

## INDEX

SL.NO	TOPIC	PAGE. No
1	INTRODUCTION	2
2	PGP(Pretty Good Privacy)	2
3	X.509 CERTIFICATE	2,3
4	LEARNING OUTCOME	3
5	COURSE WORK OUTCOME	3
6	TASK 1	4
7	TASK 2	5
8	TASK 3	5
9	TASK 4	6
10	TASK 5	7
11	TASK 6	7
12	OBSERVATIONS	8

## INTRODUCTION

The function of a digital certificate, also called a public key certificate, is to bind ownership cryptographically. For encryption and authentication, digital certificates are used to share public keys.

An entity whose public key is to be certified can be identified by a digital certificate that contains the public key. Digital certificates are distributed, authenticated, and revoked by PKI (Public Key Infrastructure). The public-key cryptography system relies on a pair of keys: a private key held by the owner, which is used for signing and decrypting, and a public key that is used to encrypt transmitted data or verify the owner's signature. To authenticate entities, digital certificates allow them to share public keys.

Digital certificates are used by all major web browsers and web servers to ensure that content hasn't been modified by unauthorized actors. Cryptographic security and privacy are provided by digital certificates.

## PGP (PRETTY GOOD PRIVACY)

In PGP, knowledge communication is encrypted and authenticated to ensure privacy and security. PGP is a cryptographic program that provides privacy and authentication for data communication. It is commonly used for signing, encrypting, and decrypting texts, emails, files, and entire disk partitions to enhance security in email communications.

PGP encryption uses a combination of hashing, data compression, symmetric-key cryptography, and public-key cryptography. Each public key is associated with a username or email address. PGP supports integrity checking and message authentication, where the former is used to detect whether a message has been altered since it was sent, and the latter is used to verify that the message was indeed sent by the claimed sender. To create a digital signature, the sender uses a PGP to compute a hash of the plain text message and then creates a digital signature from that hash using the sender's private key.

## X.509

X.509 certificates are digital certificates that conform to the standards set by the International Telecommunication Union (ITU). They are widely used in many different applications, such as websites, mobile apps, online documents, and connected devices. X.509 certificates use a combination of public and private key pairs to encrypt and decrypt messages, ensuring the identity of the sender and the security of the messages.

One common use of X.509 certificates is in TLS/SSL (Transport Layer Security/Secure Socket Layer), which provides a secure foundation for web browsing using the HTTPS protocol.

X.509 certificates differ from PGP certificates in several ways. X.509 certificates use a directory method, while PGP uses a referral method. X.509 certificates are created using strong cryptographic techniques and are governed by Certification Authorities (CAs), which are overseen by Certification Practice Statements (CPS). PGP allows for the stacking of certificates, with one signature on top of another, while X.509 organizes certificates in a linked list. PGP also allows for the use of keys associated with real people through a web of trust, while X.509 binds keys to names and trusts them transitively.

### Learning outcome

We expect to learn about Public Key Infrastructure (PKI) and digital signatures and how they are used to verify the accuracy and authenticity of various forms of communication and data. By understanding the different standards of digital certificates, such as X.509 and PGP, we can gain insight into the different methods by which these certificates are used and processed.

We also expect to learn about the chain of certificates, which begins with obtaining the certificate from the issuer and providing it to the Root Certificate Authority. This process is done for the signature, and then the certificate is sent back to the Root Certificate Authority for verification. After the verification is complete, the certificate is sent back to the owner.

### Course Work Outcome

The tasks have been specified to show how to create a digital certificate using the above-mentioned standards on a Linux OS (I have used Ubuntu).

- In Task 1, I learned how to create a self-signed PGP certificate and associated private key using GPG commands on the Linux OS. This process will generate a self-signed user ID, fingerprint and a pair of keys. The generated keys can be used to encrypt and decrypt messages, as well as digitally sign and verify messages. This self-signed certificate and key pair will also be used to authenticate the user in other applications which support the use of PGP certificates.

Command used : `Openssl genrsa -out <filename> 2048`

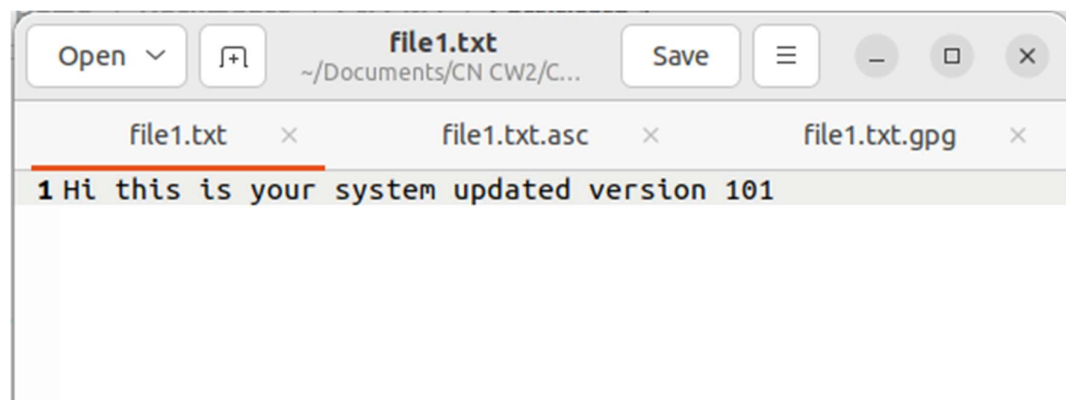
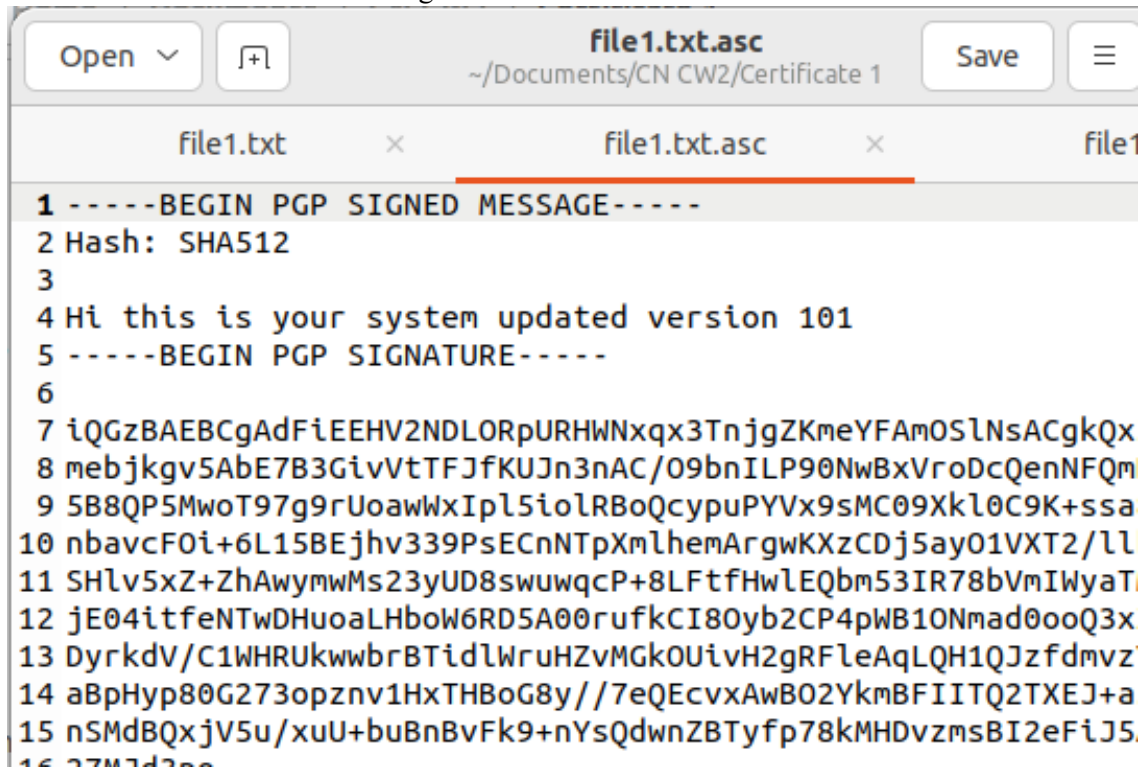


Fig 1.1: Plane text file



```
1 -----BEGIN PGP SIGNED MESSAGE-----
2 Hash: SHA512
3
4 Hi this is your system updated version 101
5 -----BEGIN PGP SIGNATURE-----
6
7 iQGzBAEBCgAdFiEEHV2NDLORpURHWNxqx3TnjgZKmeYFAMOSlNsACgkQx
8 mebJkgv5AbE7B3GivVtTFJfKUJn3nAC/O9bnILP90NwBxVroDcQenNFQm
9 5B8QP5MwoT97g9rUoawWxIpl5ioLrBoQcypuPYVx9sMC09Xkl0C9K+ssa
10 nbavcFOi+6L15BEjhv339PsECnNTPxMlhemArgwKXzCDj5ay01VXT2/ll
11 SHlv5xZ+ZhAwymwMs23yUD8swuwqcP+8LFtfHwLEQbm53IR78bVmIWyaT
12 jE04itfeNTwDHuoalHboW6RD5A00rufkCI80yb2CP4pWB10Nmad0ooQ3x
13 DyrkdV/C1WHRUkwbrBTidlWruHZvMGkOUiVH2gRfLeAqLQH1QJzfdmvz'
14 aBpHyp80G273opznv1HxTHBoG8y//7eQEcvxAwB02YkmBFIITQ2TXEJ+a
15 nSMdBQxjV5u/xuU+buBnBvFk9+nYsQdwnZBTyfp78kMHDvzmsBI2eFiJ5.
```

Fig 1.2: asc file created



```
1 \A3\00\00\00\FF\FD\90
2 \00
3 \C7t\E7\8E\J\99\E6\AC9b file1.txtc\92\92\C1Hi thi
system updated version 101\89\B3\00
4 \00!\04]\8D\B3\91\A5DGX\DCj\C7t\E7\8E\J\99\E6\c\9
5 \C7t\E7\8E\J\99\E6D\A4
\FE'\94\AC\AF\CFH7\89SY\8C&"\D4\EE"o\00\B5\8A\FB\DD
\E4\BFW\A5\84\F5D\97\AFaA_51>\BC\8F\DBi\E8'\D7j.\1C
\B3]Xf\D5\B7\EE\BBR\at97\m\96%hW* \EF\91
Yfd\9A\C1\F9\F5\9B\90ux\A0\A0\D1I \94\F8\C9ek\A5\D6:
\AC\82\9E\98\A1{"\8F\W\E0\87"\F2\9A\CA6\E7<\D9\FF\
\A5\E7s\鍾\8C\CFV\9B\B5\AF\81?\B6%\83E\ED\AF\F1w",Uc
\97\F9
```

Fig 1.3: gpg file created

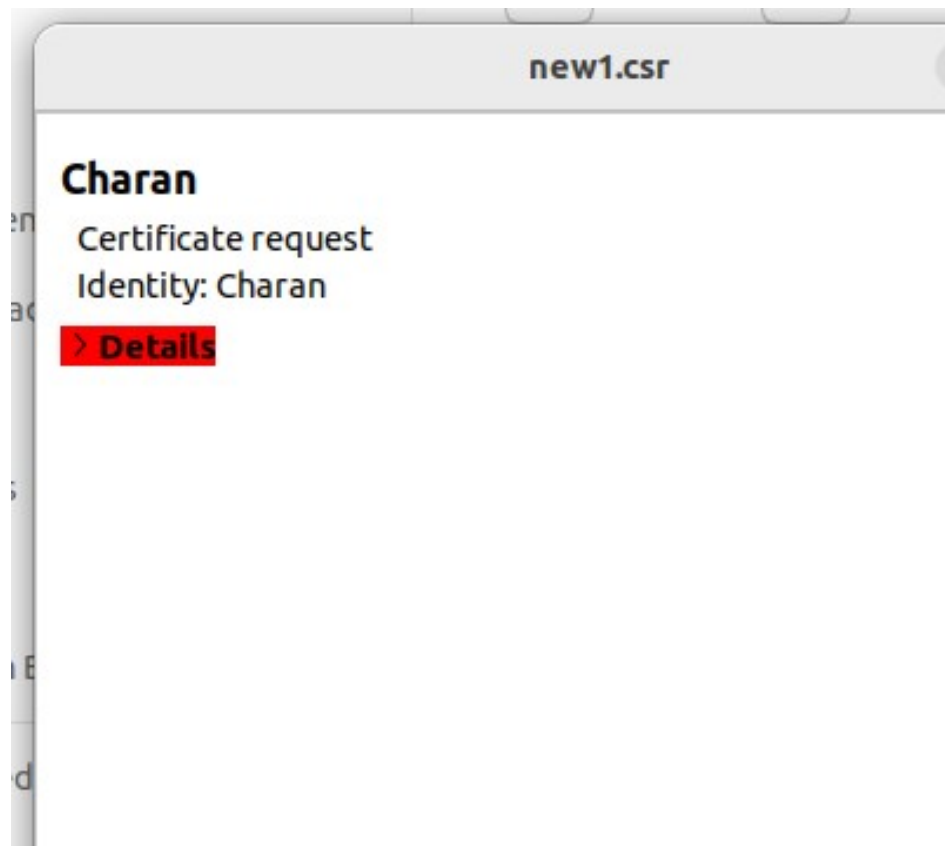


Fig 1.4: Signed csr file

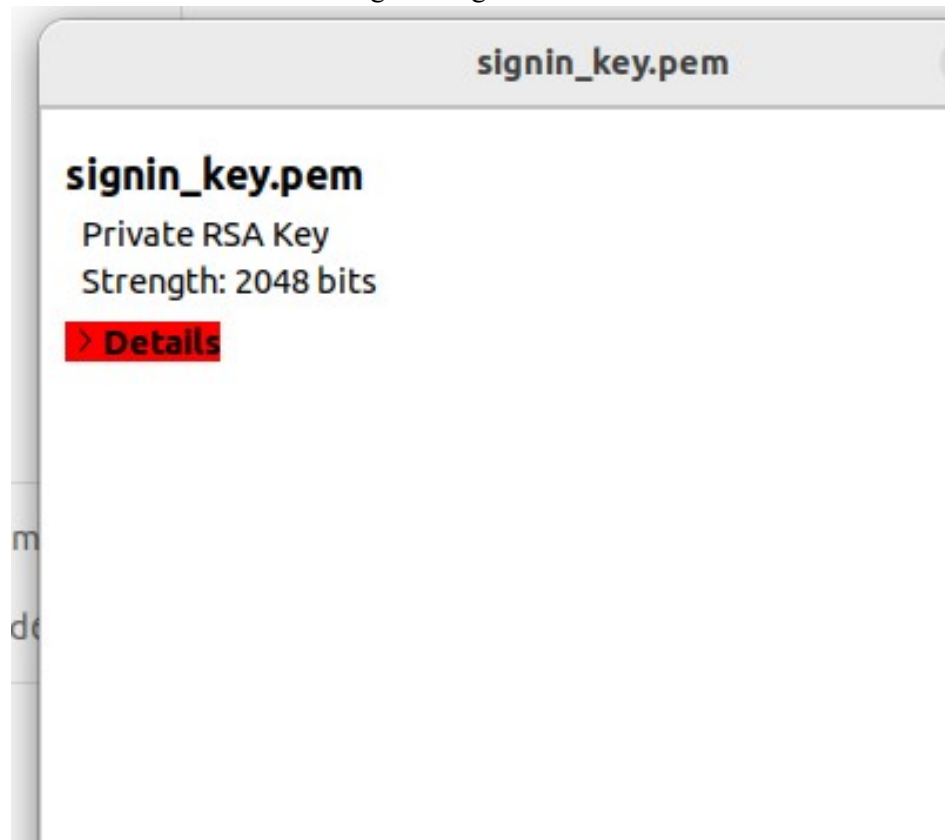
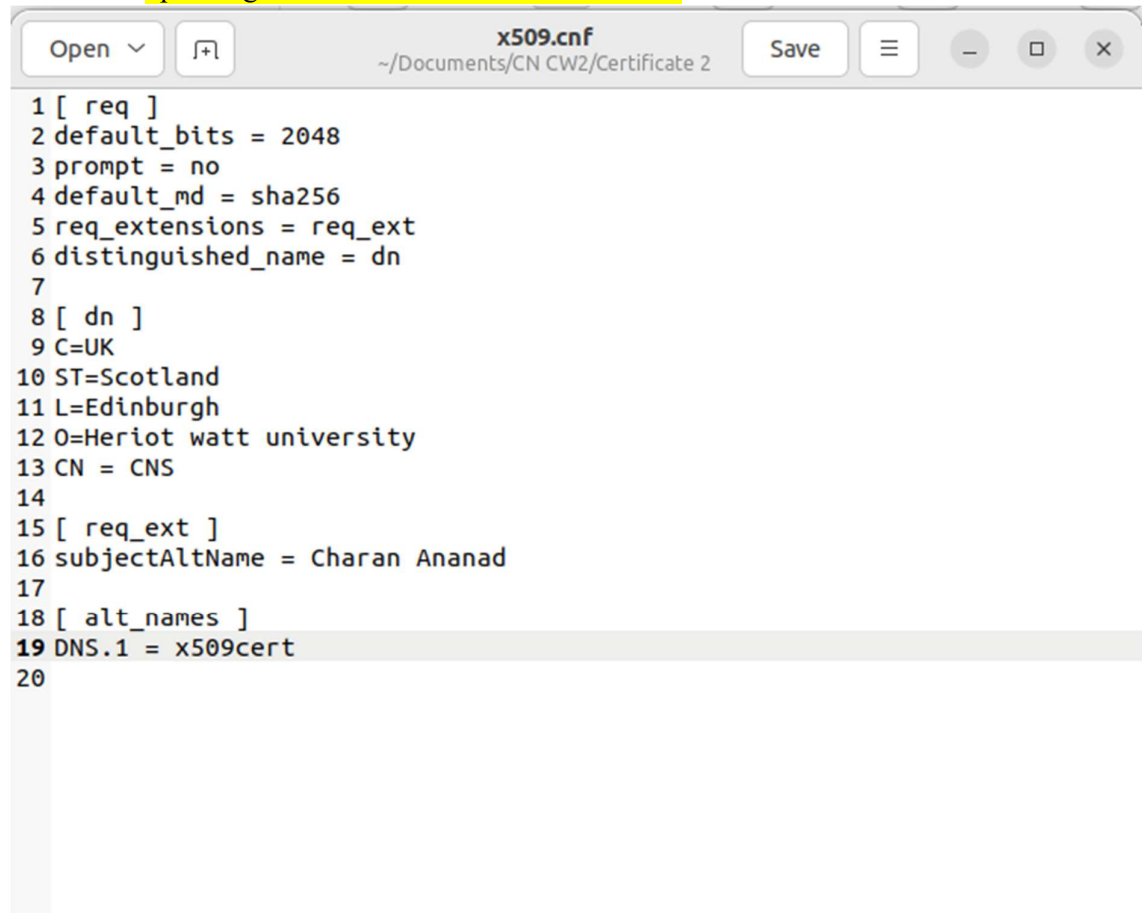


Fig 1.5: pem file created

- In Task 2, as I am doing this coursework individually I was unable to find a proper partner to perform this task. But I have managed to understand how to complete this task. We would require to import the GPG file to our directory and use the command to sign their certificate. This helps to make sure that the person is authentic to view the file.

This is done by creating a digital fingerprint of their certificate which is later on compared to that of the person. When the two fingerprints match, the person is verified.

- In Task 3, I have created a plane text file and signed it with my private key. With this I can make sure that the file is authentic and has not been tampered with.
- In Task 4, I have created a new X.509 certificate and private key using the openssl command: `openssl genrsa -des3 -out <file name> 2048`



```
1 [ req ]
2 default_bits = 2048
3 prompt = no
4 default_md = sha256
5 req_extensions = req_ext
6 distinguished_name = dn
7
8 [ dn ]
9 C=UK
10 ST=Scotland
11 L=Edinburgh
12 O=Heriot watt university
13 CN = CNS
14
15 [ req_ext ]
16 subjectAltName = Charan Ananad
17
18 [ alt_names ]
19 DNS.1 = x509cert
20
```

Fig 4.1: cnf file of X.509 certificate

This will be followed by requesting a passphrase in which the user has to input and verify using the same. For the certification request we are requested to enter information providing our locality and organization name, common name and official email address.

To generate an RSA private key which is 2048 bit long the following command is to be executed.

```
OpenSSL genrsa -out <file name> 2048
```

The information entered will be incorporated to the certificate using the following command:

```
OpenSSL req -new -key <inputfile> -out <outputfile name>
```

- In Task 5, we will be creating a local Certificate Authority to sign certificates and guarantee the integrity of the information embedded in them. Having the local CA in place, we can then sign a certificate to ensure that the information it contains is valid and trusted. This is achieved by using the CA to generate a signature and then adding it to the certificate, so that it can be verified by anyone who receives it. This signature serves to authenticate the certificate and guarantee its integrity, making it much more secure.

```
OpenSSL req -X509 -new -nodes -key <file name> -sha256 -days 365 -out <output file name>
```

After executing the above command, the same information that has been created for X.509 certificate is to be

entered again making sure either of them is matched. Using the private key which will use the message

digest SHA256 and giving the validity till 365 days and the output file be created as <filename.pem>

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQCuo/Qpst0jyvL4
wpzCJP7ZXsGlnWqL5NTMVAky66Tf5jviWRd9Jx8Ep1GnFdyH8FEphT5D7dykiuGp
7UgR1xbj+/6l0I+Tcc56owP0NcwTajg3wBL1DDsagoaZuF8kb9Sp8nag70lHQmZj
aCmrAuMKWfw6wwcDVMYh7KnpMkg2ioe6v0WLQgsBUww/PZLxGAByaue6DB6HbVNQu
jOC0qNDAG7jYTd0d0cP9AoQzT8EURd0KpmYufFxzj8oR4Werj21LXDdhpBtDuPN2
QnRKBeBUCUBkRYdx0d9KBSun170KwWS2I3QMiZWMcZH0BFFyRG04jmoiSah34Zm
/G3gB9YXAgMBAAECggEAAtpKryYjAQLXHingadA5hAFhtzJBF/B1dX1pbeYcvDc4
/vgcRj1s5iFfLwp0kLDWT4rFsEnYiZ1p+9tIkGlgCH7a54pR2Lw98IRVGw4H6MSO
dnCynfj9t/cnALQYbjmVQs8XFpHpkMstZyyXiBo63L8KM1VW9rnXn1L6i1Tj0LFXy
54iENLpRNv1nm0oQcDioUcpUVsR65b1+tdtXTcUKgjVKAX8B1g/l8bYwc/GzcLuS
+tInYVpyX+yRX4z2lwHQtX1Iu4nhi+TL0Vwklp4Kux2F9m7Vr2RRda8tdn30Xwt6
D7htcb3YmYfqcB0C5YdsS1yZTSOqxulPtoam3pe2oQKBgQDwcJf9qg61JzfIGHqH
6AcbtKbaEBJ42FoAJ3S1PEvjsytKnp12eY8QnSuMSASUPb+W0NEnlt0WfUuGrLVZ
nlmYwpnJkv18aIg7Zx8NYwq4q+3d37U1M4c8qDcn8RX6+hrJVLGsFApeEjnl3d76
WiVVnoTBpLD0vfNffvsK89icRwKBgQC58UA7yW29SaumbUusoBXa96M7/vHc9GiA
s1ty30TxGAK5UN4mJIFutAP0oLNQ7V3Q3h0ZEjzLxNNFicQHTYjmUMimEZhD0TVG
YNgiB6LJgXsFRdvpnzXxv0aDnwfsPr3uc4qz2cNtoqrp6fZC0v0kgP19YV+RcYiX
3YrSVfdvsQKBgA2F56aGuAkMSaDhb5LRRAUU5gwBveg6EuXLuk8XMxV9cEPkI6av
s5I1pMthCZDk4C+1Uu4tGAeqSvMqJ5EAzP1AhLHHqGyM3Iyqwh5Yob09R8Wg3WLY
OpT4yRFgB+JzyqnkRvessOCVmdgJ4I6oH01vevwBLUq2nEeUtr3o9Rf1AoGAeThL
P07baQyvJ8eXDwoqVV8d/s39FaQMw0Ks2pwhcP/LPs72LH02GFqPJLrLS/wDL1iv
NZoLinjF107yCiTE/AlsVb+guSqBicky/ngy8xVDgz0A47RUsa0JxoMV0T3wCpUu
toNf8JVawTYywmv0RIzJYWTgreILP55Bk1BSCHECgYEA0V2NBUIP+QewcIECL+a7
00qfVaxQsX7JjmPcqdyVNzhYl0C4U05cV0gLHQqu12Be5iVqDIBni+B1LXRdf0+
2Iya/nrvMvosQ1itqjF06Y6artzgw+9DirEpYy/j1ITJ1qiA9qAxrybis+tRtNN0
2qTUhuFFaowm2iMwGYHHPwE=
-----END PRIVATE KEY-----
```

Fig 4.2: X509 key generated



- In task 6, unfortunately I was unable to connect to other members to proceed with this task as well.

#### Observations:

- Once Task 3 is implemented, the resulting text document will likely contain both the plain text and an encrypted PGP certificate. The PGP certificate will be encrypted using the SHA1 hash algorithm.
- We have observed that unauthorized access to a system or network may be possible through the use of a "man-in-the-middle" attack. In this type of attack, a threat vector (such as a malicious actor or software) creates a fake keypair and poses as a reliable source to trick one of the victims into using the attacker's public key. The attacker then acts as a middleman to intercept and potentially manipulate the information being exchanged between the sender and the receiver without their knowledge or consent. This type of attack can be particularly effective if the victim is not aware of the threat and trusts the attacker's key as a genuine one from a reliable source. It is important to always verify the authenticity of any key or certificate before using it to ensure that it is not being used as part of a man-in-the-middle attack.
- In a certificate signing request, the process of obtaining a digital signature from a certificate authority (CA) typically involves the creation of a keypair. One key is kept private and the other is sent to the CA to be digitally signed. The CA then performs various checks and verifications before signing the public key and issuing a certificate. This certificate may include additional features or information, such as the identity of the certificate holder or the purpose for which the certificate can be used. The digital signature from the CA provides a level of assurance that the public key belongs to the entity that it claims to represent, and can be trusted for secure communication or authentication.

NOTE: I was unable to attach all the references so kindly check the files submitted through gitlab for codes used and certificate files.