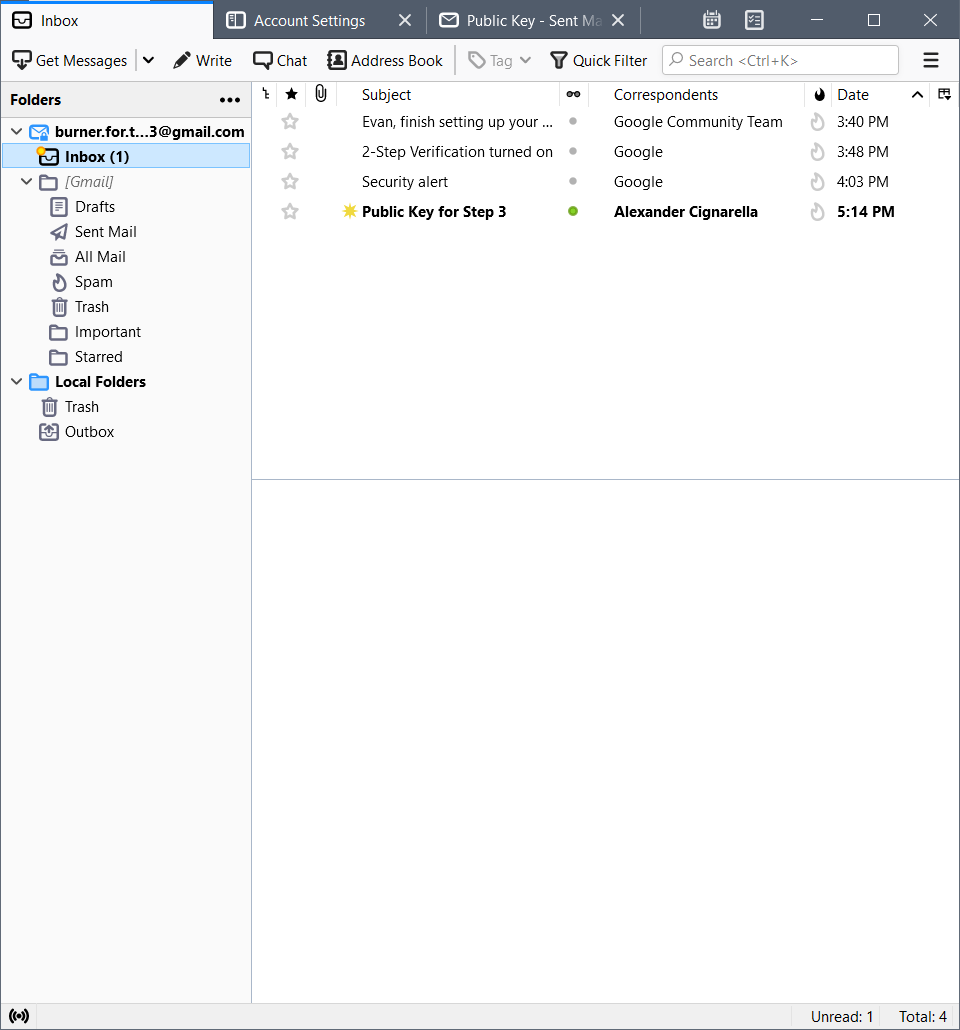
Evan Smith

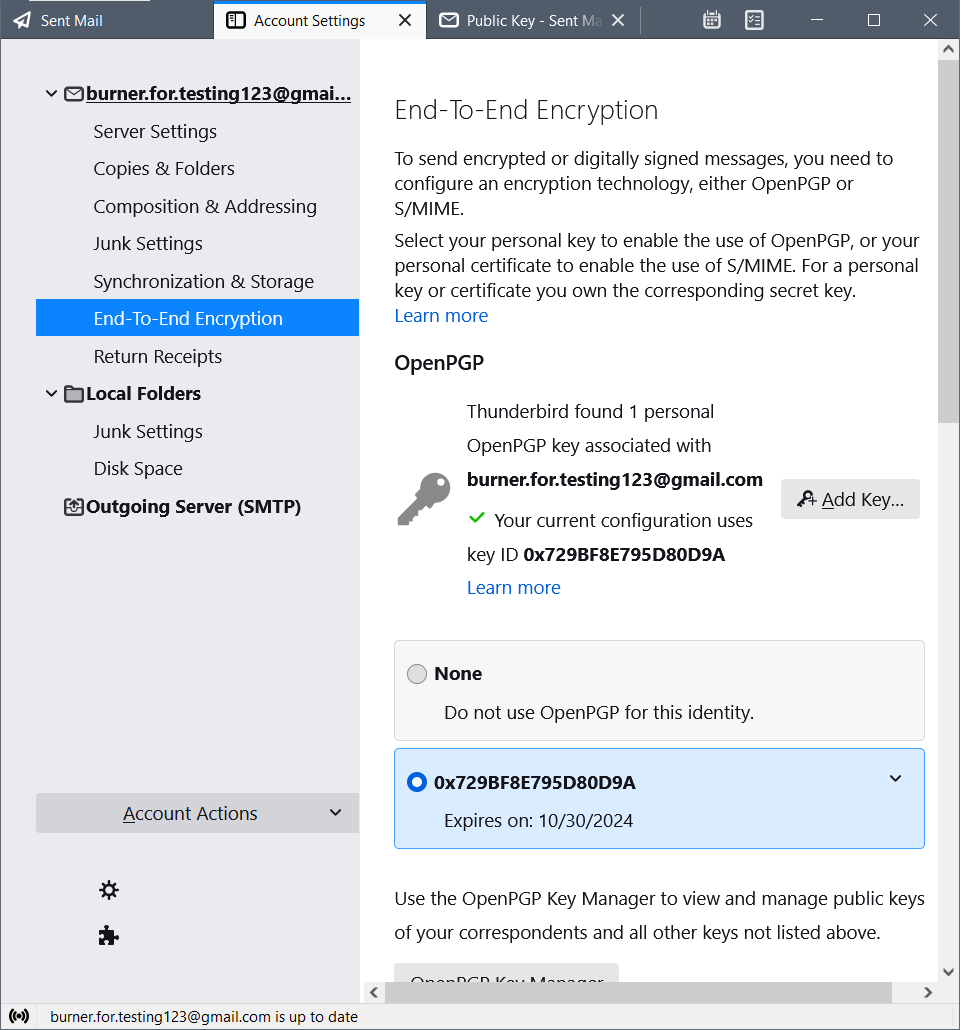
CIS 628, Cryptography

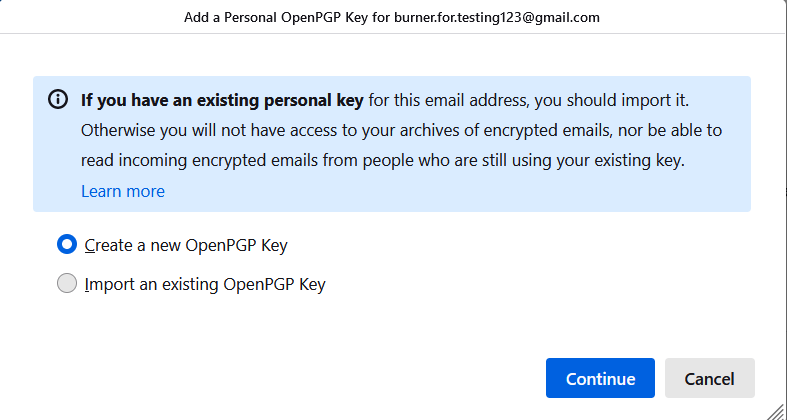
HW 2

Step 1: Setting up Thunderbird



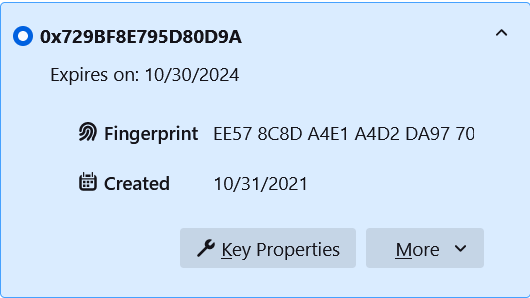
Step 2: Configure Cryptography

2a: 

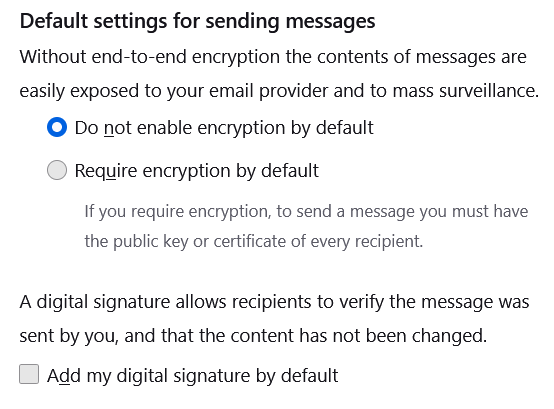
2b/2c: 

2d: missed this screenshot and now don’t want to reset my key

2e:

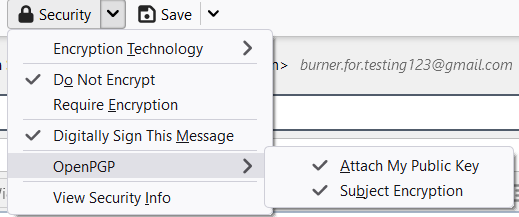


2f:

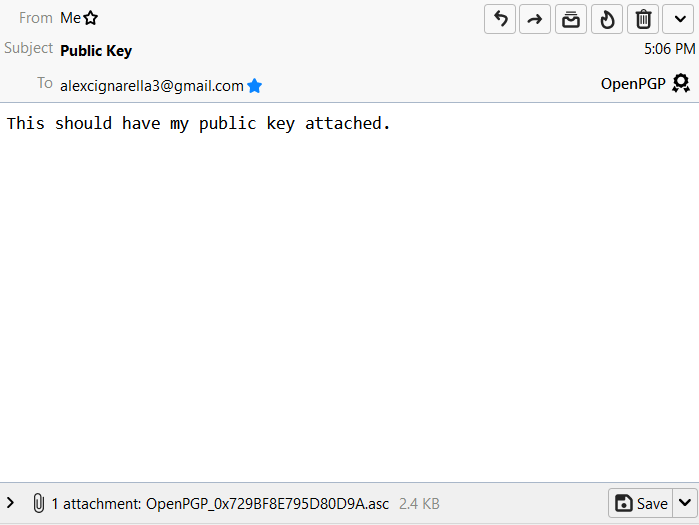


Step 3: Sending Emails to Partner

3a:

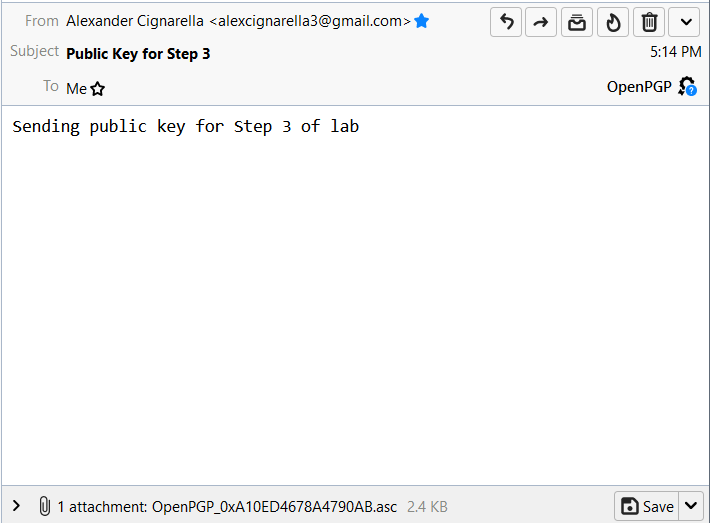


3b:

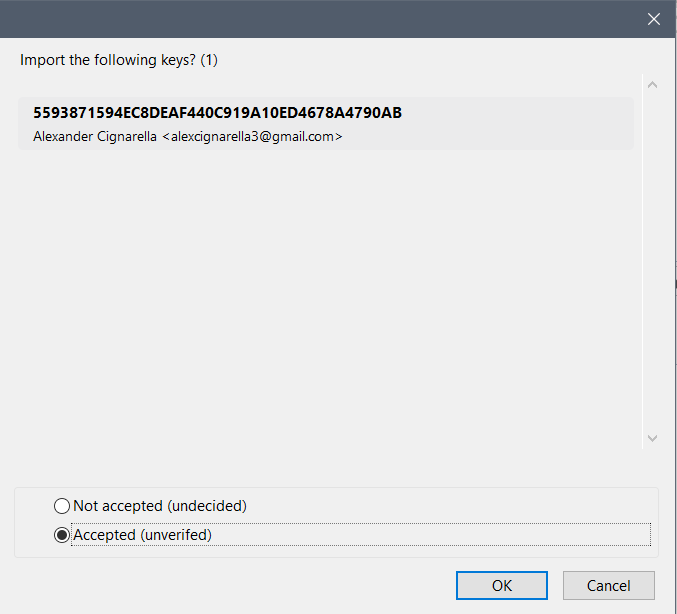


Step 4: Working with Partner’s Public Key

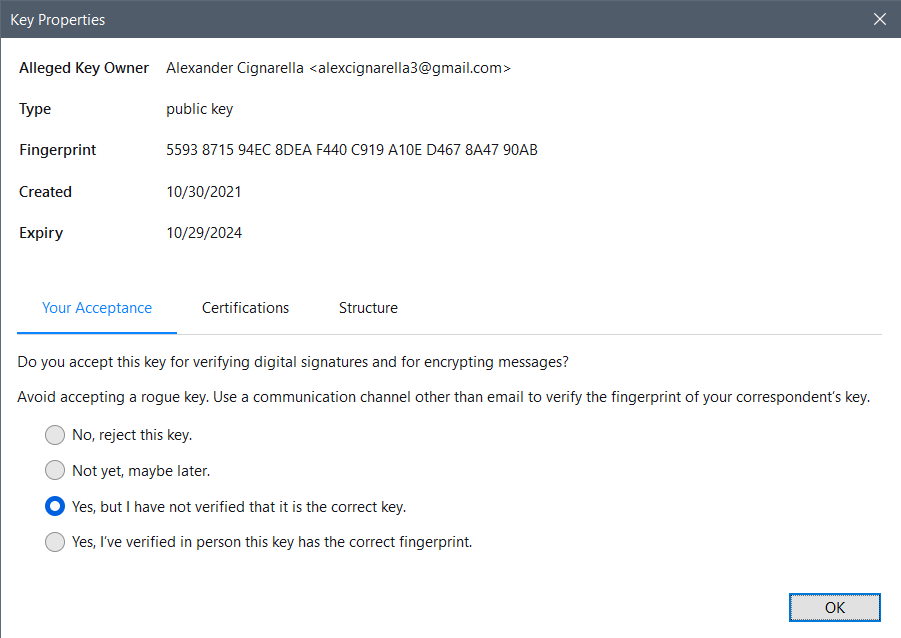
4a:



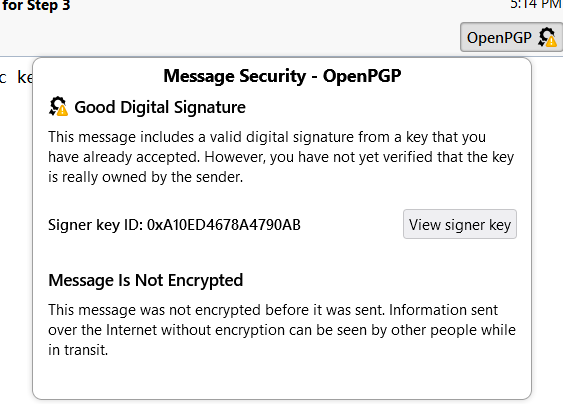
4b:



4c/4d:

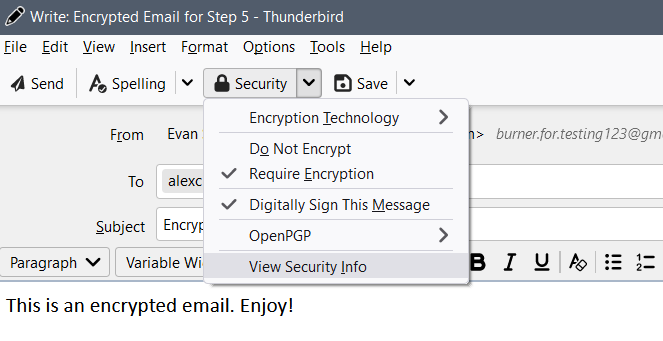


4e:

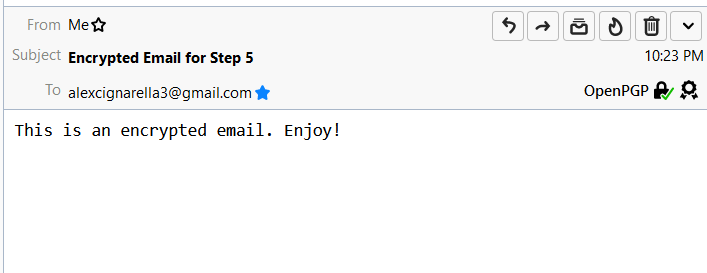


Step 5: Sending Encrypted Email Using Key

5a/5b:

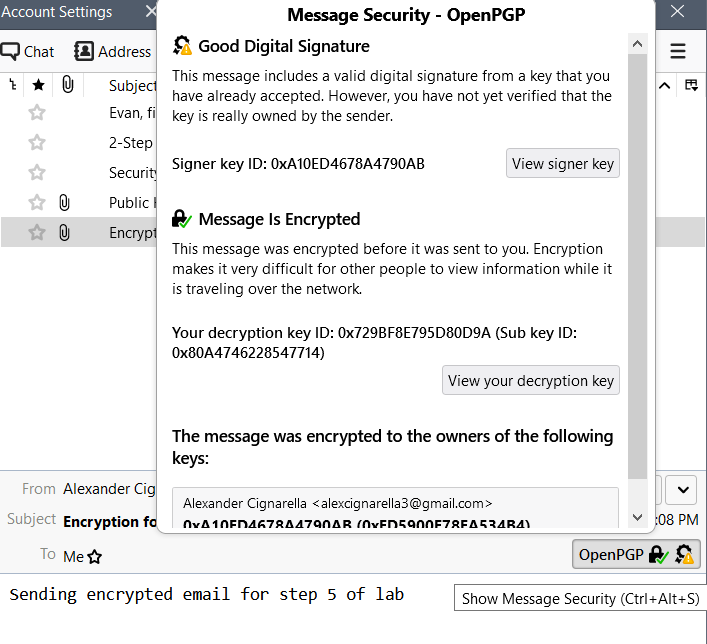


5c:

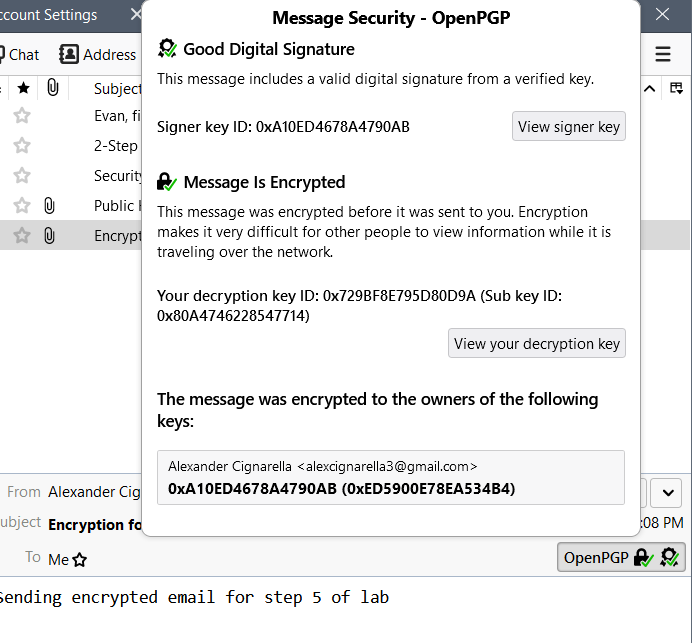


Step 6: Reading Partner’s Encrypted Email

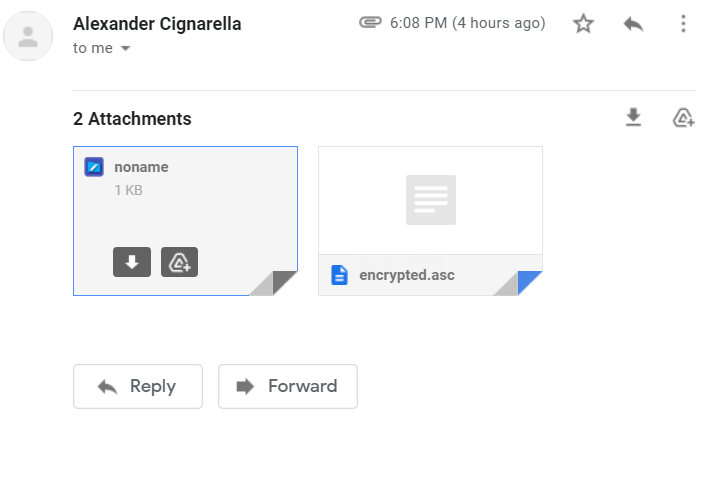
6a:



6b:



6c:



Step 7:

7a: In the browser, the encrypted email does not have body text or a subject line. The data that would make up those things is seen just as an attachment. That attachment is the encrypted data that Gmail does not have the key to decrypt. In Thunderbird, the settings that were established means that the data is decrypted into readable subject and body text.

7b: The symmetric key encrypted my email to my partner.

7c: I used my partner’s public key to encrypt the symmetric session key.

7d: My partner decrypted the email using the symmetric session key.

7e: My partner decrypted the symmetric key using their private key.

7f: We used two different keys because symmetric key encryption is fast but less secure, while asymmetric encryption is much slower, but more secure. This is a combination of the benefits while mitigating the drawbacks.

7g: I used my private key to sign my email.

7h: My partner used their private key to sign their email.

7i: Confidentiality was accomplished due to the asymmetric approach used to encrypt the symmetric key. This means that the data once encrypted using a public key, is encrypted to anyone without the correct corresponding private key.

7j: Integrity was accomplished because the message, if modified in its encrypted state, would fail a checksum verification, or would appear as gibberish.

7k: Nonrepudiation was accomplished due to the combination of the facts above, as well as the usage of digital signatures. These are encrypted using the sender’s private kay, such that anyone with the public key can verify that the message was actually sent by that person. This means that a message with a signature cannot be repudiated by the signer, since they are the only ones who could have signed it.