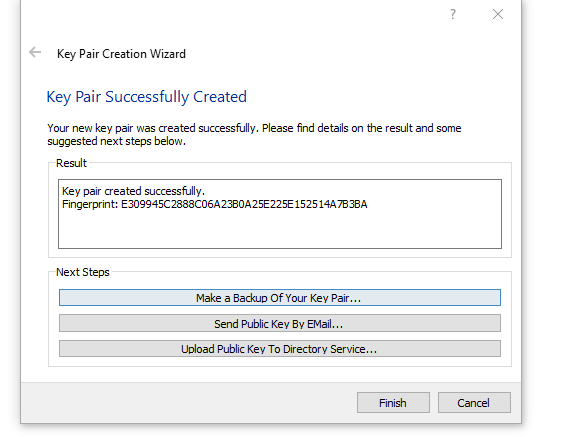
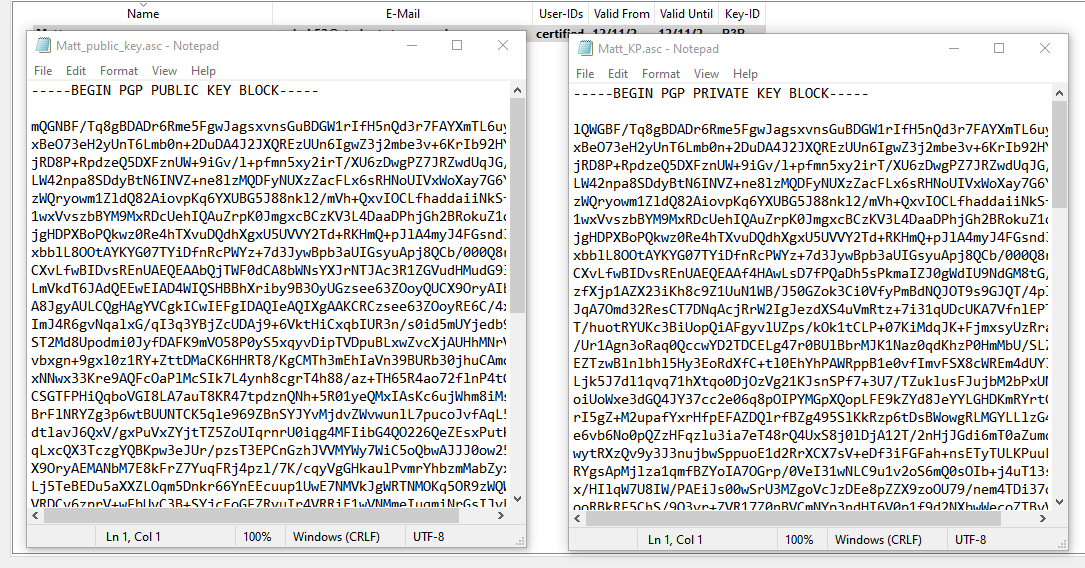
Matt wants to email Rob an encrypted and signed message

Both rob and Matt generate an OpenPGP keypair, this consist of a public and private key.

The cryptographic function used is RSA.

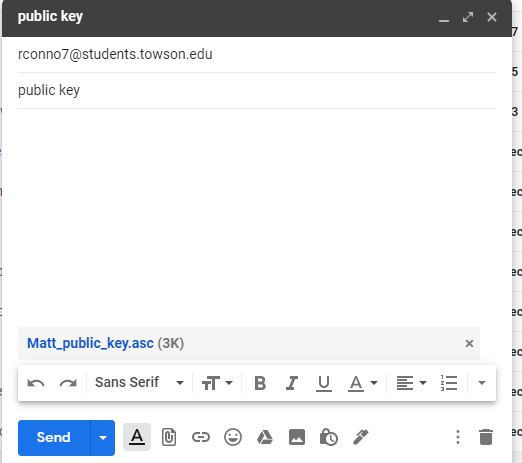


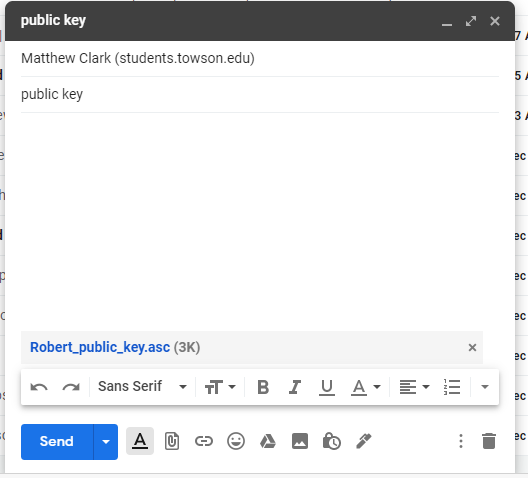
Matt’s key pair:



Rob’s key pair:

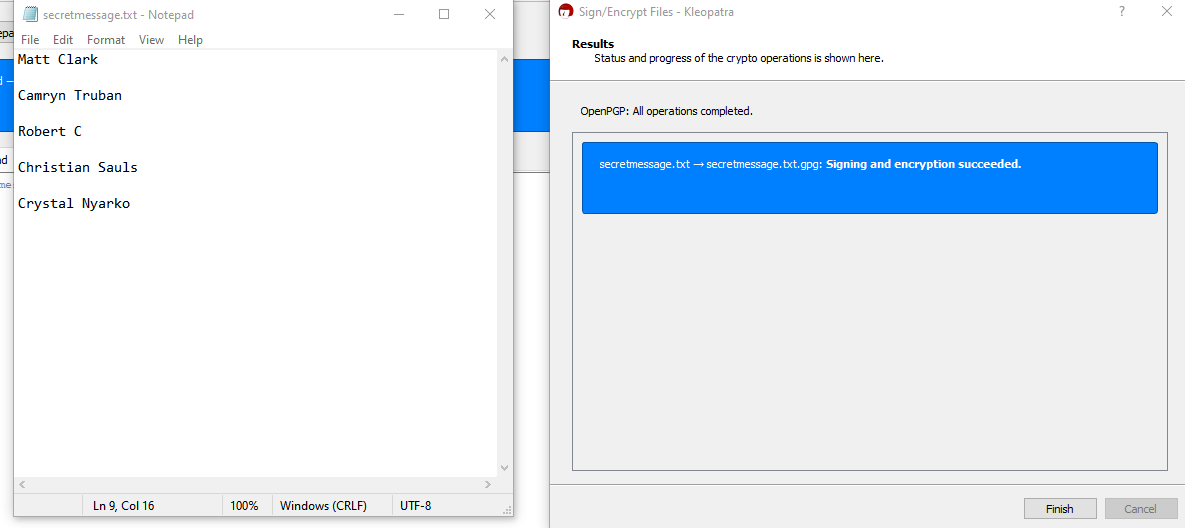


Rob sends his public key to Matt and Matt sends his public key to rob

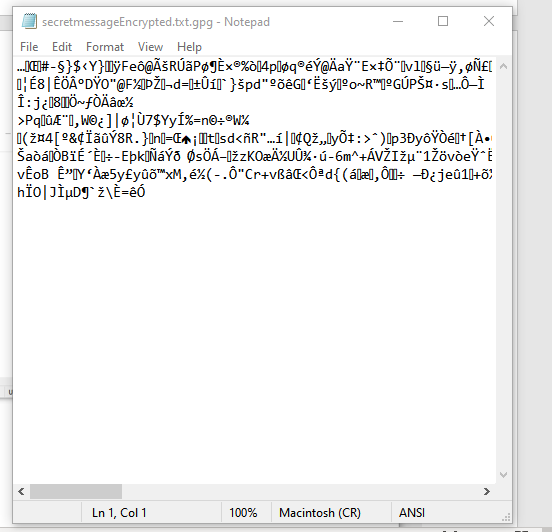


Both import the others key after downloading the attached file.

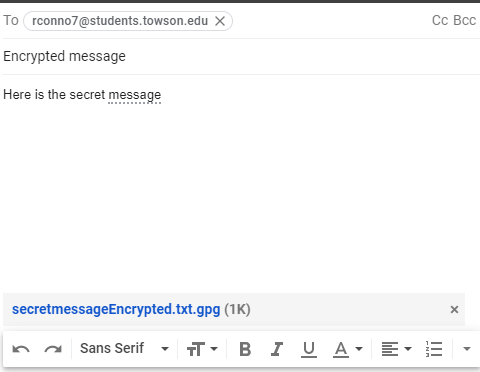
Matt signs the message with his own private key and encrypts it with Rob’s public key. The signing is done with SHA1 hash function, which OpenPGP uses by default.



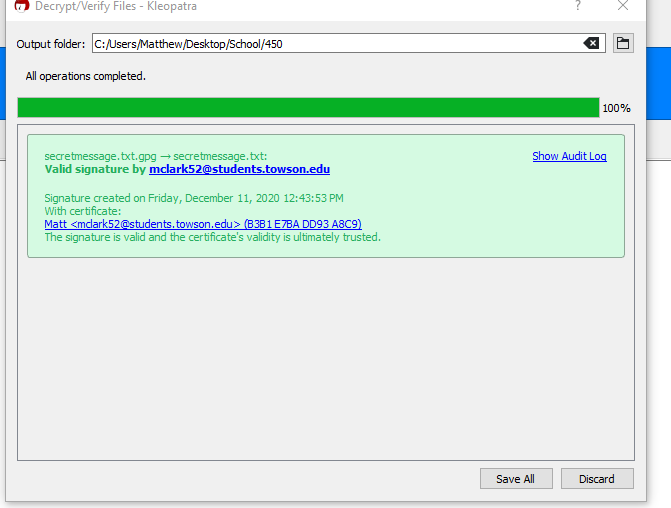
Here is what the cypher text looks like



Matt sends the message to Rob.



Rob receives the encrypted/signed message and decrypts with his private key, verifies it with Matt’s public key



Here is the message after successful encryption:

