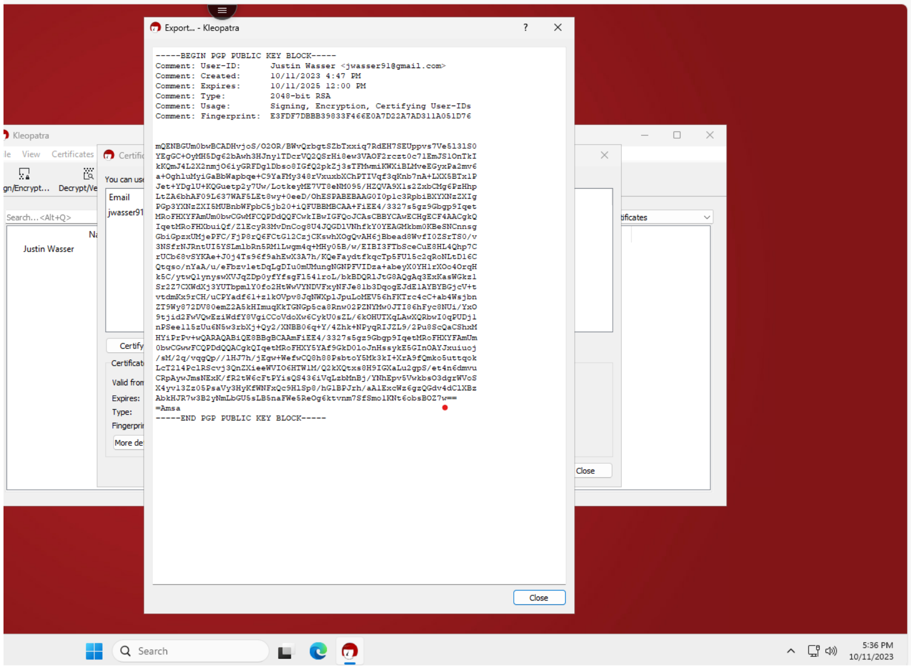
PGP (GPG) Project Report

Scenario:

Another individual and I created separate asymmetric encryption keys using PGP and exchanged our public keys. We then encrypted messages using each other's public keys and exchanged messages. Lastly, we decrypted each other's messages using a secret key.

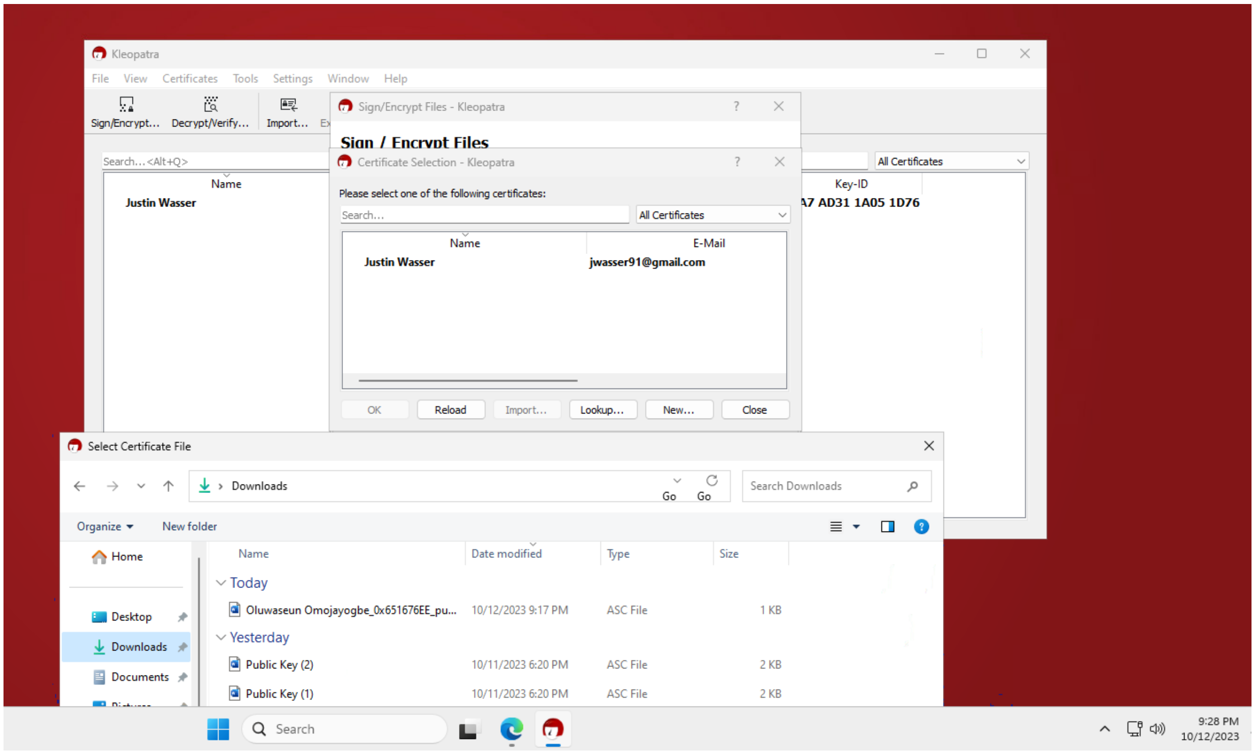
Figure 1: Creating key pair



```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User-ID:       Justin Wasser <jwasser91@gmail.com>
Comment: Created:       10/11/2023 4:47 PM
Comment: Expires:       10/11/2025 12:00 PM
Comment: Type:          2048-bit RSA
Comment: Usage:         Signing, Encryption, Certifying User-IDs
Comment: Fingerprint:   E3FDF7DBBB39833F466E0A7D22A7AD311A051D76


mQENBGUm0bwBCADHvjoS/O2OR/BWvQrbgtSZbTxxiq7RdEH7SEUppvs7Ve5131S0
YEgGC+OyMH5Dg62bAwh3HJny1TDcrVQ2QSrHi8ew3VAOF2rczt0c71EmJS1OnTkI
kKQmJ4L2X2nmjO6iyGRFDg1Dbso8IGfQ2pkZj3sTFMwmiKWXiBLMveEGyxPa2mv6
a+OghluMyiGaBbWapbqe+C9YaFMy348rVxuxbXChPTIVqf3qKnb7nA+LXX5BTx1P
Jet+YDg1U+KQGuetp2y7Uw/LotkeyME7VT8eNM095/HZQVA9X1s2ZxbCMg6PzHhp
LtZA6bhAF09L637WAF5LEt8wy+0eeD/OhESPABEBAAG0I0plc3RpbiBXYXNzZXIg
PGp3YXNzZXI5MUBnbWFpbC5jb20+iQFUBBMBCAA+FiEE4/3327s5gz9Gbgp9Iqet
MRoFHXYFAmUm0bwCGwMFCQPDdQQFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQ
IqetMRoFHXbuiQf/Z1EcyR3MvDnCog8U4JQGD1VNhfkY0YEAGMkbm0KBeSNCnnsg
GbiGpzxUMjePFC/FjP8rQ6FCtG12CzjCKswhXOgQvAH6jBbead8WvfI0ZSrTS0/v
3NSfrNJRntUI5YSLm1bRn5RM1Lwgm4q+MHy05B/w/EIBI3FTbSceCuE8HL4Qhp7C
rUCb68vSYKAe+J0j4Ts96f9ahEwX3A7h/KQeFaydtfkqcTp5FU15c2qRoNLtD16C
Qtqso/nYaA/u/eFbzv1etDqLgDIu0mUMungNGNPFVIDza+abeyX0YH1rXOo4OrqH
k5C/ytwQ1ynyswXVJqZDp0yfYfsgF1541roL/bkBDQR1JtG8AQgAq3ExKasWGkz1
Sr2Z7CXWdXj3YUTbpm1Y0fo2HtWwVYNDVFxyNFJe81b3DqogEJdE1AYBYBGjcV+t
vtdmKx9rCH/uCPYadf61+z1kOVpv8JqNWXp1JpuLoMEV56hFKTrc4cC+ab4Wsjbn
ZT9Wy872DV80emZ2A5kHImuqKkTGNGp5ca8Rnw02PZNYMw0JTI86hFyc8NUi/YxO
9tjid2FwVQwEziWdfY8VgiCCoVdoXw6CykU0sZL/6kOHUTXqLAwXQRbwI0qPUDj1
nPSee115zUu6N5w3rbXj+Qy2/XNBB06q+Y/4Zhk+NPyqRIJZL9/2Pu8ScQaCShxM
HYiPrPv+wQARAQABiQE8BBgBCAAmFiEE4/3327s5gz9Gbgp9IqetMRoFHXYFAmUm
0bwCGwwFCQPDdQQACgkQIqetMRoFHXY5YAf9GkD0loJnHssykE5GInOAYJxuiuoj
/sM/2q/vqgQp//1HJ7h/jEgw+WefwCQ8h88PsbtoY5Mk3kI+XrA9fQmko5uttqok
LcT214PclRScvj3QnZXieeWVIO6HTW1M/Q2kXQtxs8H9IGXaLu2gpS/et4n6dmvu
CRpAywJmsNExK/fR2tW6cFtPYisQS436iVqLzbMnBj/YNhEpv5VwkbsO3dgrWVoS
X4yv13Zz05PsaVy3HyKfWNFxQc9H1Sp8/hG1BPJrh/aA1ExcWz6gzQGdv4dC1XBz
AbkHJR7w3B2yNmLbGU5sLB5naFWe5ReOg6ktvnm7SfSmo1KNt6obsBOZ7w==
=Amsa
-----END PGP PUBLIC KEY BLOCK-----
```

Figure 2: Importing partner’s key



Name	Key-ID
Justin Wasser	A7 AD31 1A05 1D76

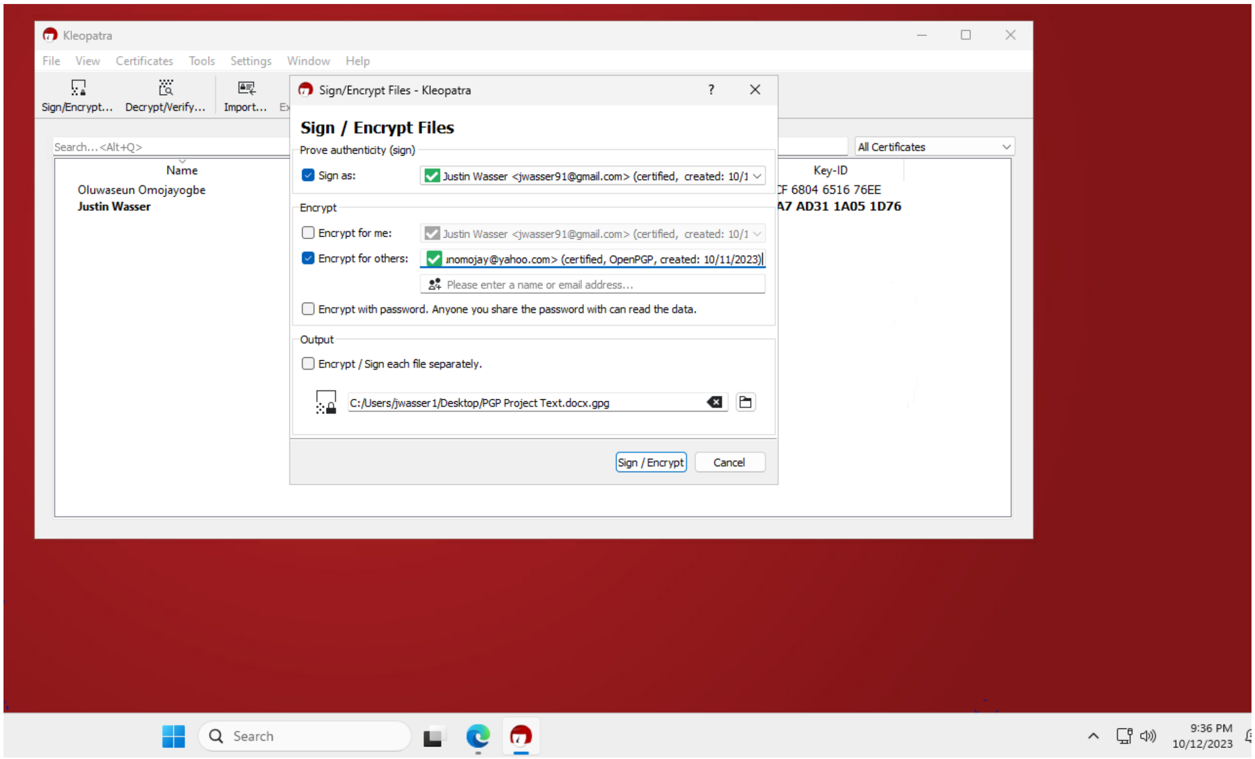
Please select one of the following certificates:

Name	E-Mail
Justin Wasser	jwasser91@gmail.com

Name	Date modified	Type	Size
Today			
Oluwaseun Omojayogbe_0x651676EE_pu…	10/12/2023 9:17 PM	ASC File	1 KB
Yesterday			
Public Key (2)	10/11/2023 6:20 PM	ASC File	2 KB
Public Key (1)	10/11/2023 6:20 PM	ASC File	2 KB

I downloaded my partner’s public key from the discussion board and then clicked ‘sign/encrypt files’ selected my text file, unselected ‘encrypt for me’ then clicked on the add people icon next to the ‘encrypt for others’ then selected the ‘import’ option when prompted to select a certificate. I then went to the download section, selected my partner’s public key I had downloaded earlier, and then used his public key to encrypt the text file.

Figure 3: Encrypting my text file with my partner's public key


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt… Decrypt/Verify… Import…
Search…<Alt+Q>
All Certificates

Name	Key-ID
Oluwaseun Omojayogbe	CF 6804 6516 76EE
Justin Wasser	**A7 AD31 1A05 1D76**

Sign/Encrypt Files - Kleopatra

Sign / Encrypt Files

Prove authenticity (sign)

☑ Sign as: Justin Wasser <jwasser91@gmail.com> (certified, created: 10/1

Encrypt

□ Encrypt for me: Justin Wasser <jwasser91@gmail.com> (certified, created: 10/1

☑ Encrypt for others: ınomojay@yahoo.com> (certified, OpenPGP, created: 10/11/2023)

Please enter a name or email address…

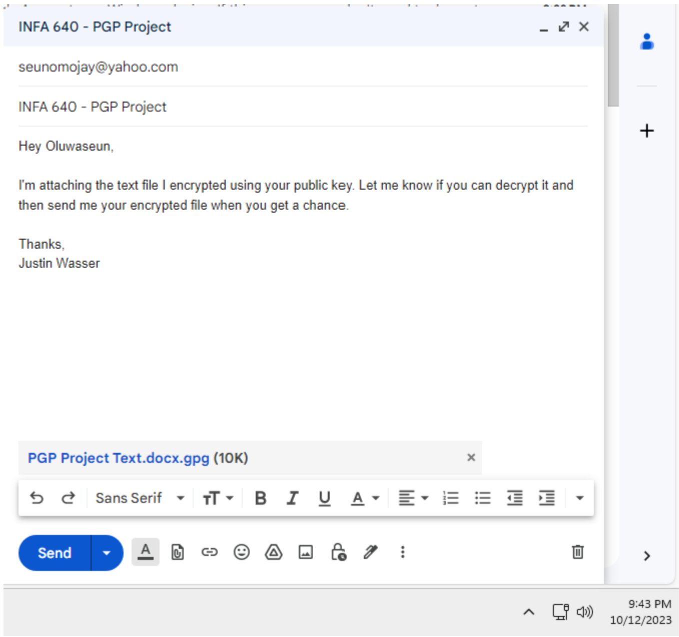
□ Encrypt with password. Anyone you share the password with can read the data.

Output

□ Encrypt / Sign each file separately.

C:/Users/jwasser1/Desktop/PGP Project Text.docx.gpg

Figure 4: Emailing encrypted file to my partner



seunomojay@yahoo.com

INFA 640 - PGP Project

Hey Oluwaseun,

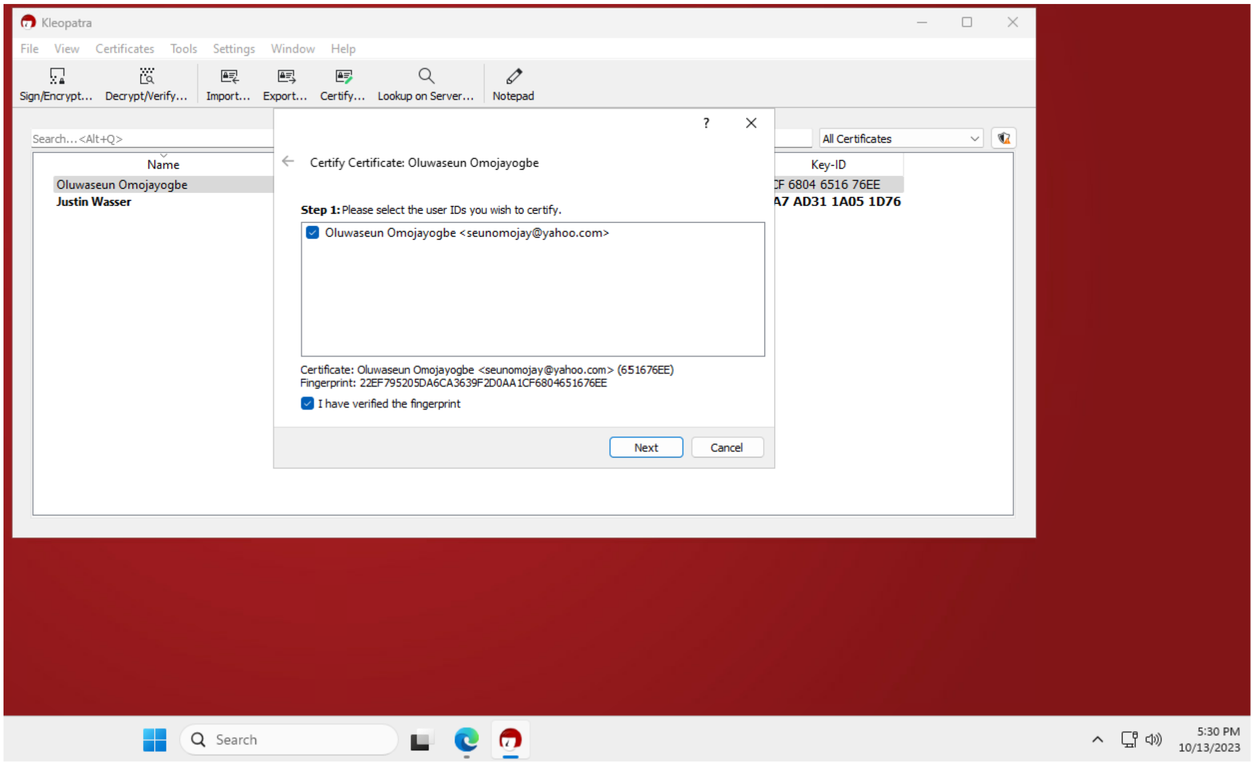
I'm attaching the text file I encrypted using your public key. Let me know if you can decrypt it and then send me your encrypted file when you get a chance.

Thanks,
Justin Wasser

PGP Project Text.docx.gpg (10K)

I downloaded the encrypted message emailed to me and then I opened Kleopatra and certified my partner’s certificate.

Figure 5: Certifying partner’s certificate



Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt… Decrypt/Verify… Import… Export… Certify… Lookup on Server… Notepad
Search…<Alt+Q>
All Certificates
Next
Cancel
5:30 PM
10/13/2023

Name	Key-ID
Oluwaseun Omojayogbe	CF 6804 6516 76EE
Justin Wasser	**A7 AD31 1A05 1D76**

Certify Certificate: Oluwaseun Omojayogbe

Step 1: Please select the user IDs you wish to certify.

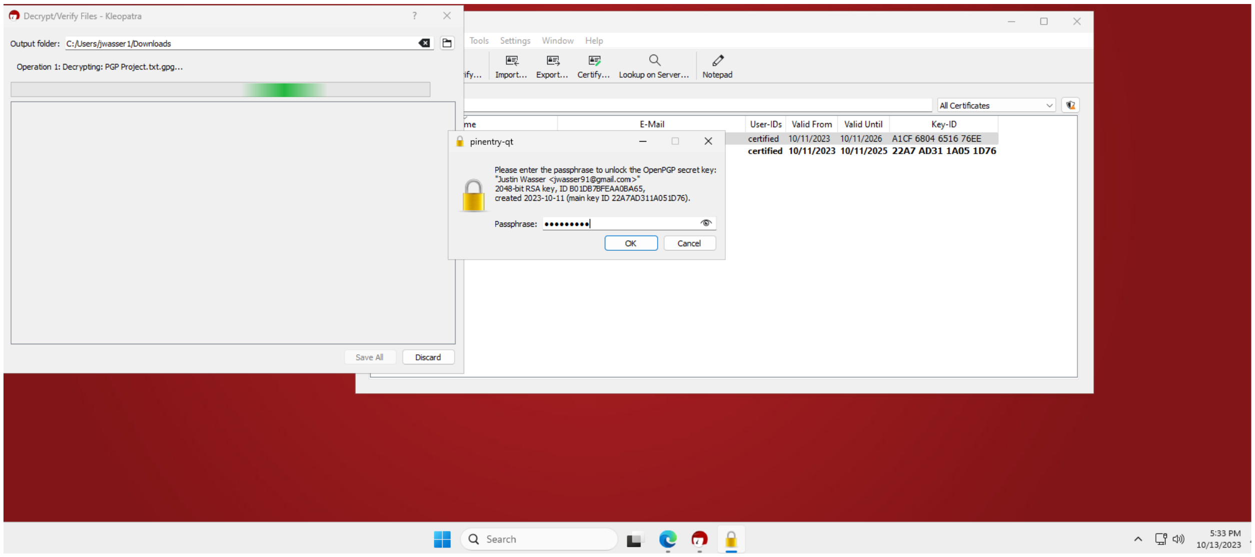
☑ Oluwaseun Omojayogbe <seunomojay@yahoo.com>

Certificate: Oluwaseun Omojayogbe <seunomojay@yahoo.com> (651676EE)
Fingerprint: 22EF795205DA6CA3639F2D0AA1CF6804651676EE

☑ I have verified the fingerprint

I then clicked the ‘decrypt/verify’ button selected the encrypted file from the downloads folder and entered my passphrase to decrypt the message.

Figure 6: Entering passphrase for message decryption



Decrypt/Verify Files - Kleopatra
Tools Settings Window Help
Import… Export… Certify… Lookup on Server… Notepad
All Certificates
pinentry-qt
OK
Cancel
Save All
Discard
5:33 PM
10/13/2023

Output folder: C:/Users/jwasser1/Downloads

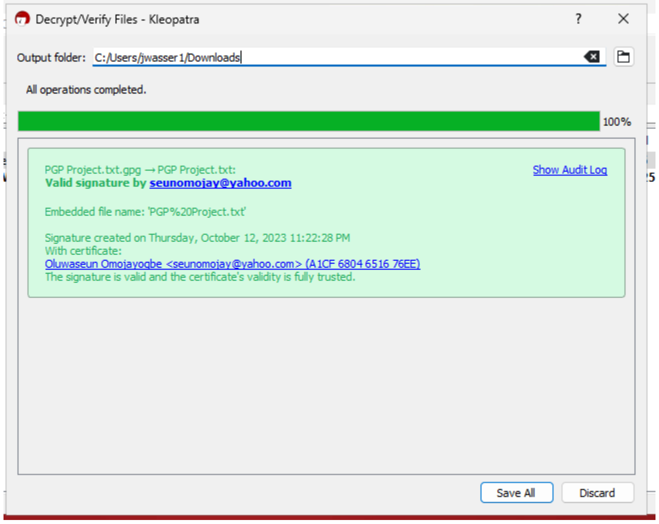
Operation 1: Decrypting: PGP Project.txt.gpg…

me	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
		certified	10/11/2023	10/11/2026	A1CF 6804 6516 76EE
		certified	**10/11/2023**	**10/11/2025**	**22A7 AD31 1A05 1D76**

Please enter the passphrase to unlock the OpenPGP secret key:
"Justin Wasser <jwasser91@gmail.com>"
2048-bit RSA key, ID B01DB7BFEAA0BA65,
created 2023-10-11 (main key ID 22A7AD311A051D76).

Passphrase: •••••••••

Figure 7: Successfully decrypting partner’s message



Output folder: C:/Users/jwasser1/Downloads

All operations completed.

100%

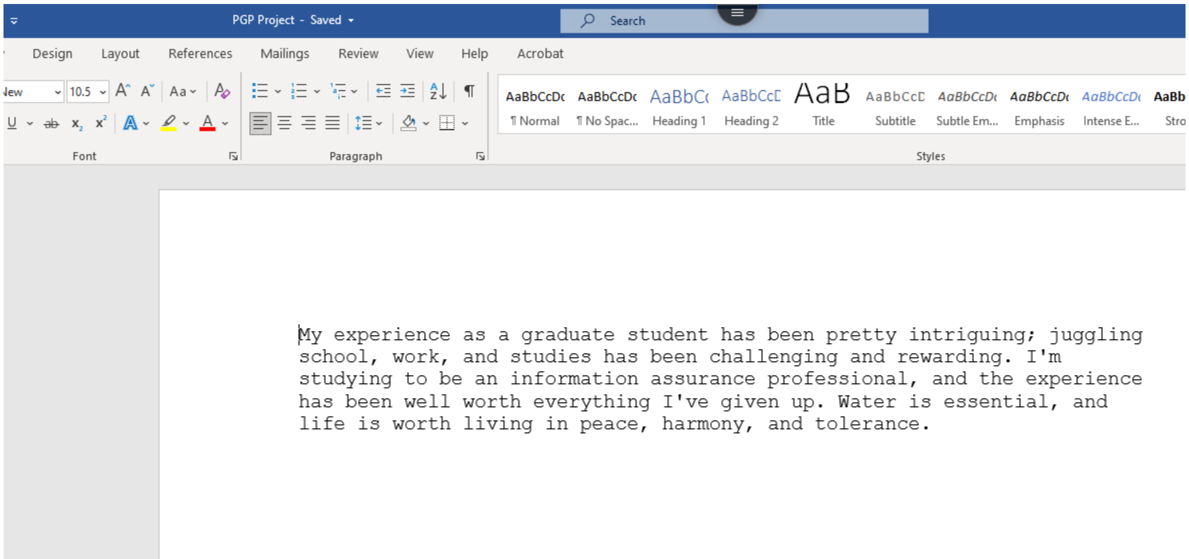
PGP Project.txt.gpg → PGP Project.txt:
Valid signature by seunomojay@yahoo.com

Embedded file name: 'PGP%20Project.txt'

Signature created on Thursday, October 12, 2023 11:22:28 PM
With certificate:
Oluwaseun Omojayogbe <seunomojay@yahoo.com> (A1CF 6804 6516 76EE)
The signature is valid and the certificate's validity is fully trusted.

I then opened the decrypted message using Microsoft Word.

Figure 8: Partner’s plaintext message



```
My experience as a graduate student has been pretty intriguing; juggling
school, work, and studies has been challenging and rewarding. I'm
studying to be an information assurance professional, and the experience
has been well worth everything I've given up. Water is essential, and
life is worth living in peace, harmony, and tolerance.
```

Section	Date	Action	Activity Description

1	10/11/2023	Creating the key pair	Created PGP key pair
2	10/11/2023	Posting the public key	Posted my public key to the discussion board
3	10/12/2023	Downloading partner’s public key	Downloading partner’s public key
4	10/12/2023	Receiving encrypted message	My partner emailed me an encrypted message
5	10/12/2023	Sending encrypted message	I emailed my partner the encrypted message
6	10/13/2023	decrypting message and emailing the plain text	I decrypted my partner’s message and emailed him back the plaintext message which is as follows… My experience as a graduate student has been pretty intriguing; juggling school, work, and studies has been challenging and rewarding. I'm studying to be an information assurance professional, and the experience has been well worth everything I've given up. Water is essential, and life is worth living in peace, harmony, and tolerance.
7	10/13/2023	Receiving the decrypted message from partner and sending an acknowledgment	My partner emailed me my decrypted message which is as follows… The method for creating the substitution cipher I have chosen is to substitute a given letter of the plaintext with another letter in the alphabet, and the specific correlation between a plaintext letter and

			its corresponding ciphertext letter can be altered each time data is encrypted. For example, using my cipher, where the key is cyphertext minus 1 the cyphertext string ‘ifmmp xpsme’ translates/deciphers to ‘hello world’.