The report shows how I extracted the private key and public key using the OpenSSL library.

<u>**Step1:**</u> **Key Pair Generation (private key)**

Key size can be anything among 512-bits, 1024-bits, 2048-bits. I decided to use 2048-bits as it is secure.

- The command to run to generate the key is as follows,

  “**openssl genrsa -aes128 -out privatekey.pem 2048**”

  Output will be as follows:

  ```
  Generating RSA private key, 2048 bit long modulus (2 primes)

  .....................................................+++++

  ..................................................+++++

  e is 65537 (0x010001)

  Enter pass phrase for privatekey.pem:

  Verifying - Enter pass phrase for privatekey.pem:
  ```

<u>**Step2:**</u> **Certificate Generation (using private key)**

In this step, we take the private key as the input and create a certificate in ‘.crt’ format and the number of days the certificate we want to be valid for.

- The command to run to generate a certificate is as follows,

  “**openssl req -new -x509 -key privatekey.pem -out certificate.crt -days 360**”

  Output will be as follows:

  ```
  Enter pass phrase for privatekey.pem:

  You are about to be asked to enter information that will be incorporated

  into your certificate request.

  What you are about to enter is what is called a Distinguished Name or a DN.

  There are quite a few fields but you can leave some blank

  For some fields there will be a default value,

  If you enter '.', the field will be left blank.

  -----


  Country Name (2 letter code) [AU]:US

  State or Province Name (full name) [Some-State]:NewMexico

  Locality Name (eg, city) []:LasCruces
  ```

Organization Name (eg, company) [Internet Widgits Pty Ltd]:NMSU

Organizational Unit Name (eg, section) []:NMSU

Common Name (e.g. server FQDN or YOUR name) []:RahulGarigipati

Email Address []:rahulg@nmsu.edu

<u>Step3:</u> Converting the Certificate to a readable format

In this step, we convert the certificate to a readable format, i.e., PKCS12 format.

- The command to run to convert the certificate to '.p12' is as follows,

  "**openssl pkcs12 -export -inkey privatekey.pem -in certificate.crt -out certificate.p12 -name "My Certificate"**"

  Output will be as follows:

  Enter pass phrase for privatekey.pem:

  Enter Export Password:

  Verifying - Enter Export Password:

- And the command to run to convert the certificate from '.p12' to '.txt' is as follows,

  "**openssl pkcs12 -in certificate.p12 -out certificate.txt -nodes**"

  Output will be as follows:

  Enter Import Password:

<u>Step4:</u> Public Key Extraction from the privatekey

In this step, we take the private key as the input to generate the public key.

- The command to run to generate the public key is as follows,

  "**openssl rsa -in privatekey.pem -pubout -out publickey.pem**"

  Output will be as follows:

  Enter pass phrase for privatekey.pem:

  writing RSA key

- The Passphrase for the privatekey.pem that I have chosen is: "14789".