

# Homework 2: Configuring and Using GPG

Mudit Vats  
mpvats@syr.edu  
4/24/2020

## Table of Contents

---

Overview .....	3
Step 1 .....	3
Step 1a .....	3
Step 1b .....	4
Step 1c .....	4
Step 1d .....	7
Step 1e .....	9
Step 1f .....	11
Step 1g .....	13
Step 1h .....	15
Step 1i .....	18
Step 1j .....	20
Step 1k .....	21
Step 2 .....	22
Step 2a .....	22
Step 2b .....	22
Step 2c .....	22
Step 2d .....	23
Step 2e .....	23
Step 2f .....	23
Step 2g .....	23
Step 2h .....	23

## Overview

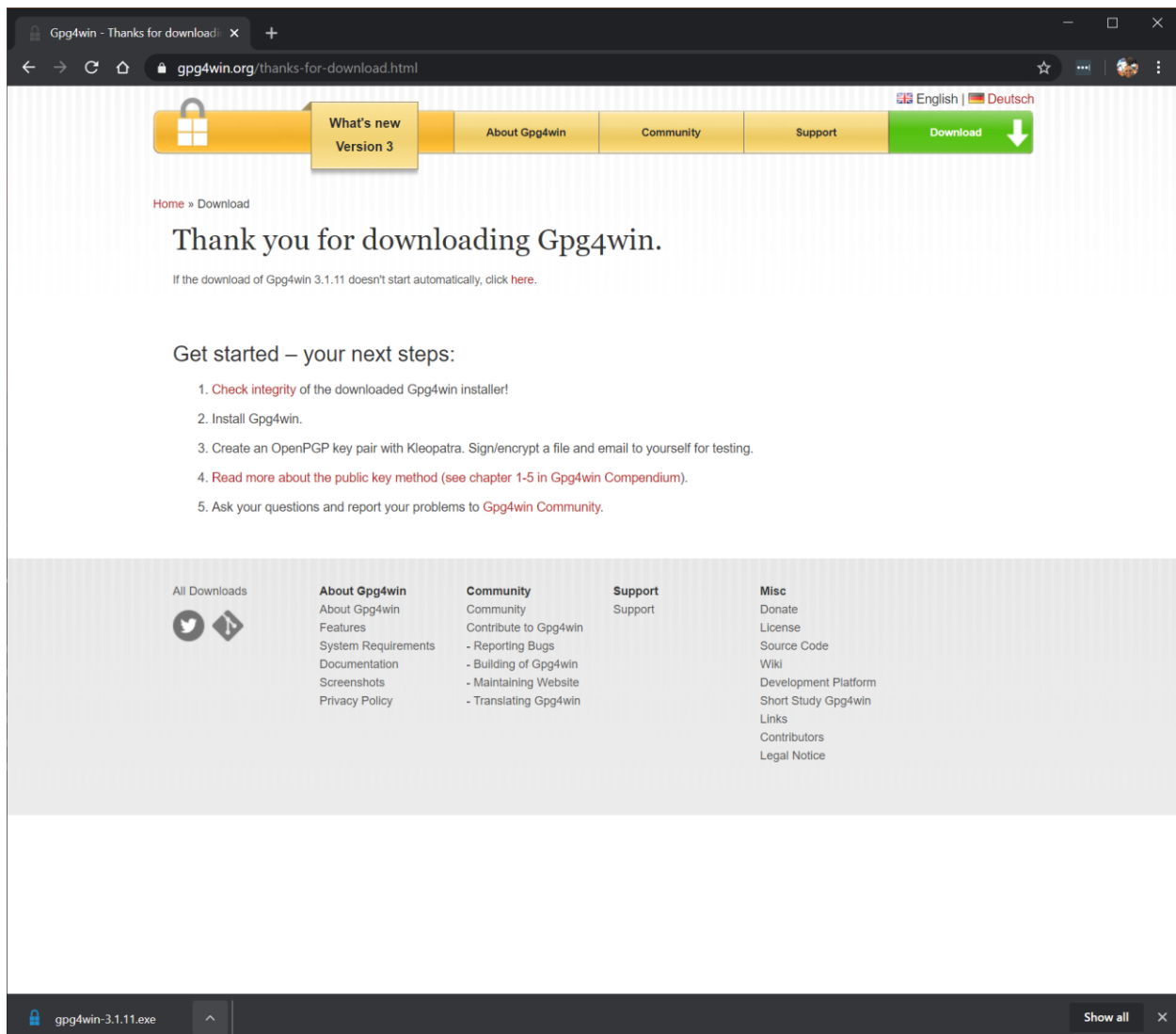
This lab report presents observations and explanations for the tasks described in the Configuration and Using GPG Lab Exercise (weisman\_gpg\_2\_2\_2.pdf).

## Step 1

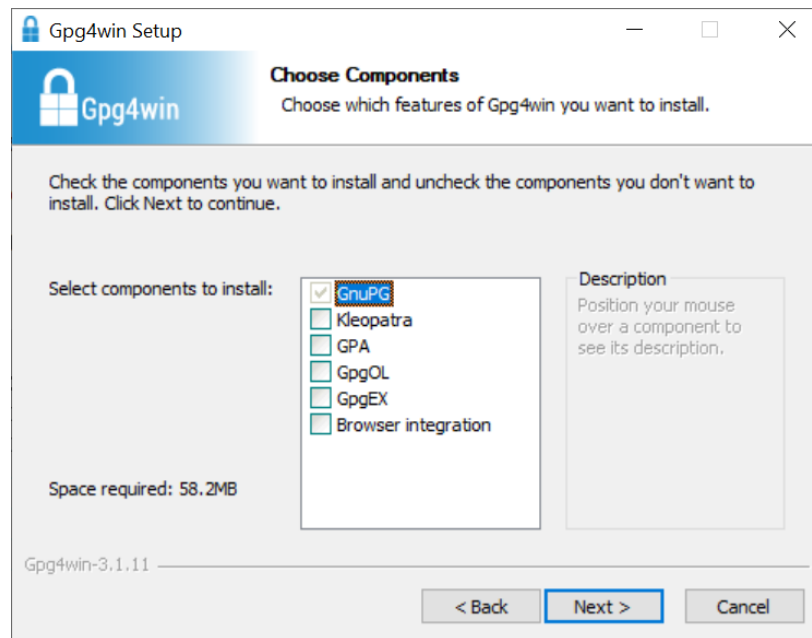
This section describes / shows each step performed per the exercise in Step 1.

### Step 1a

Download Gpg4Win.

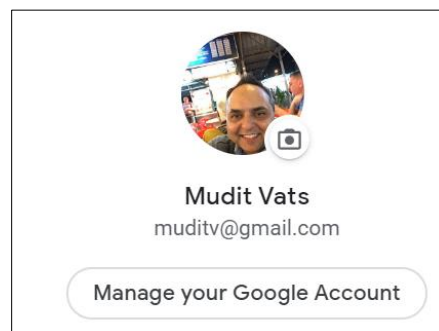


Uncheck all options except GPG.



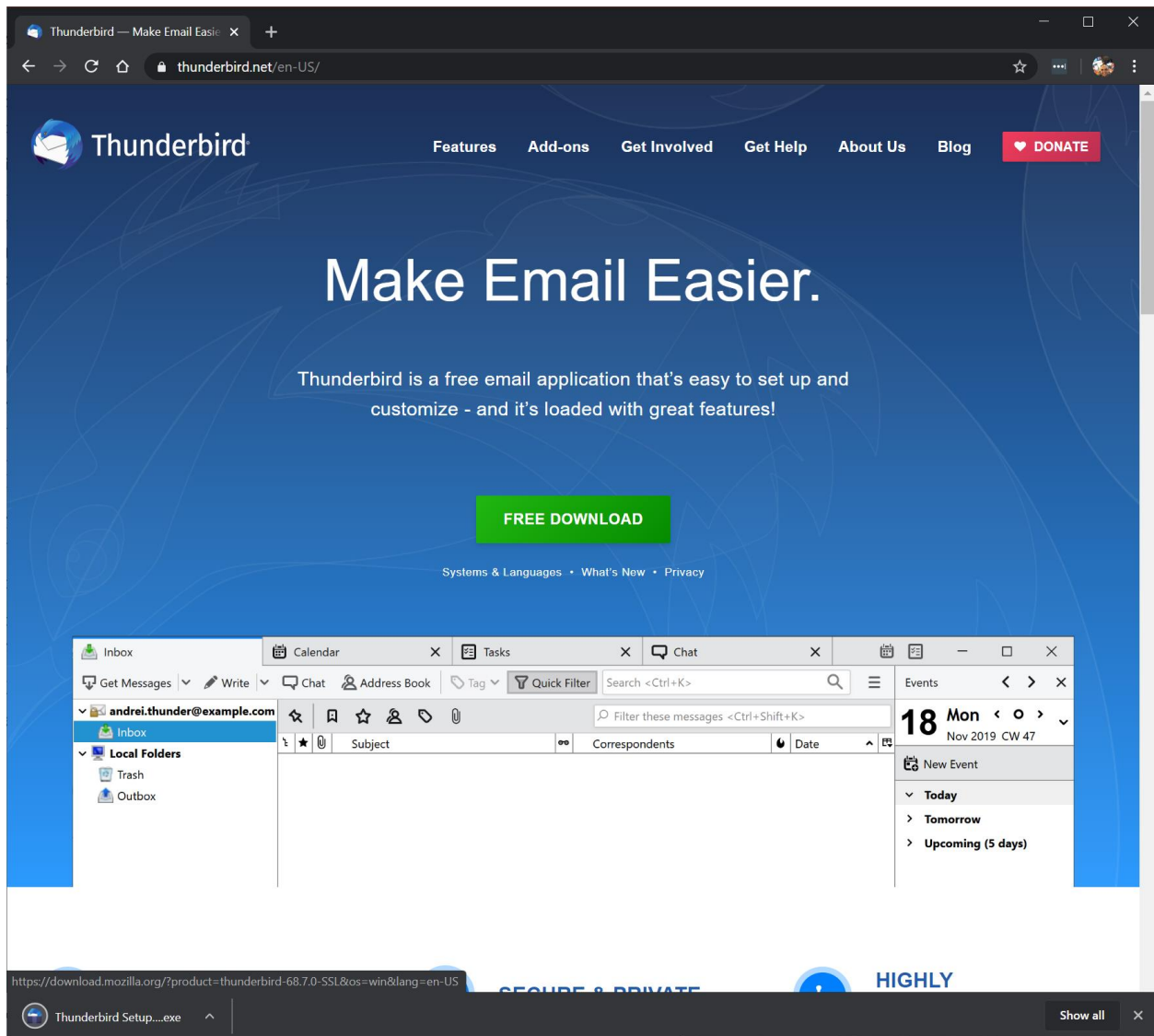
### Step 1b

Create Gmail account. I use this email as my primary personal email. Already created.

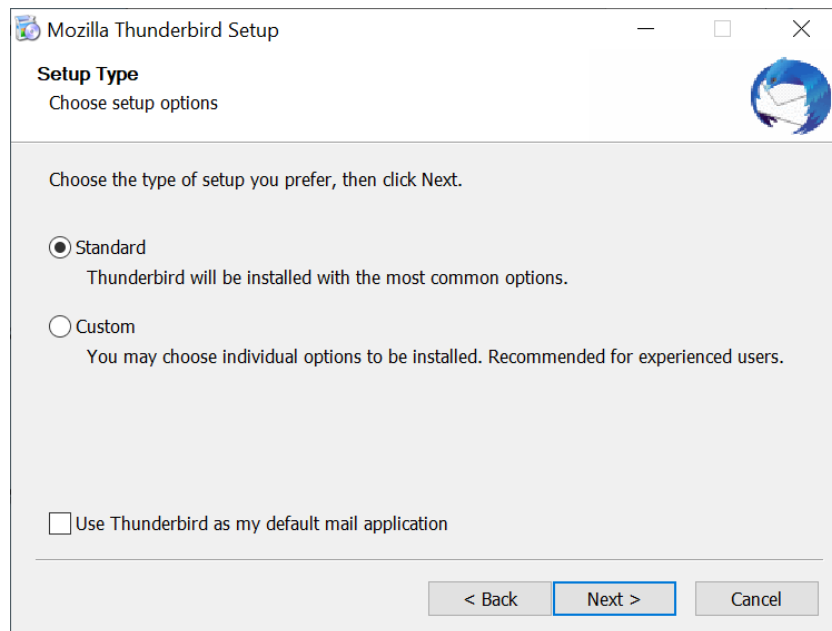
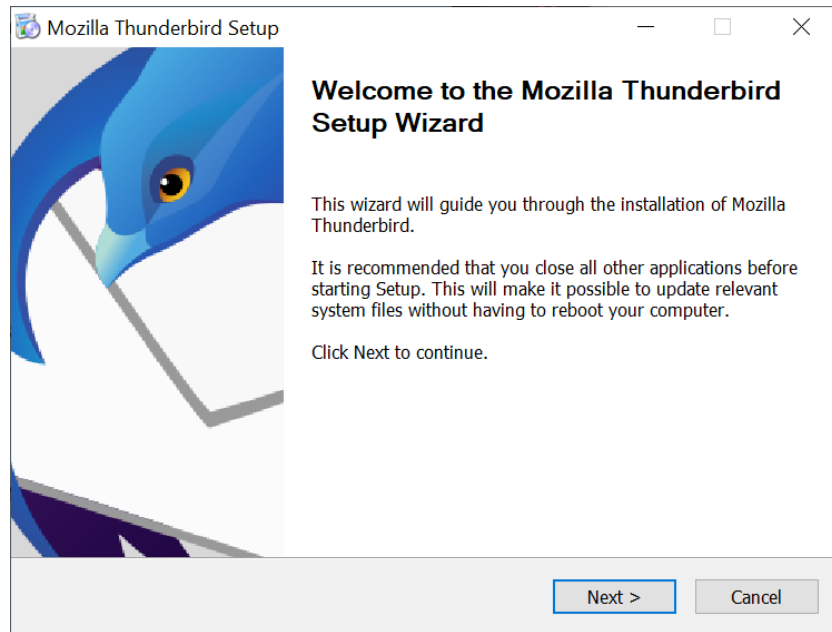


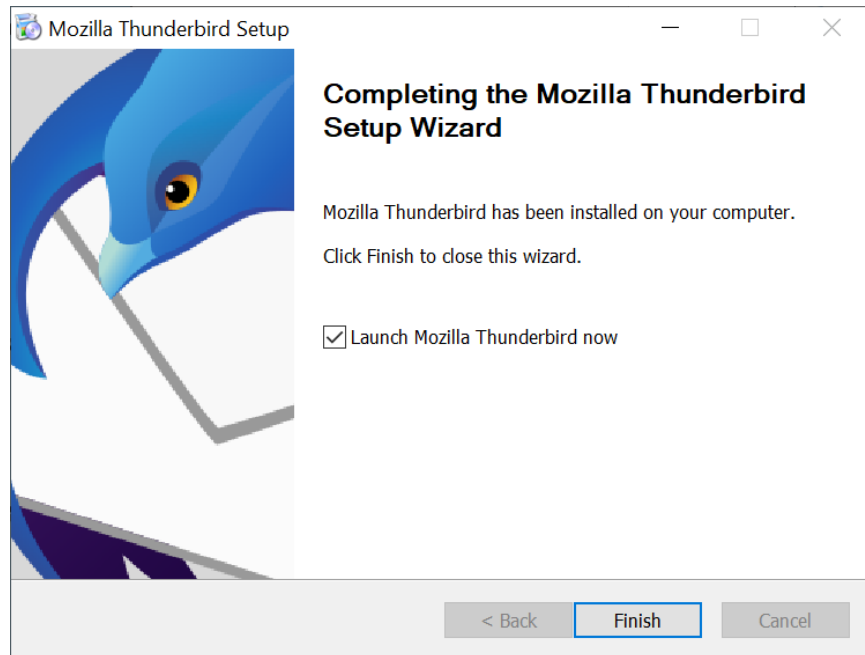
### Step 1c

Download Thunderbird.



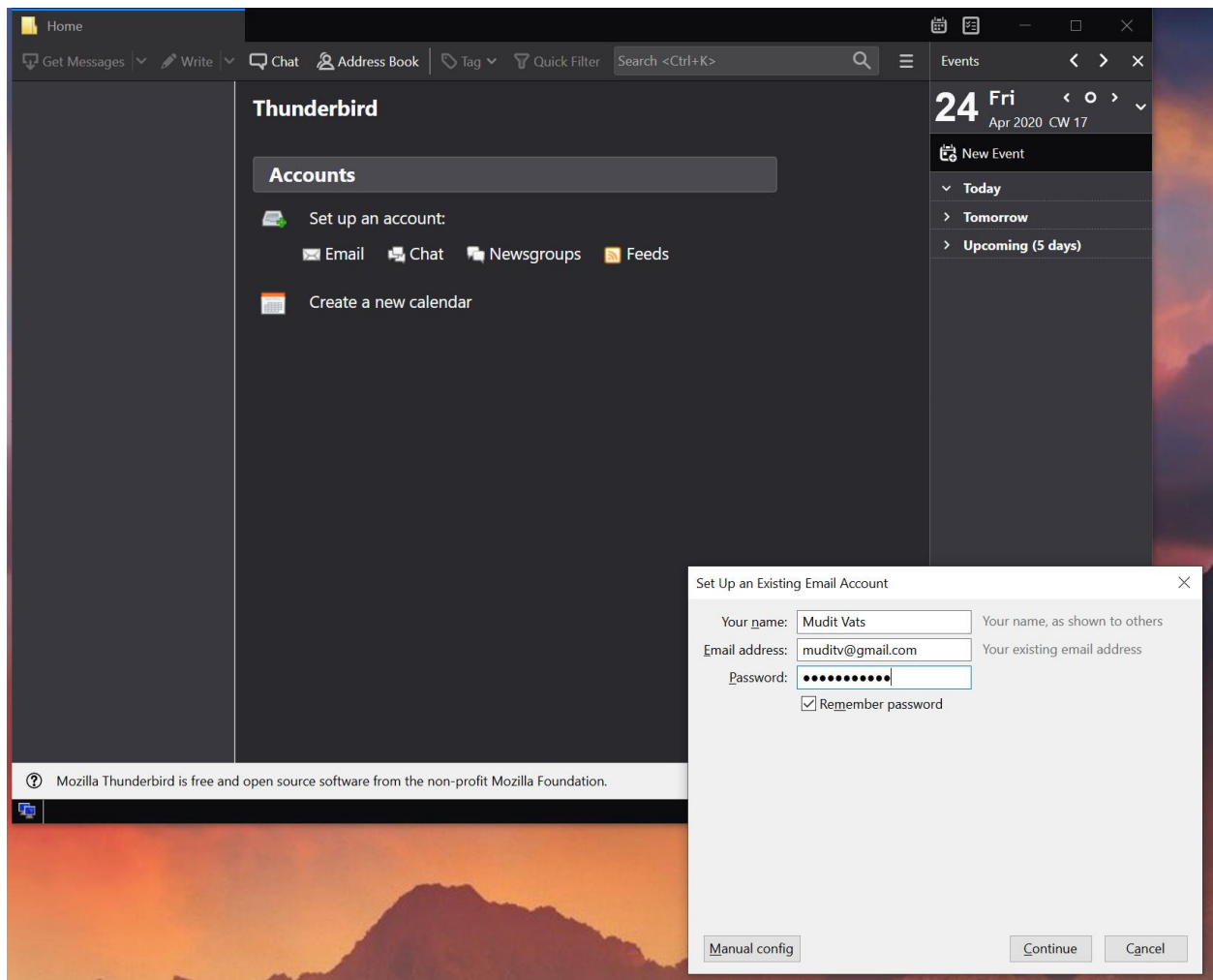
Install Thunderbird.





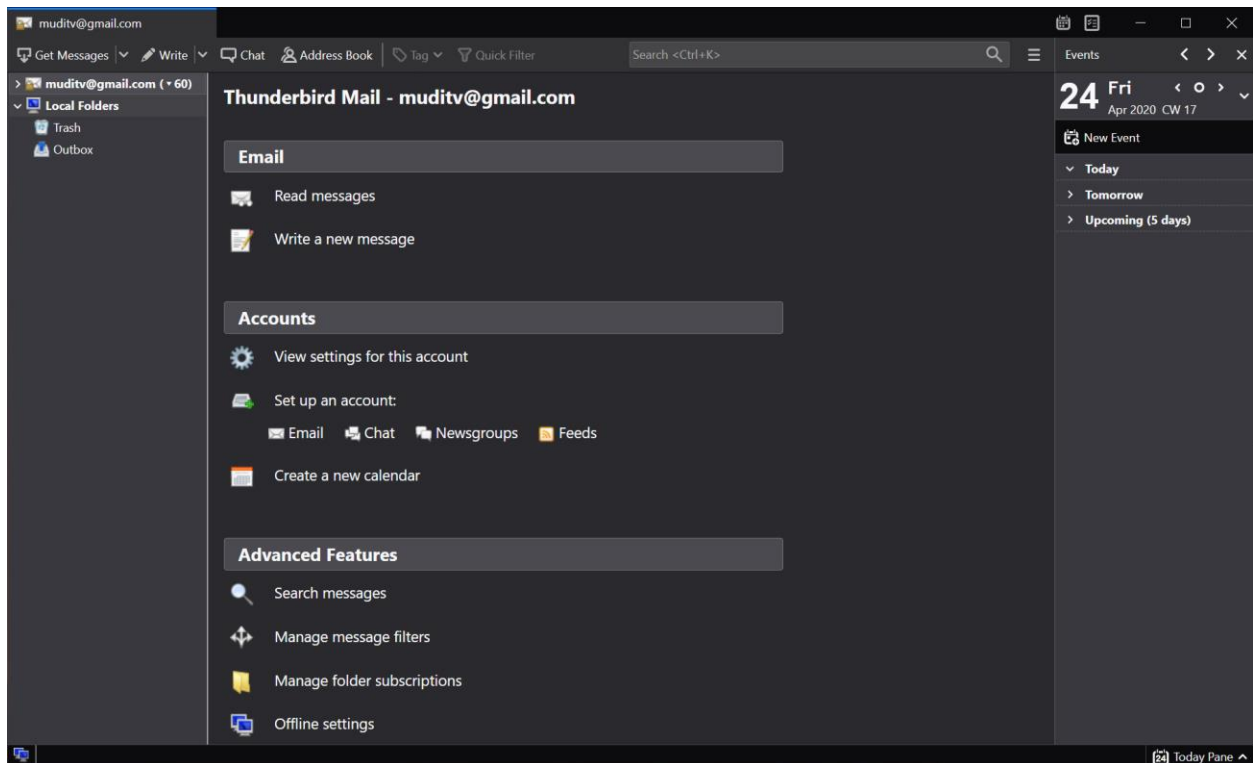
### Step 1d

Setup Existing Email Account.



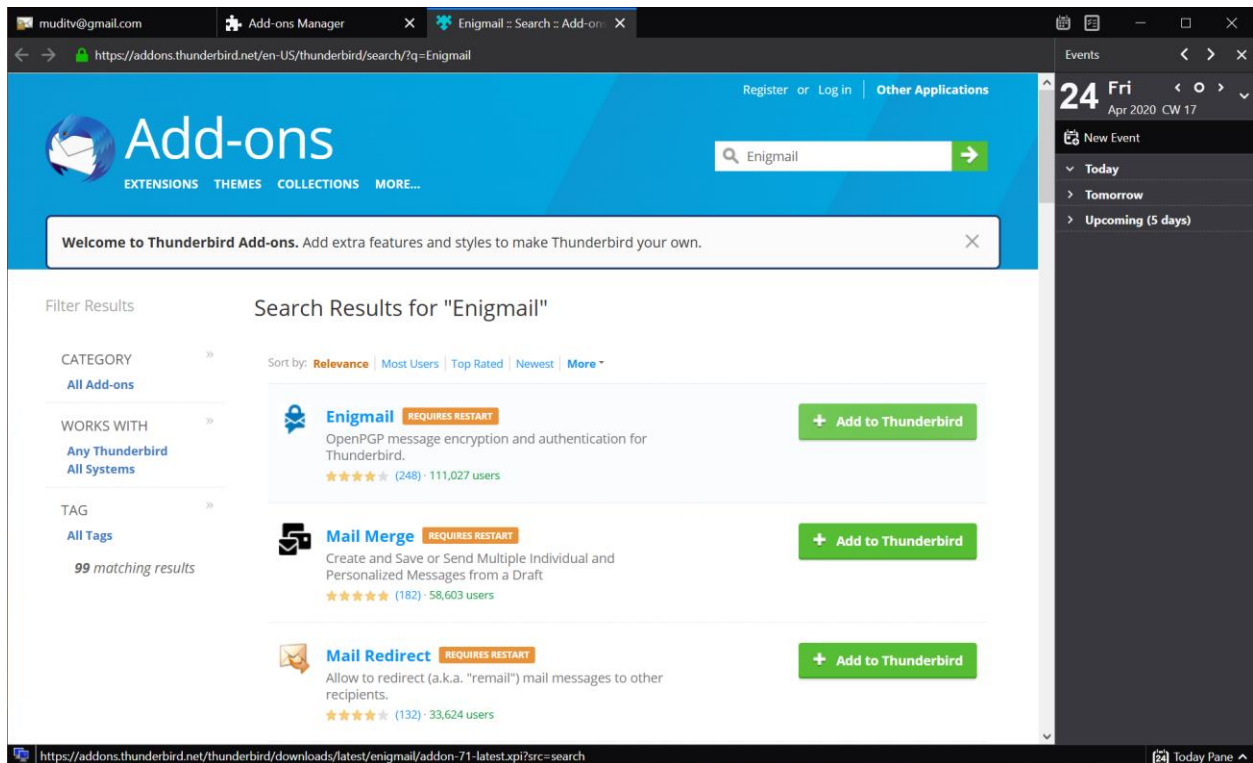
Thunderbird showing Gmail ([muditv@gmail.com](mailto:muditv@gmail.com)) successfully setup.



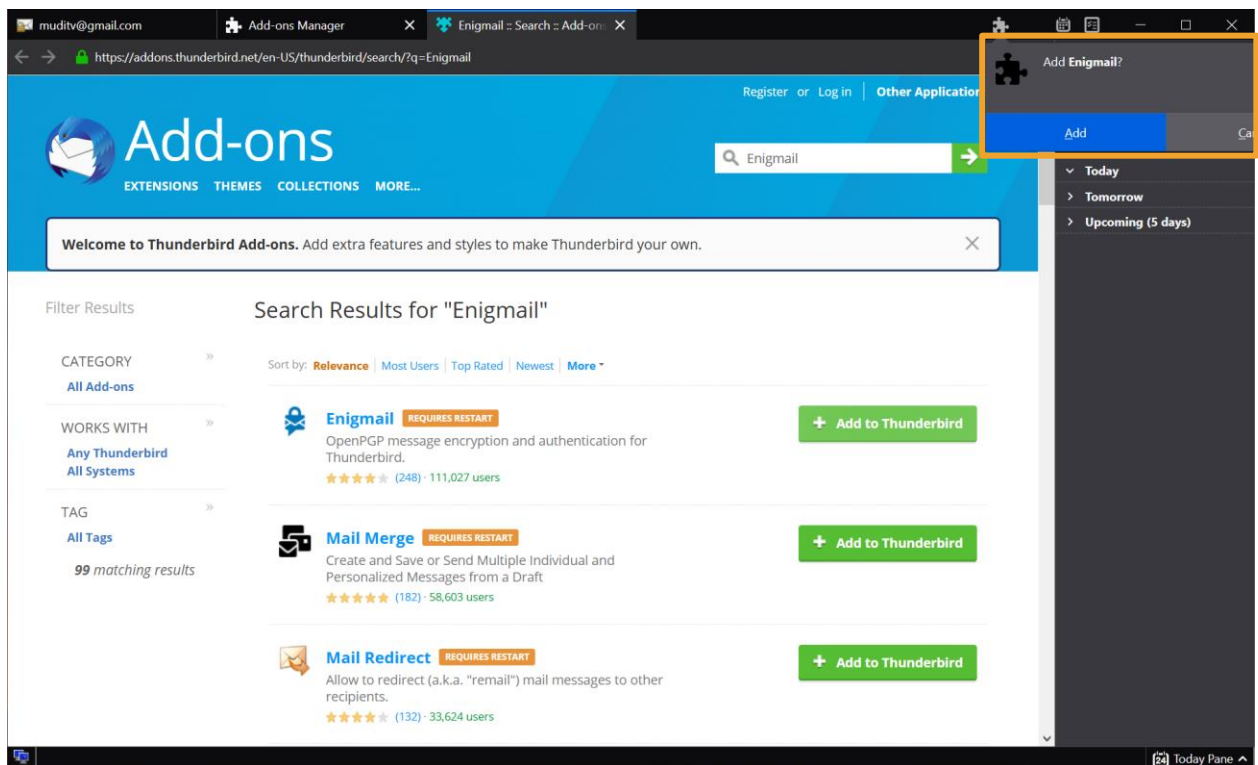


## Step 1e

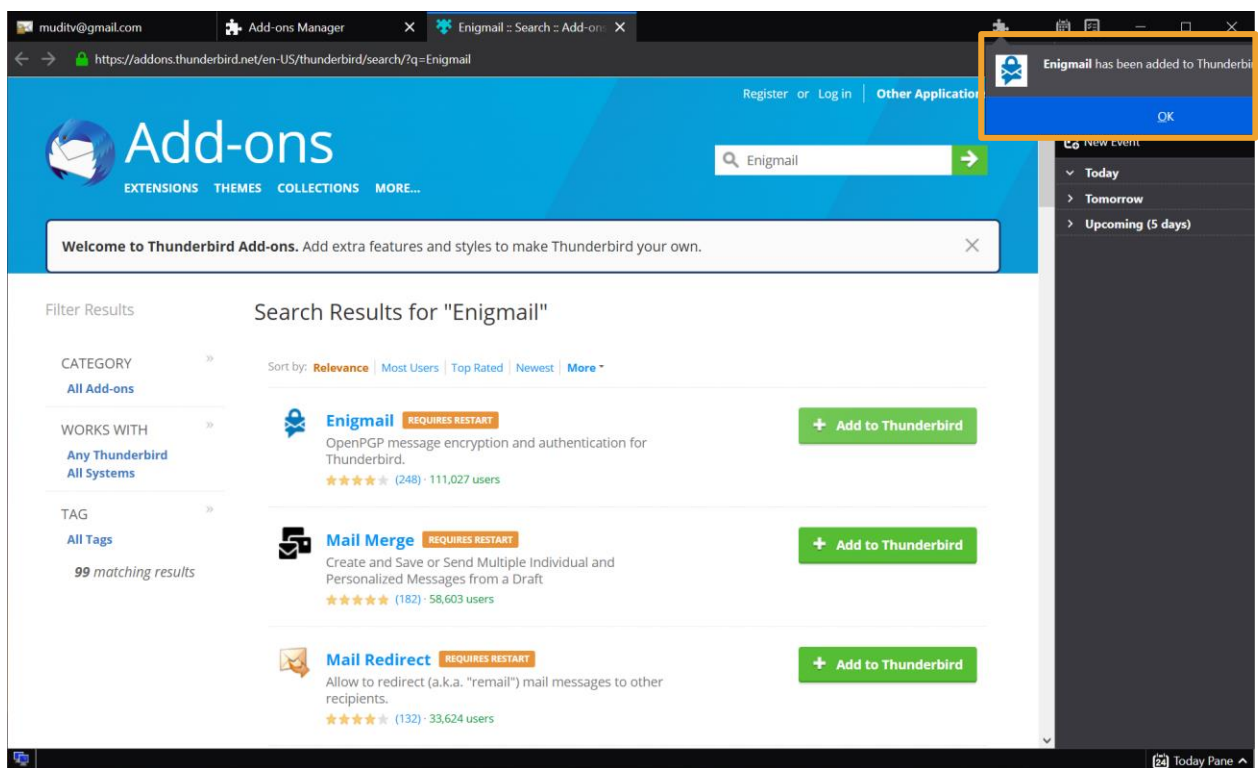
Add Enigmail addon.



Adding Enigmail.

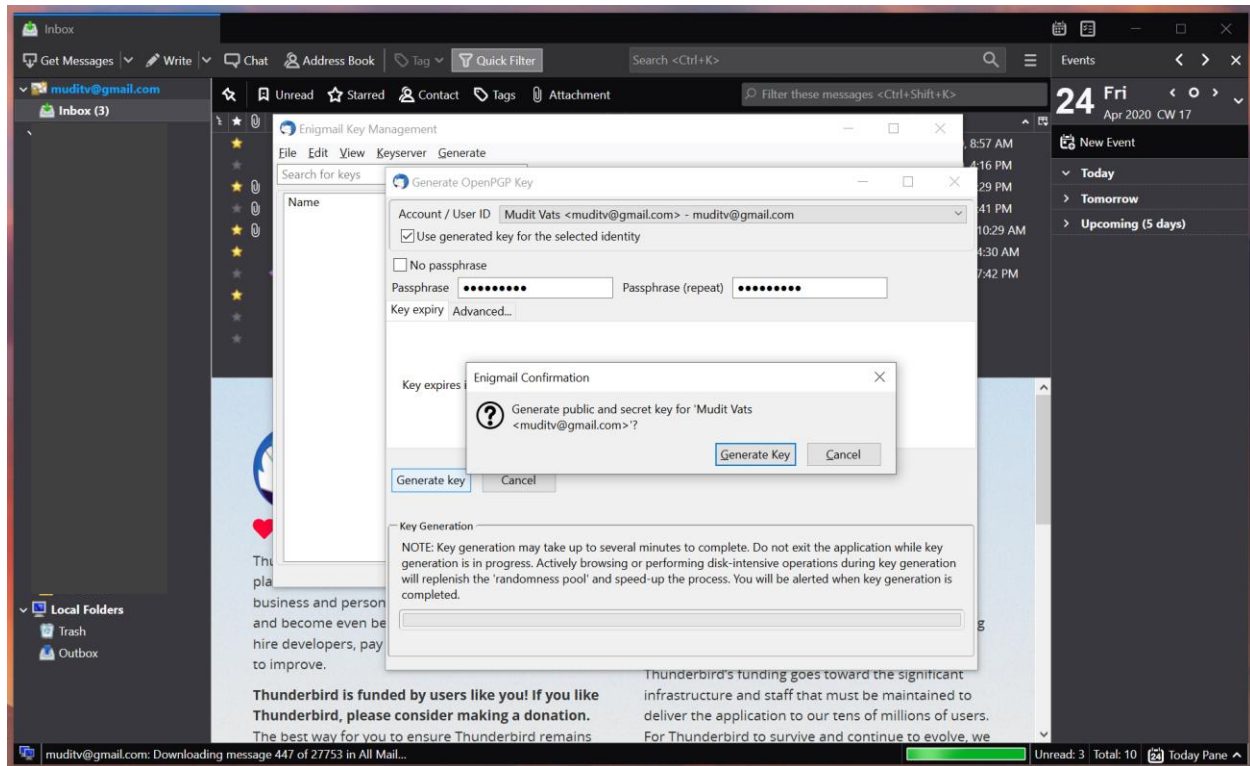


Enigmail successfully added.

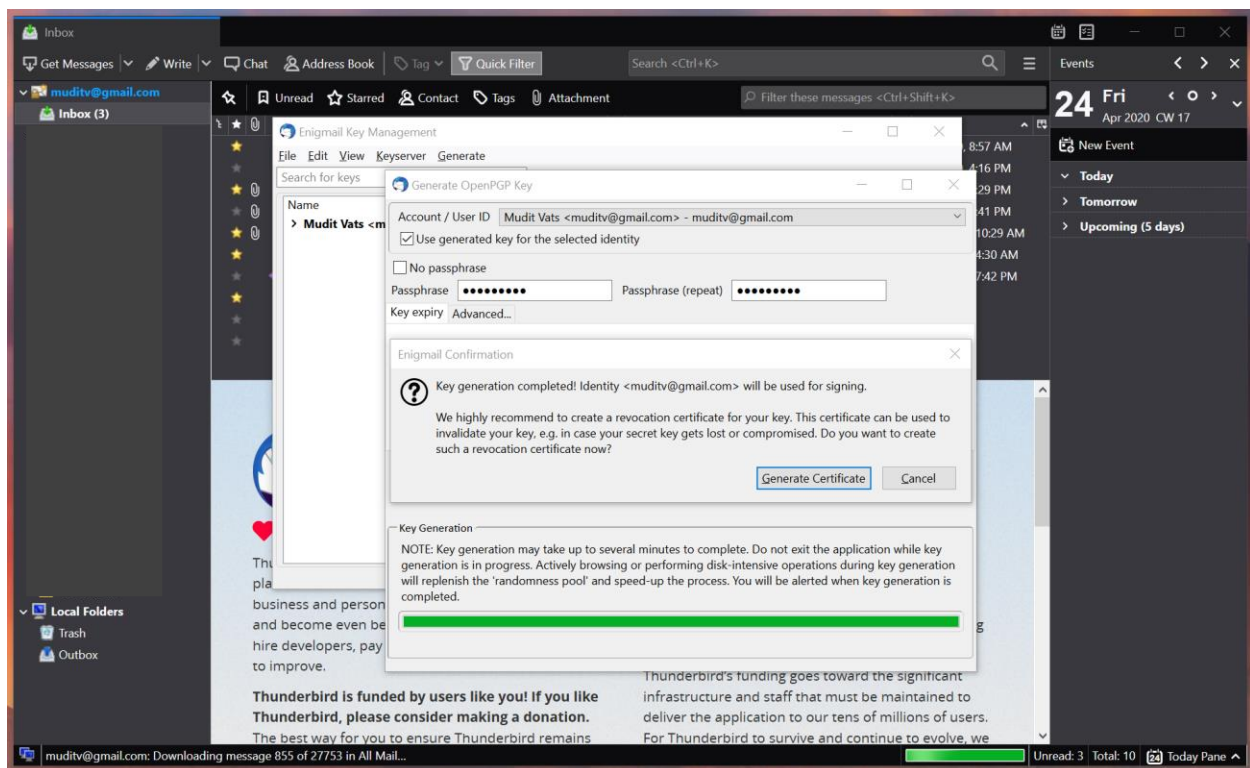


## Step 1f

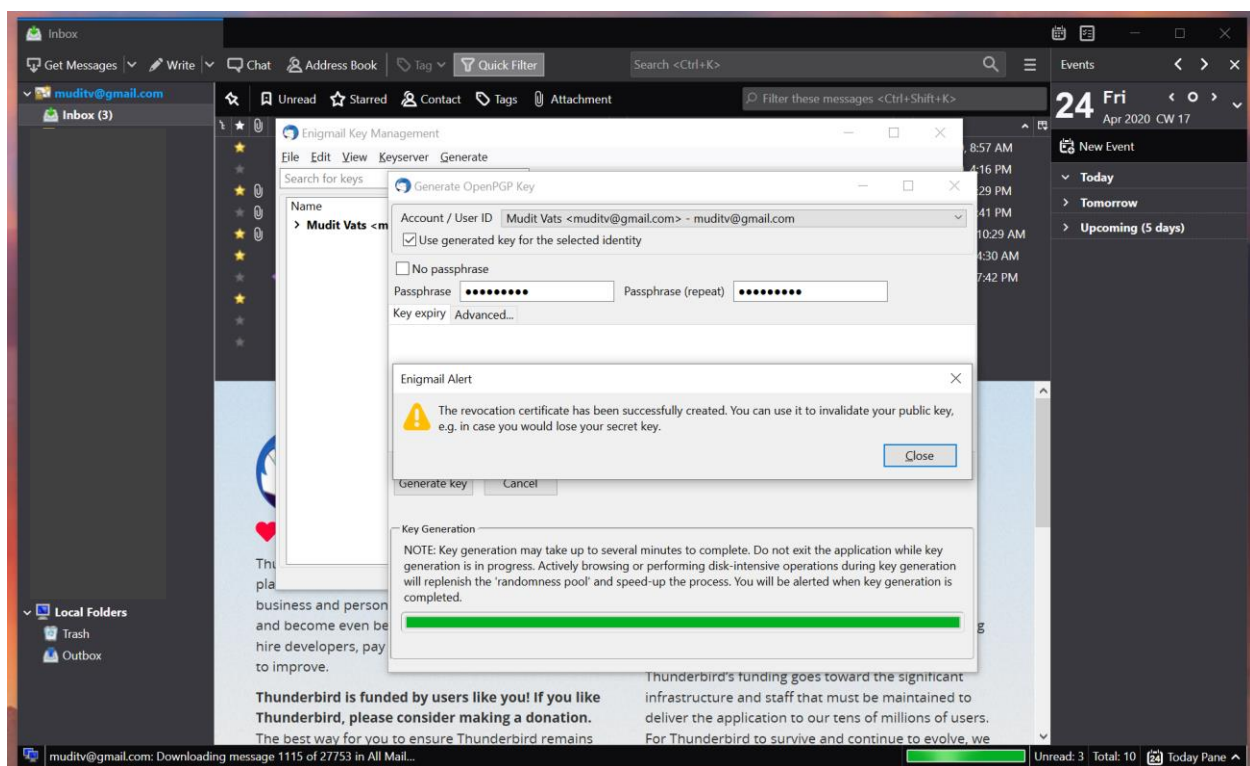
Generate Public / Private keys. The Setup Wizard did not work for me. It was able to find GPG, but it stalled on "Checking Your Existing Setup". I also double-checked the fix recommended in "enigmail\_fix\_2.pdf" and my setting were setup the same way. I therefore resorted to manually generating the public / private keys.



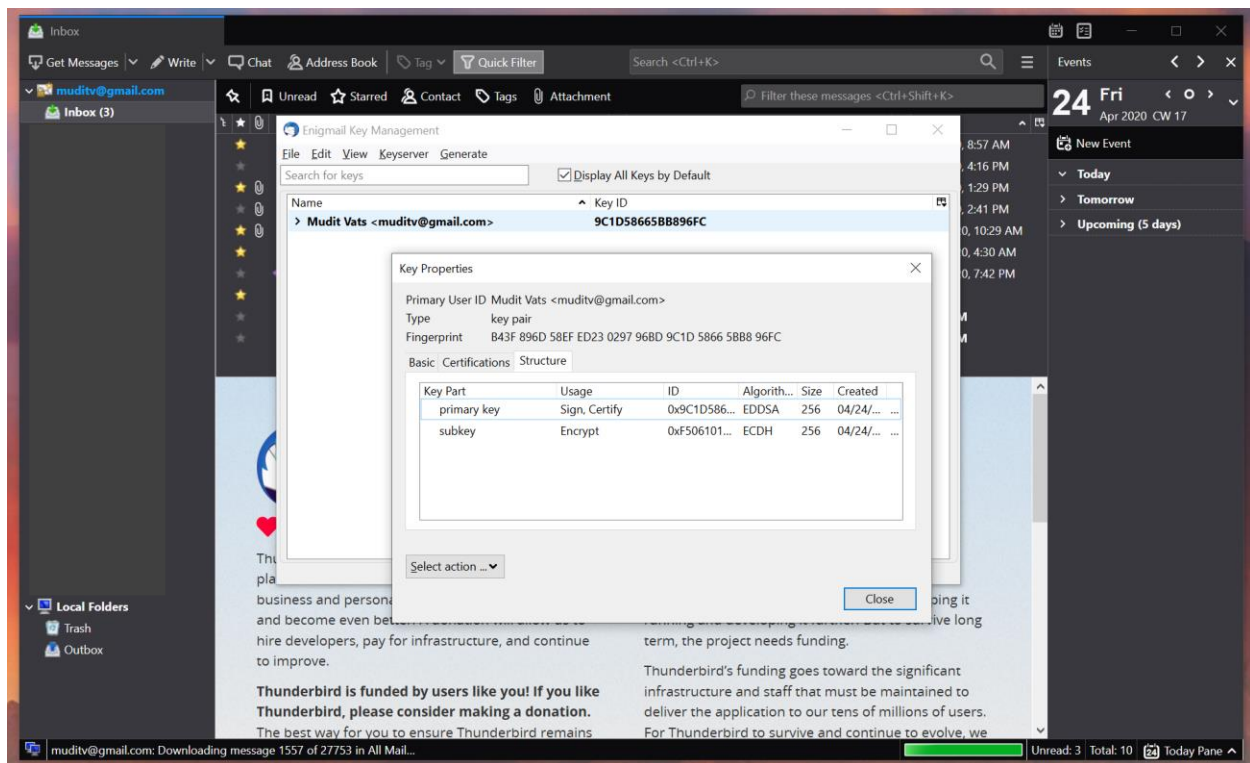
Generate Certificates.



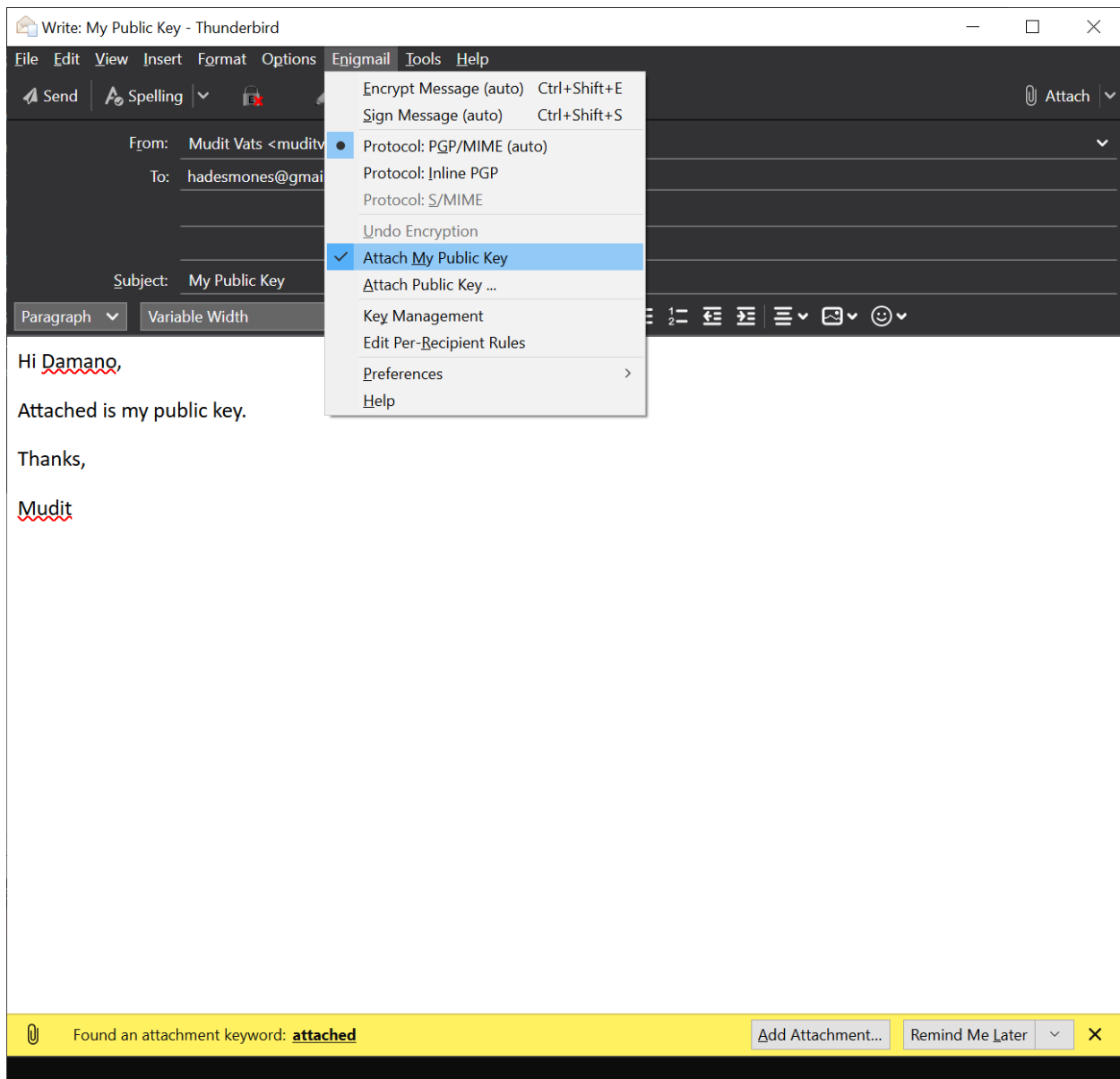
Save Revocation Certificate.



Final keys created.

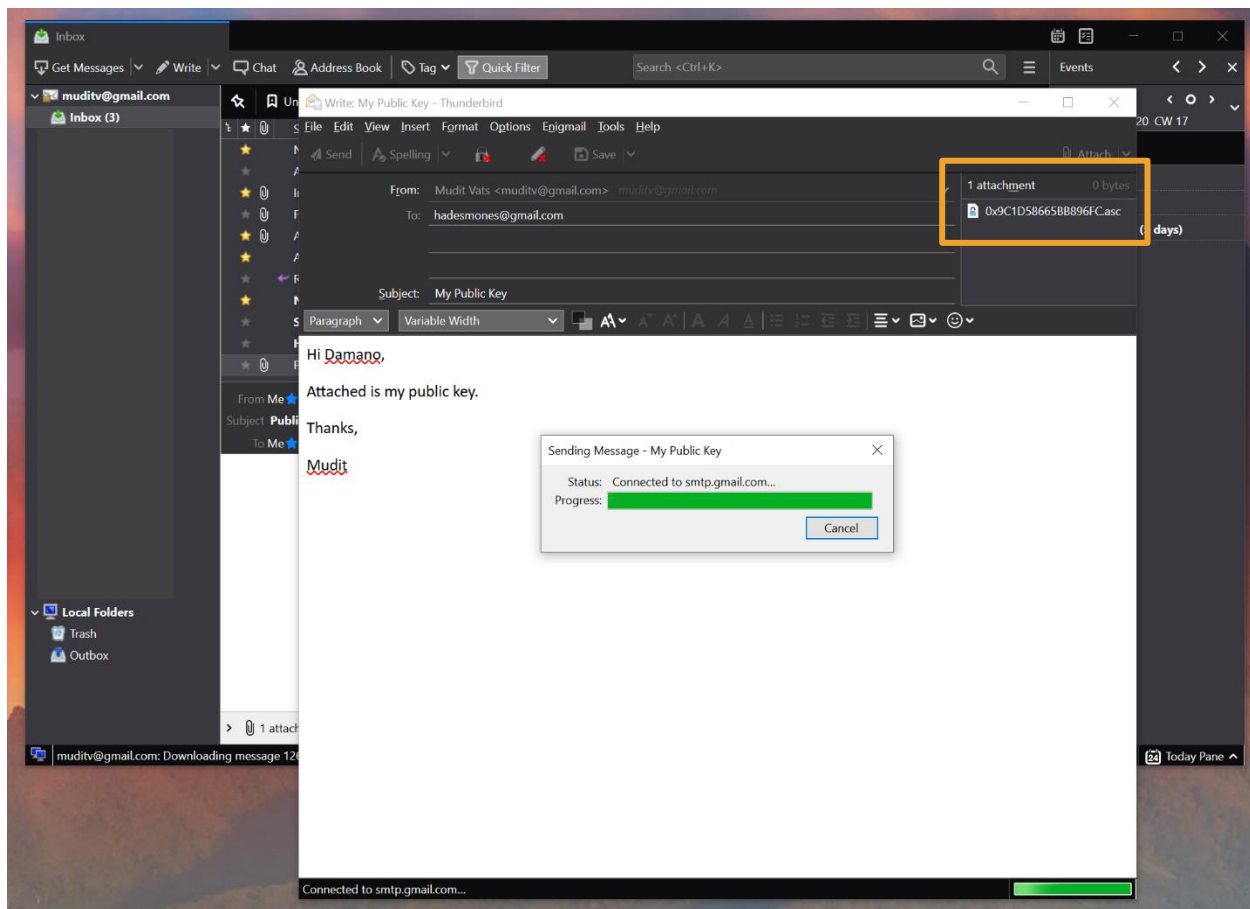


**Step 1g**  
Send public key.



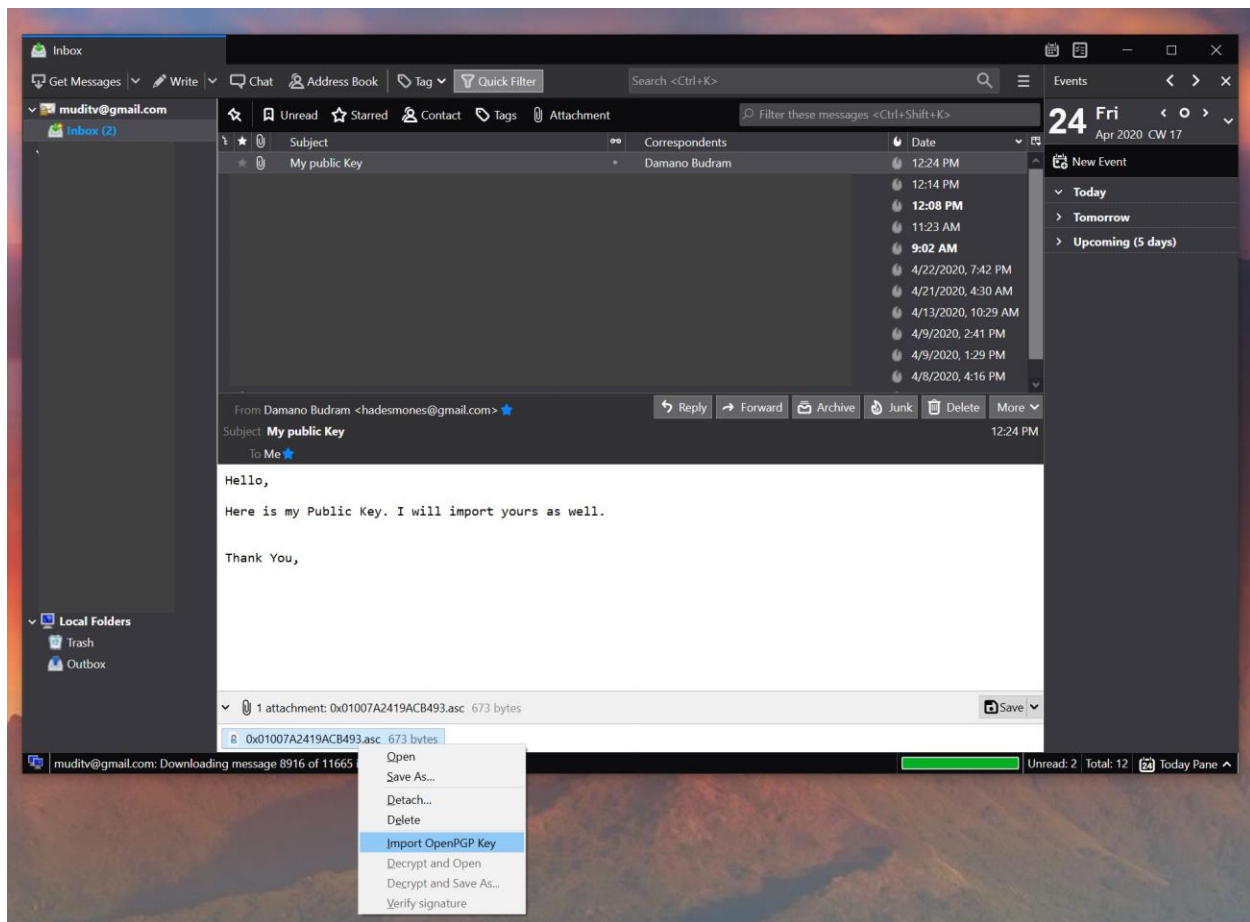
Send email to partner with attached Public Key. Attachment can be seen in the upper-right hand corner of the email. This is the file with the asc extension; i.e. my public key.





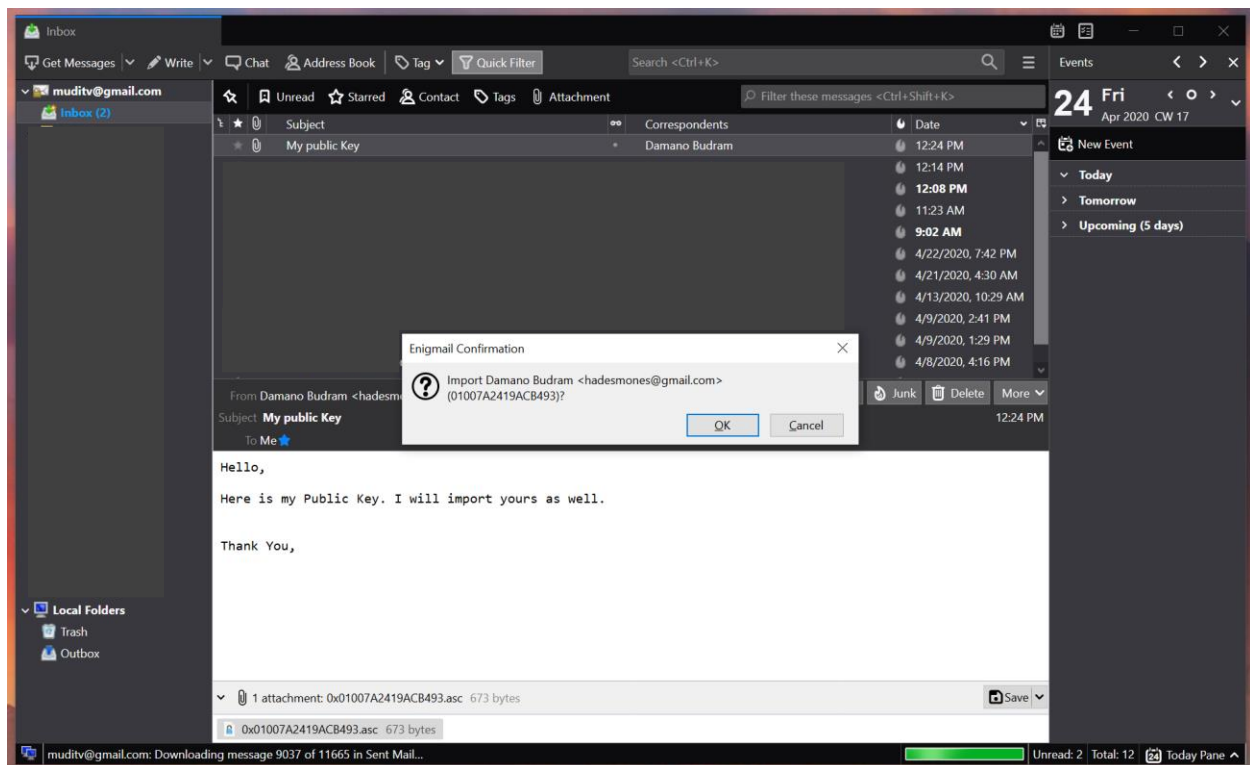
## Step 1h

Import partners public key. In the screenshot below, you can see the received message from my partner and me choosing the option to Import OpenPGP Key.

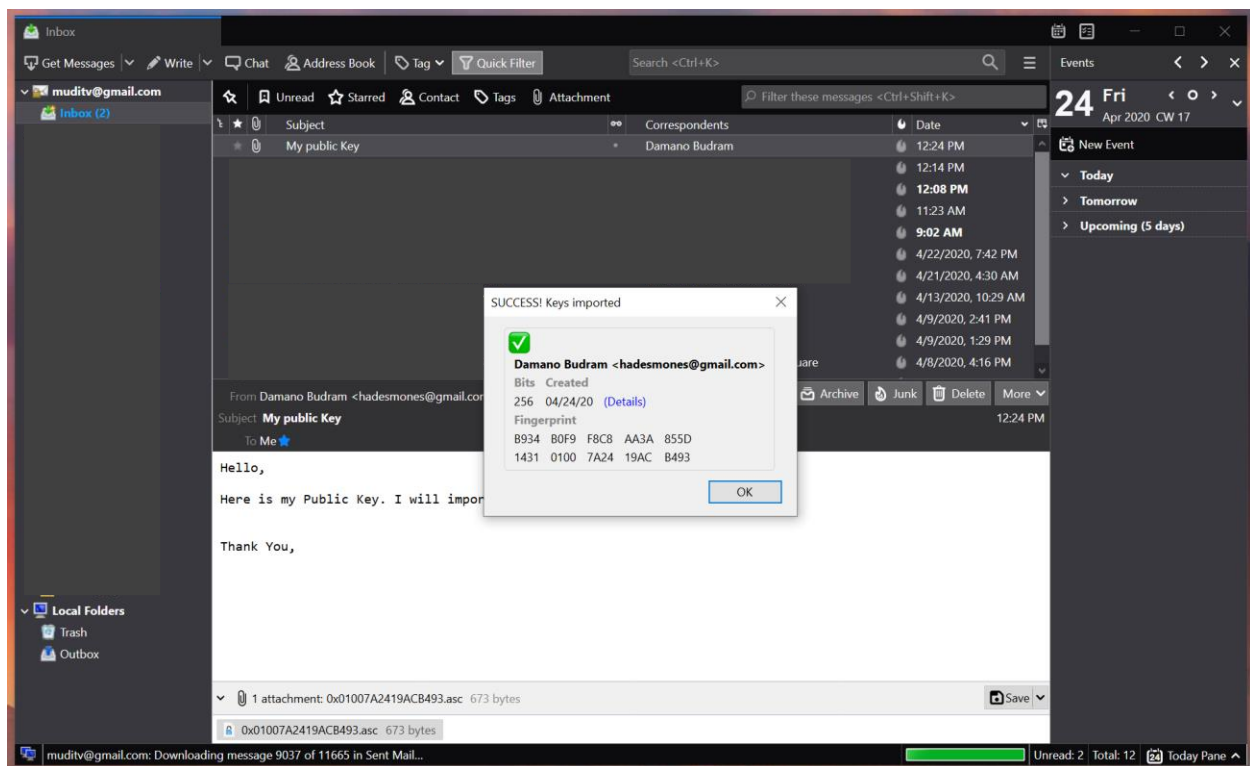


Below is the screenshot to confirm import.



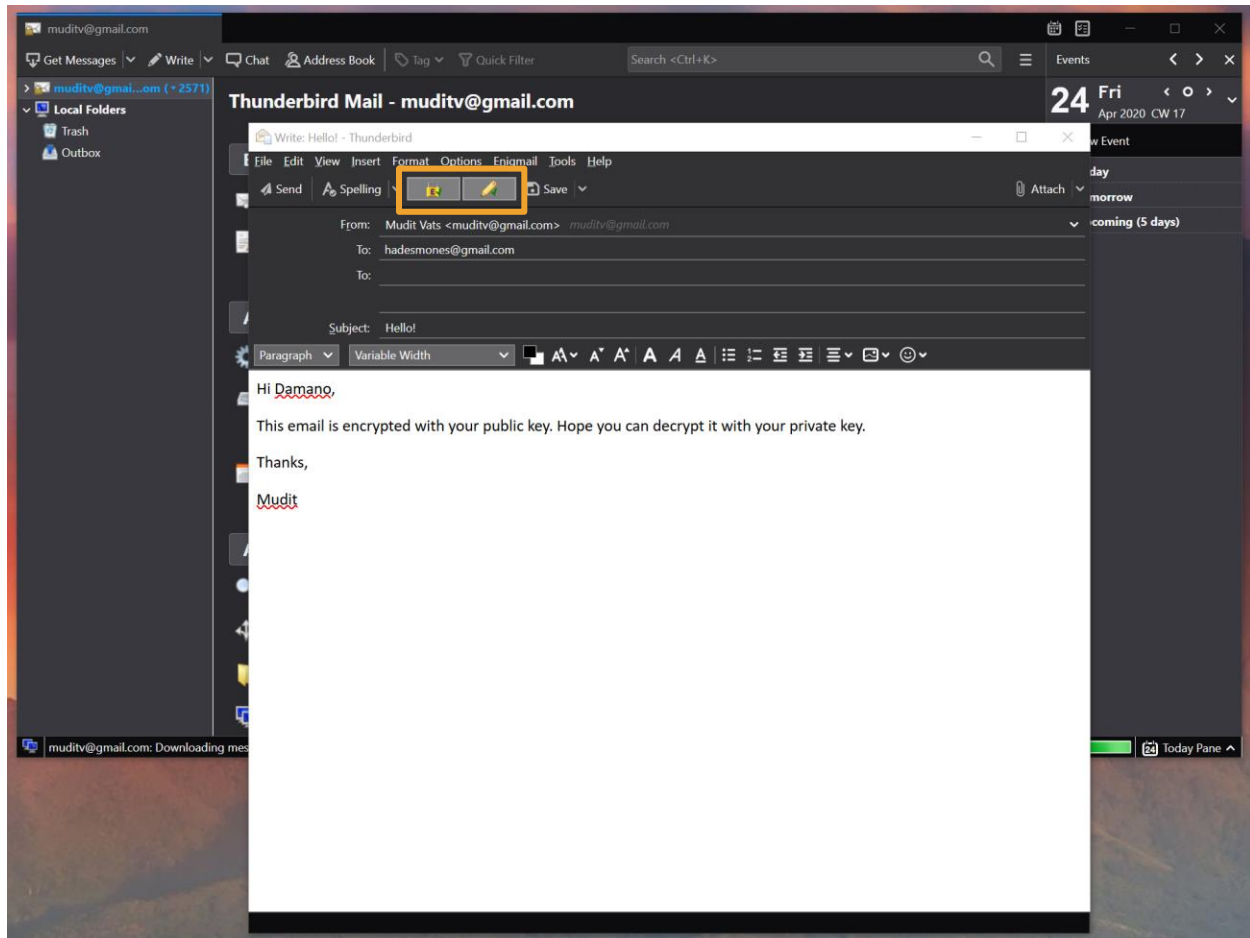


Final import success message.

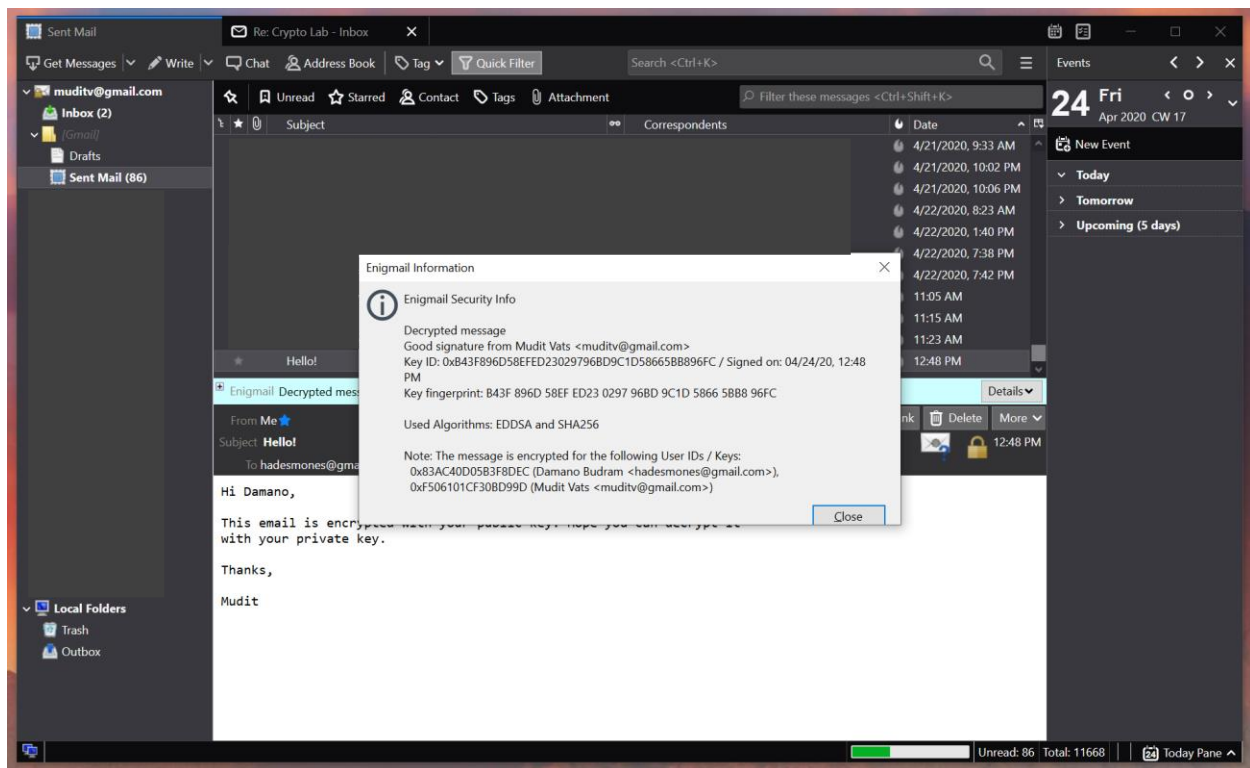


## Step 1i

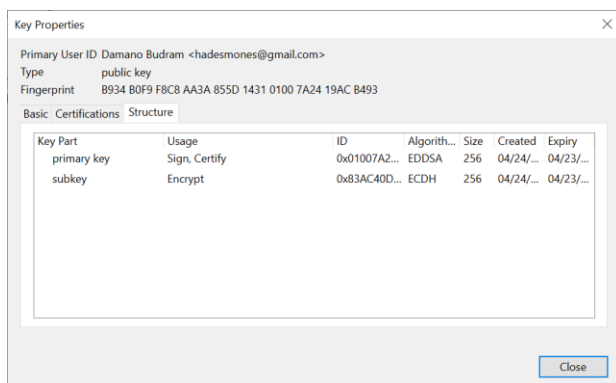
Send email to partner using their public key. The screenshot below shows me typing an email to my partner. The Encrypt and Sign icons are selected so the email message will be encrypted by the partner's public key and signed by my private key.



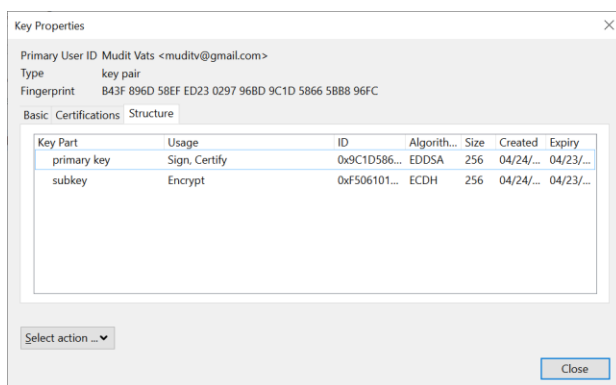
Looking at the details of the sent message below, we can see that the message signature is from Mudit (me, the sender) and it's encrypted for Damano (using his public key; 0x83AC... this is the subkey of Damano) and the sender (me using public key 0xF506... this is the subkey for Mudit).



Primary and subkey of partner, Damano.

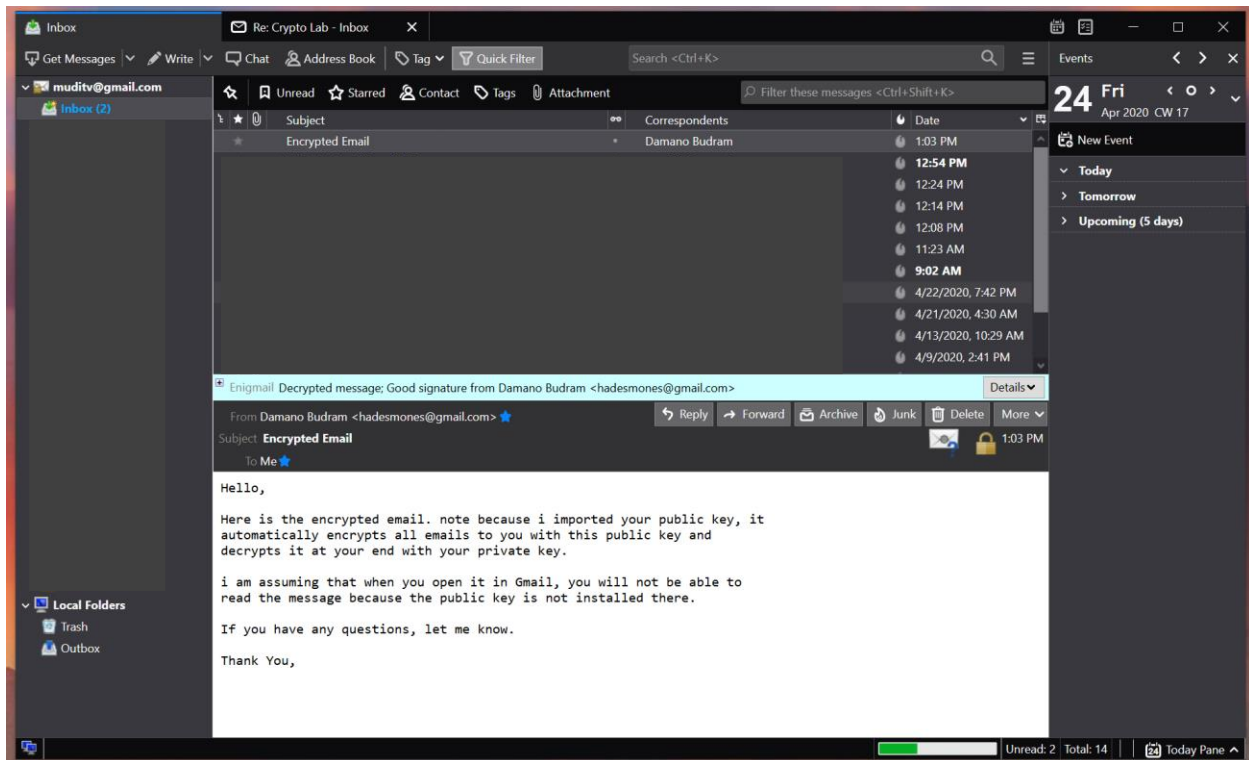


My primary and subkey.

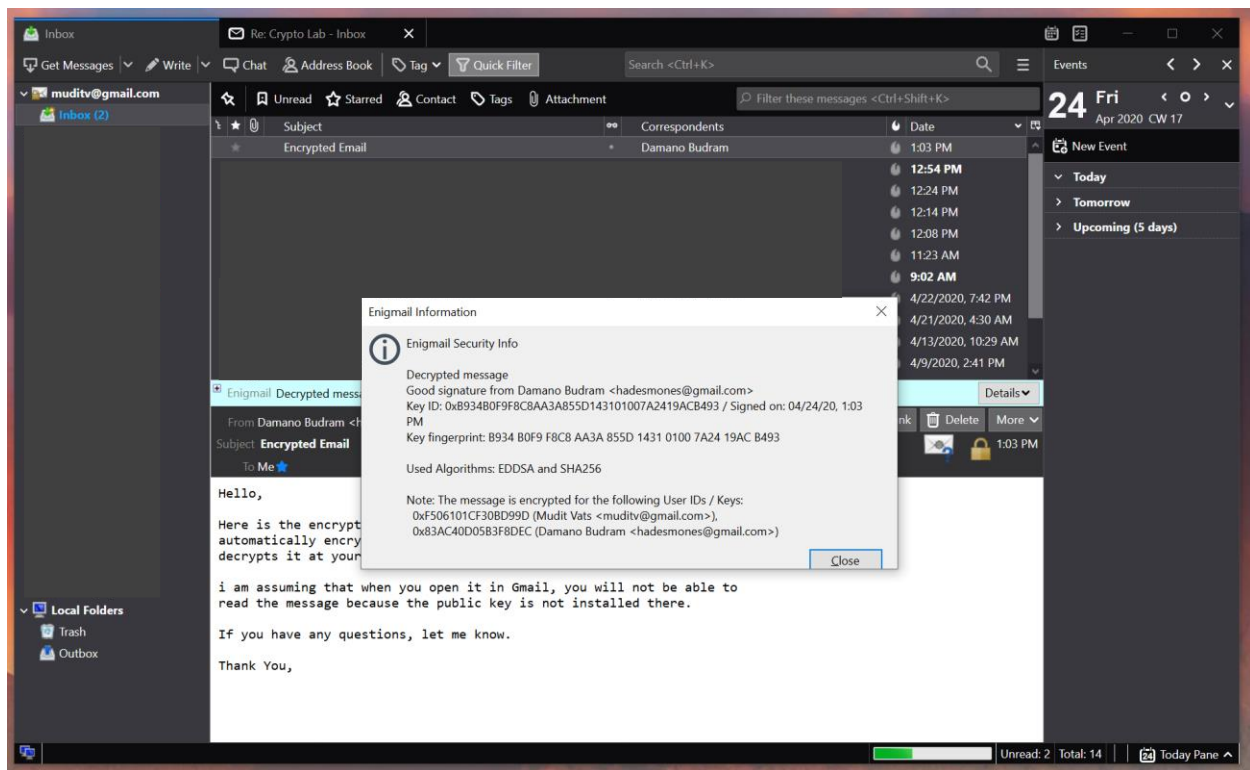


## Step 1j

Open partners mail below. Upon selecting the email, it is decrypted. We can see the "Decrypted message; Good signature from Damano Budram".

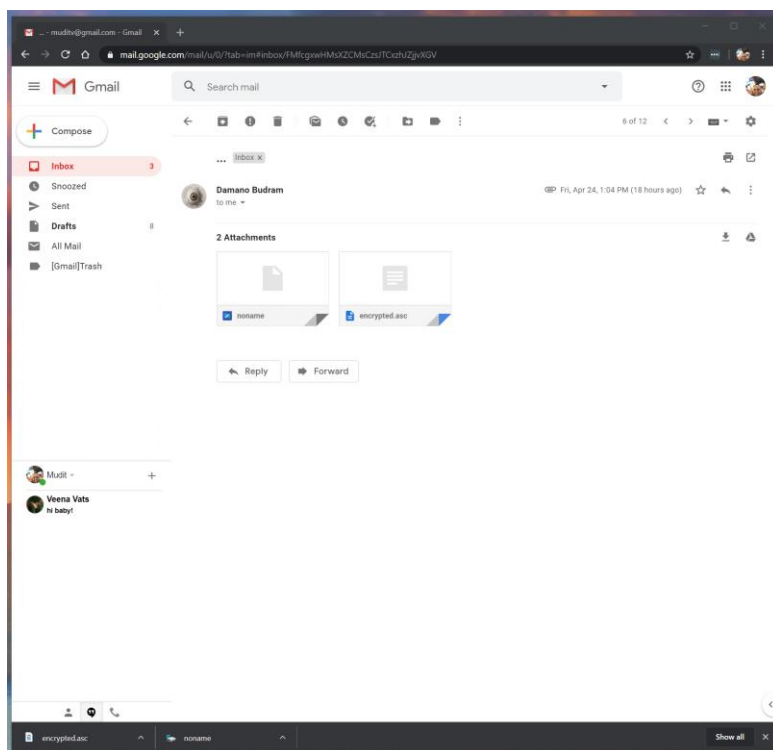


Getting more details on the message, we can see that the signature was from my partner, Damano. We can also see that the message was encrypted using the public keys for Damano and Mudit below. In the previous section, these were identified as the subkey's for Damano and Mudit respectively.



## Step 1k

View email from Google Gmail. The messages are actually attachments, including the encrypted message.



## Step 2

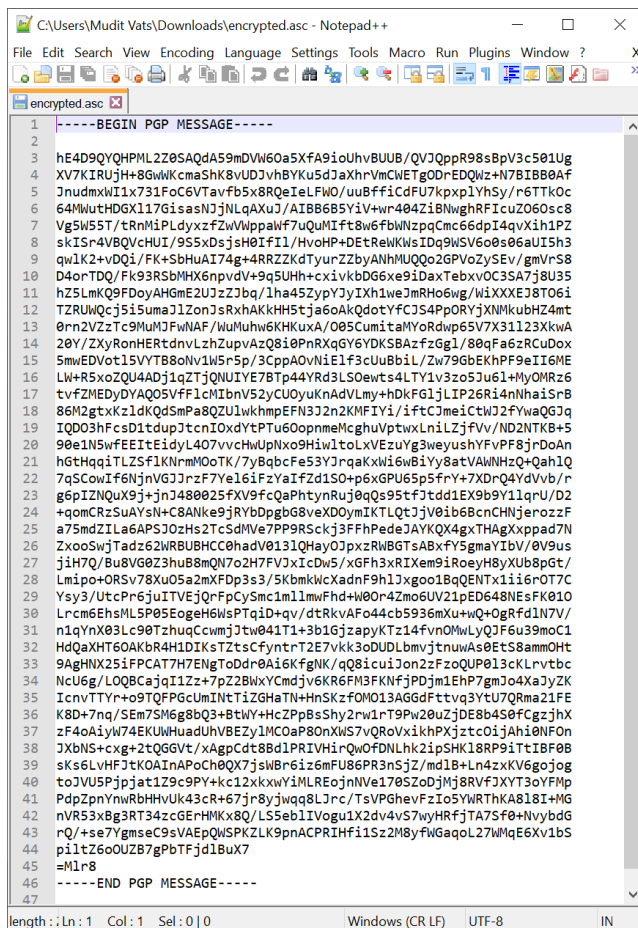
This section describes / shows each step performed per the exercise in Step 2.

### Step 2a

Q: How does the e-mail look in the Web browser compared to how it looks in Thunderbird? Why is this the case?

The email looks like an empty email message with attachments. The attachments include the “encrypted.asc” which is encrypted message and a “noname” file which contains version info.

If we look at “encrypted.asc” file we see the content to be an ascii encrypted message.



```
1 -----BEGIN PGP MESSAGE-----
2
3 hE4D9QYQHPL2Z0SAQdA59mDVW60a5XFA9i0UhvBUUB/QVJQppR98sBpV3c501Ug
4 XV7KIRUjH+8GwWkCmaShK8vUDJvhBYKu5d3aXhrVmcWETgODrEDQWz+N7BIBB0Af
5 JnudmxWl1x731Foc6VTavfb5x8RQeIeLFwO/uuBff1CdFU7kpxp1YhSy/r6TTkOc
6 64MwtHDGX117GisasNjJNLqAXuJ/AIBB6B5Y1V+wr404ZiBNwghRFIcuZ060sc8
7 Vg5W55T/tRnM1PLdyxzFZWVppawf7uQuMIft8w6FbWVzpqCmc66dpI4qvX1h1PZ
8 skISr4VBQvCHUI/955xDSjsH0IF1I/HvoHP+DEtReWkWSIDq9WSV60s06aUI5h3
9 qwLK2+vDQ1/FK+SbHuAI74g+4RRZZKdTYurZZbyANhMUQqo2GpVoZySeV/gmVrS8
10 D4orTDQ/Fk93R5bMHX6npvdV+9q5UHH+cxivkbDG6xe9iDaxTebxvOC3SA7j8U35
11 hZ5LmkQ9FDoyAHGmE2UjzZ3bq/1ha452ypYjYIXh1weJmRHo6wg/WiXXEXEJ8T06i
12 TZRUWQcJ5i5umaJ1ZonJ3sRxhAKkH5tja6oAkQdotYfCJ54PpORYjXNMkubHZ4mt
13 0rn2VZzTc9MuMjFwNAF/WuMuhw6KHkuxA/O05CumitaMYoRdwp65V7X31123Xkwa
14 20Y/ZXyRonHERtdnvlzhZupvAzQ8i0PnRXqGY6YDKSBAzfzGg1/80qFa6zRCuDoX
15 mmwEDVot15VYT88oN1w5r5p/3CpPA0vN1E1f3cUuBb1L/Zw79GbEKHPF9eII6ME
16 Lw+R5xoZQU4ADj1qZTjQUYIE7BTp44Yrd3LS0ewts4LTy1v3zo5Ju61+MyOMRz6
17 tvfZMEDyDYAQ05VFf1cMIbnV52yCUoyuKnAdVLmy+hDkF61jLIP26Ri4nNhaiSr8
18 86M2gtxKz1dKQd5mPa8QZU1wkhmpEFN3J2n2KMFIY1/iftCJmeiCtWJ2FywaQGJq
19 IQD03hFcsD1tdupJtcnIOxdYtPTu6OopnmMcghuVptwxLn1LZjFVv/ND2NTKB+S
20 90e1N5wFEEItEidyl407vvcHwUplNxo9HivLtoLxVEZuYg3weyuyYFvPF8jrd0An
21 hgThqaiTLZ5f1KnmM0oTK/7yBqbcF53YJ3rqAKw16wB3Yy8atVAINHzQ+Qah1Q
22 7qScowIf6NjnvGJJrzF7Ye16iFzYaIfZd1SO+p6xGPU65p5FrY+7XDnQ4YdVvb/r
23 g6pIZNQX9j+jn3480025XV9fCqPahptynRuJ0qQs95tfjtd1EX9b9Y11qrU/D2
24 +qomQRZ5uAYsN+C8ANke9jRYbDpgb68veXDOymIKTLQtjV0ib68cnCHNjerozF
25 a75mdZLa6APSJ0zHs2TcSdMVe7PP9R5ckj3FFhPedeJAYKQX4gxTHAgXppad7N
26 ZxooSwjTadz62WRBUBHCC0hadV0131QHayOJpxzRWBGTSABxPY5gmaYIbV/0V9us
27 j1H7Q/Bu8V68Z3uB8mQN7o2H7FVJXicDw5/xGFh3XRIXEm9iRoeyH8yXub8pGt
28 LmiPo+OR5v78Xu05a2mXFDp3s3/5KbmkWcXadnF9h1Jxgoo1BqQENTX1i16rOT7C
29 Ysy3/UtcPr6juITVEjQrFpCysmc1m1mwFhd+W0R4Zmo6UV21pED648NEsFK010
30 Lrcm6EhsML5P05EogeH6WsPtq1d+qv/dtRkVAFo44cb5936mXu+wQ+OgRfd1N7V/
31 n1qYnX03Lc90TzhuqCwmjJtw041T1+3b1GjzapyKTz14Fvn0MwLyQJF639moC1
32 HdQaXHT60AKbR4H1DIKsTztsCfyntRtZ2E7vkk3oDUOLbmjvtuwaS0EtS8ammOht
33 9AgHNX25iFPCAT7H7ENgToDdr0A16Kf8gNK/qQ8icuiJon2zFzoQUP013cKLrvtbc
34 Ncu6g/LOQBcJqj1IzZ+7pZ2BwXyCmDjv6KR6FM3FKNfjPDjm1EhP7gmJo4XaJyZK
35 IcnvTTYr+o9TFPGcUmIntT1ZGHaTN+HnSkzFOM013AGGdfttqv3YtU7QRma21FE
36 K8D+7nq/5Em7SM6g8bQ3+BtWY+HcZPpB8Shy2rwlrT9Pw20uZjDE8b4S0FCgzjhX
37 zF4oAiyW74EKUHuadUHVBEZy1MCOaP8OnXW57vQroVxikPXjztC0iAjh0NF08
38 JXbNS+cxg+2tQGvT/xAgpCdt88d1PRIVHirQwOfDNLhk2ipSHK18RP9i1tIBF08
39 sks6LVHFjtkOAIaPocH0QX7jsWBr6iz6mFU86PR3nSjZ/md1B+Ln4zXKV6gojog
40 toJvUSPjPjat129c9PY+Kc12xkxwY1MLREojnNve170SZoDmj8RVfJXYT3oYfMp
41 PdpZpnYmRbHhVuk43cR+67j8r5yjqwq8LJrc/TsVPghevFzIo5YWRThKA81I+MG
42 nVR53xBg3RT34zcGERHMKx8Q/L5Seb1LVogu1X2dv4vS7wyHrfJTA7Sf0+NvybdG
43 rQ/+se7YgmseC9sVAEPQWSPKZLK9pnaCPRIHf11S2M8yfwGaqoL27WmQ6Gxv1b5
44 piltZ6oOUZ87gPbTFjd1Bux7
45 =M1r8
46 -----END PGP MESSAGE-----
47
```

### Step 2b

Q: When encrypting the e-mail to your partner, which key did you use?

When encrypting the message to my partner, GPG used my partner’s public key which was previously imported per my partner sending me his public key.

### Step 2c

Q: When your partner decrypted that e-mail, which key did he or she use?

My partner used his private key to decrypt the message that was encrypted with the public key that was sent to me.

### Step 2d

Q: When signing your e-mail to your partner, which key did you use?

When signing my email to my partner, GPG used my private key.

### Step 2e

Q: When your partner verified your signature, which key did he or she use?

When verifying the signature at my partner's end, GPG used my (sender) public key to verify the signature.

### Step 2f

Q: How was confidentiality accomplished?

Confidentiality is accomplished by encrypting the message sent to the partner. Since the public key of the partner is used, but only his private key can be used to decrypt it. As such, the data is confidential (protected) and can only be seen by the one holding the private key; i.e. the partner.

### Step 2g

Q: How was integrity accomplished?

Integrity is accomplished by signing (hashing and encrypting) the email with the sender's private key. Since the hash is included as part of the signature, the computed hash, by the partner, is compared to the decrypted hash from the sender. If they are equal, then the message has not been tampered with.

Additionally, by decrypting the signature with the public key of the sender, it can be verified that the sender "did" send the message and it was not re-hashed and re-signed by someone else.

So, two things – integrity verified by double-checking the hash. Recipient / partner can trust the hash since it was encrypted by the party who sent it.

### Step 2h

Q: How was nonrepudiation accomplished?

Nonrepudiation is accomplished by verifying the signature of the email. As mentioned in the previous question, by decrypting using the sender's public key, it can be verified that only the sender could have sent it since only the sender's public key can decrypt something encrypted by the sender's private key.