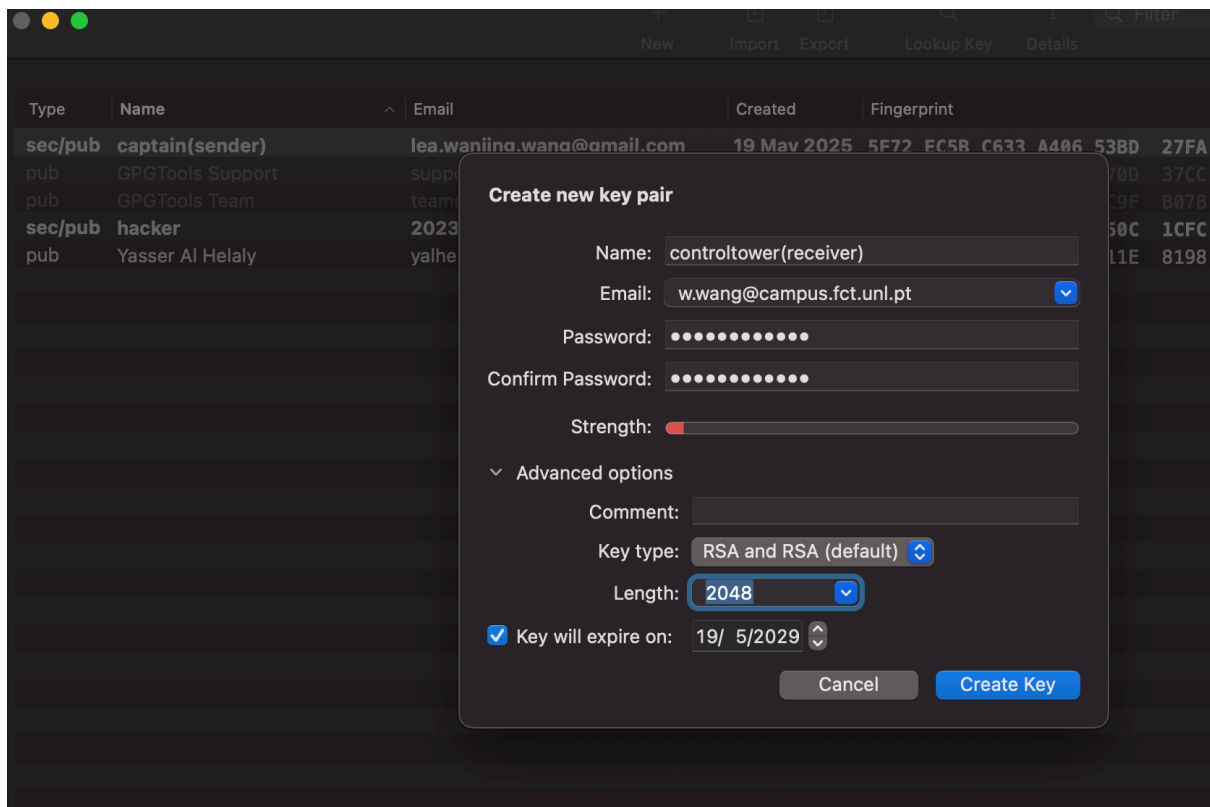
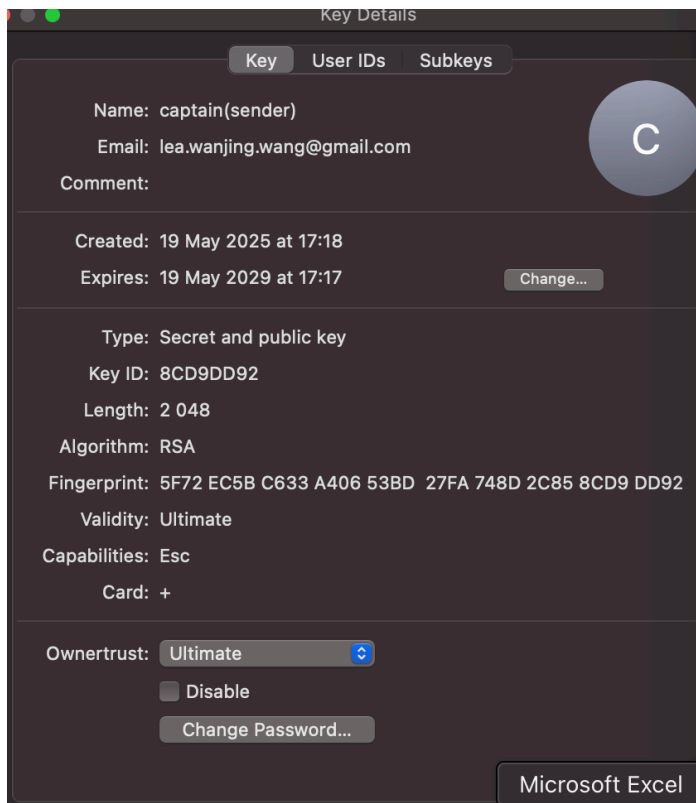
## Key Pair Keyring

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)





```

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]

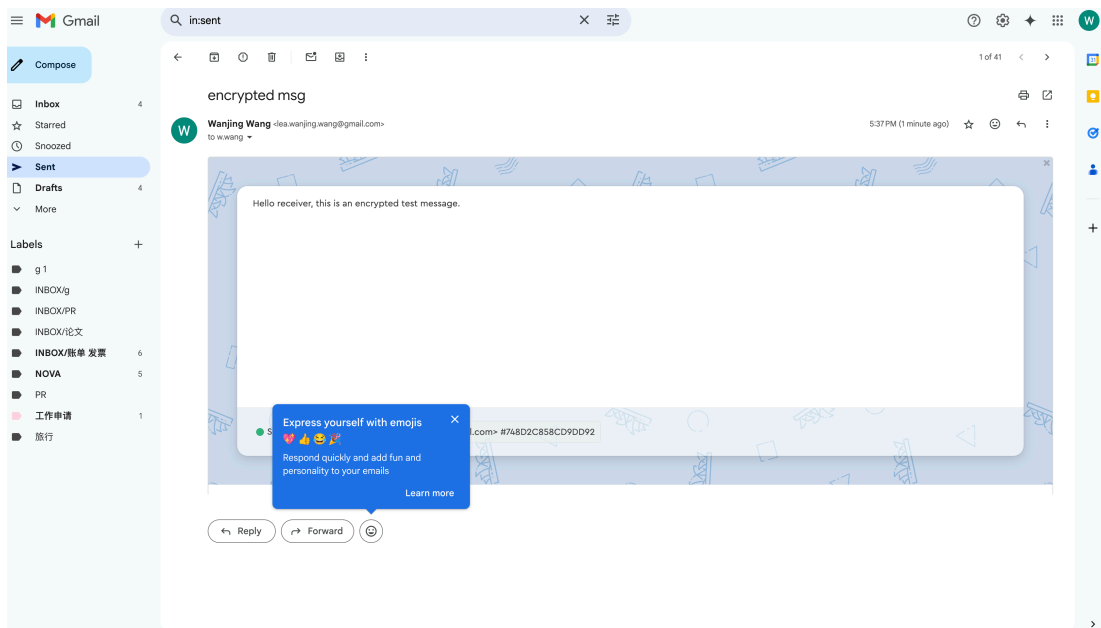
sec   rsa2048 2025-05-19 [SC] [expires: 2029-05-19]
      C46979630F709F2D2B13CEF5E63B16524BB7757C
uid   [ultimate] controltower(receiver) () <w.wang@campus.fct.unl.pt>
ssb   rsa2048 2025-05-19 [E] [expires: 2029-05-19]

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]

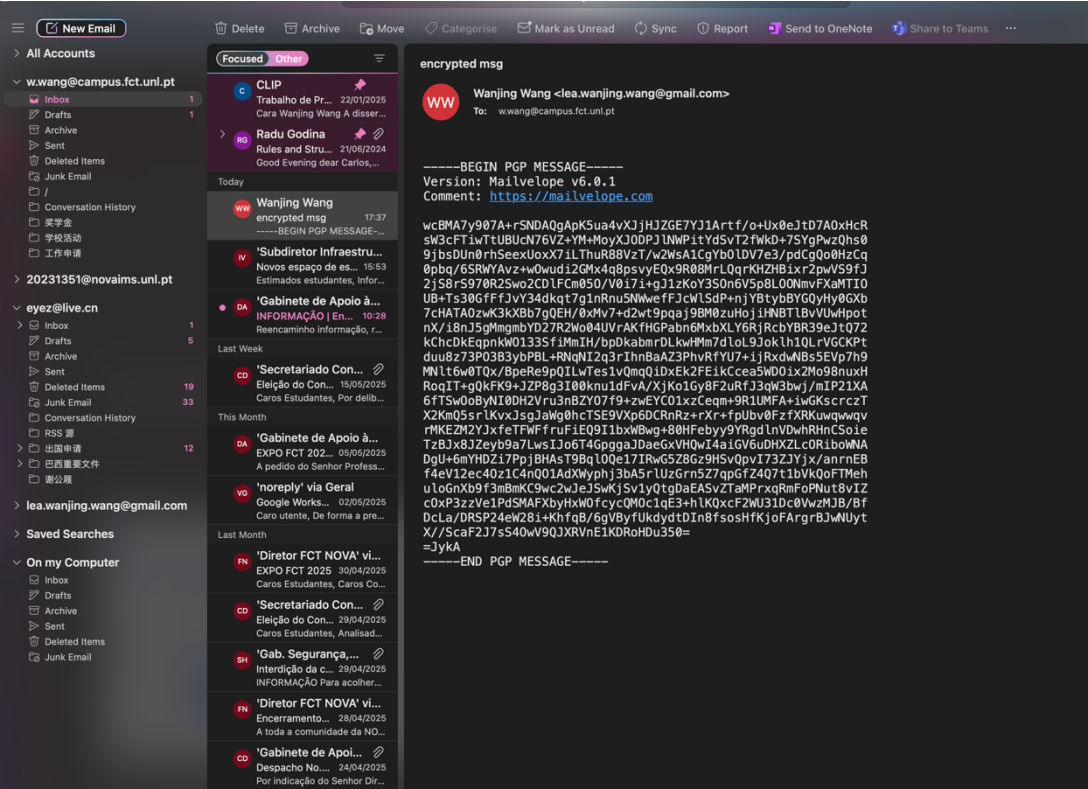
```

## 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.

Enter key password

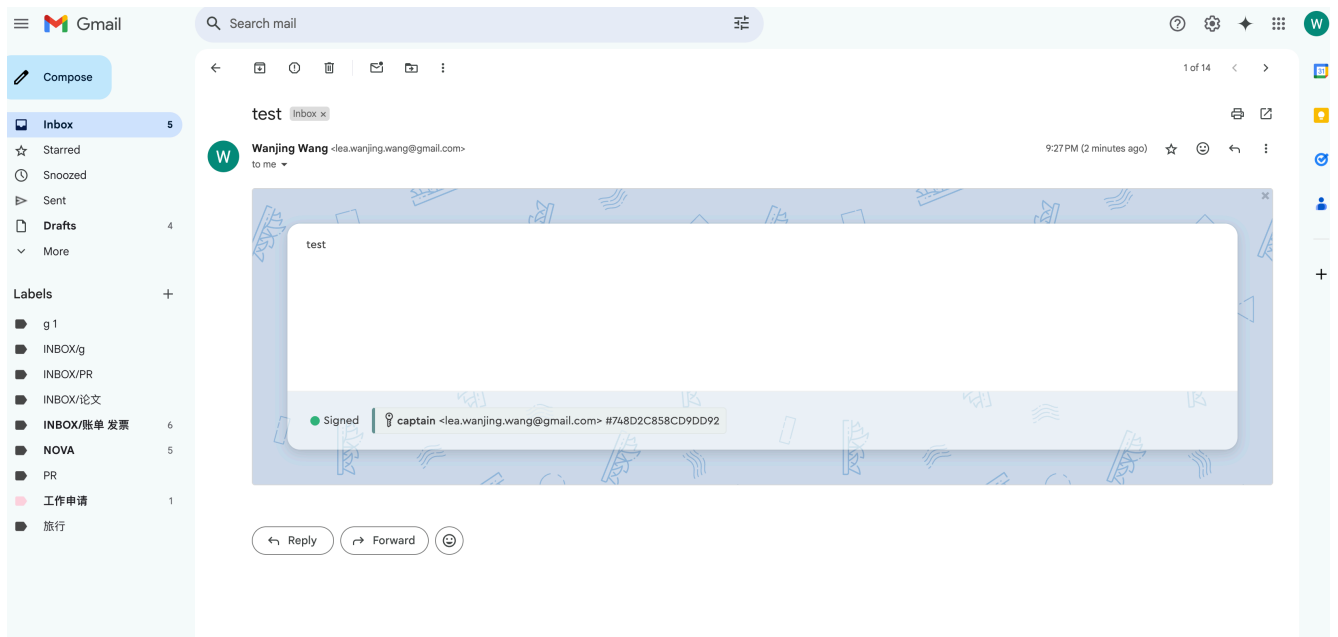
captain(sender) 0 <lea.wanjiang.wang@gmail.com>  
748D2C858CD9DD92

Please enter your key password to decrypt this message.

.....

☒ Remember password temporarily

Cancel OK



- The public keys being imported and verified.

< Key Management

**captain** ● valid

Remove

Export

Revoke

Default

## Assigned user IDs

Add new

Primary	Name	Email	Status	Signatures	
✓	captain	lea.wanjing.wang@gmail.com	● valid	1	>

The key is not synchronized with the Mailvelope key server.

Synchronize

## Key details

Main Key 748D2C858CD9DD92 ▼

Status	● valid	Key ID	748D2C858CD9DD92
Created	19/05/2025	Algorithm	RSA (Encrypt or Sign)
Expires	19/05/2029 <a href="#">Change</a>	Length	2048
Password	..... <a href="#">Change</a>	PGP Fingerprint	5F72 EC5B C633 A406 53BD 27FA 748D 2C85 8CD9 DD92

## 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 message 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.

Mailvelope

Key Management

Encrypt

Decrypt

Options

Make Mailvelope

Personalize now

Decryption of the text is not possible. No private key found for this message. Required private key IDs: BCBDD3B03EAD2343

Decrypt data

Decrypt

Attachments

Drag file to this window or 

Add file

Text to decrypt

9t3K90MIEnk2m3s0EH6F1ZKWcfYXcKjWc9i4j6fNCMgMrNeHgd7oURZzLrDd  
K31AF38JDZuw/zV+6VNxFZiayyODPMMhtAYZ4U9GF57KK4HKigW8Duwpp/1N  
x+ILf024jqVGebVotMmF3iqV8xnflHxd6S2K8MZ9Mwpc5jcPZ7j/HVghIJZ5t  
dd2XlIfGmX/RzkUjV98tLm0Bkb5dTj0eb1RvFziDeuzRX0QeKJRCYXLQj  
5KeAPSB6fllRG87zUil3Hr9g+BxTFnbE4QgsEhSxmlyS6CTTITCwAN+yEJfJ  
FXcnaG1hZFGukUhbQD4A2JQR2g/rcU8dvD1nEEfst1ejLRpnlJy2D7OFINKB  
XVomLFGXFZq7/cbcSa3daB5UdgPkg==  
=buZM  
—END PGP MESSAGE—

© 2024 Mailvelope GmbH

6.0.1