Confidential Computing – Assignment 1

Submit by: Noam Tarshish (207761024) & Daniel Hodisan (205795016) & Lavi Ben-Shimol (3307866756)

Creating Digital Certificates

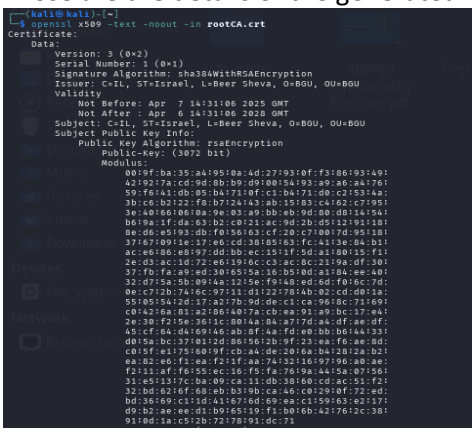
1. Firstly, we generate the RSA private key for the root CSA using this command:

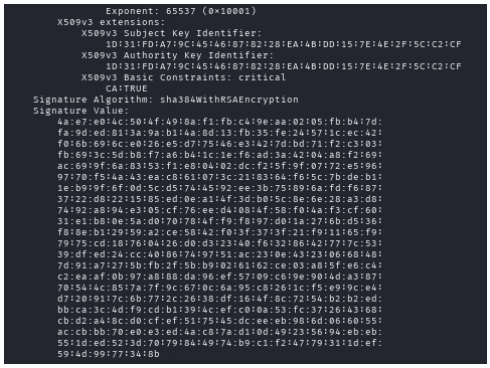
openssl genrsa -out rootCA.key 3072

then, we create the self-signed root certificate with serial number 01 using this command:

openssl req -x509 -new -nodes -key rootCA.key -sha384 -days 1095 -out rootCA.crt -set_serial 01

Those are the details of the generated root certificate:





2. we generate Alice's RSA key pair and certificate for Alice with those steps:
Generate Alice's RSA private key:

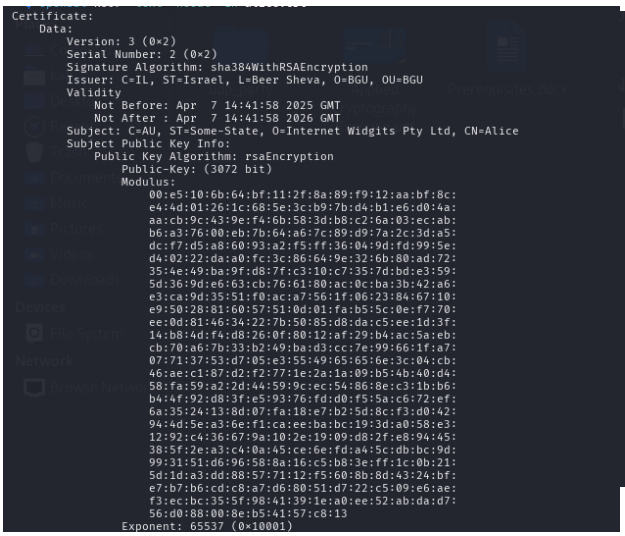
openssl genrsa -out alice.key 3072

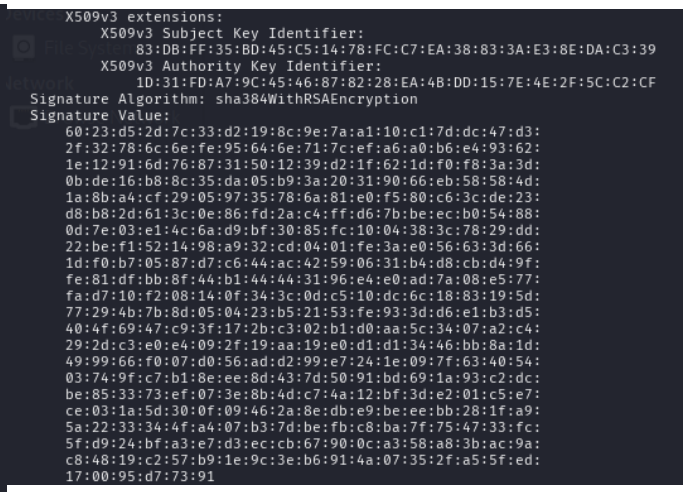
Create Alice's Certificate Signing Request (CSR) :

openssl req -new -key alice.key -out alice.csr -sha384

Sign Alice's CSR with the root CA:

openssl x509 -req -in alice.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out alice.crt -days 365 -sha384 -set_serial 02
We got the certificate:





3. we generate Bob's RSA key pair and certificate for Alice with those steps:
Generate Bob's RSA private key:
openssl genrsa -out bob.key 3072

Create Alice's Certificate Signing Request (CSR):
openssl req -new -key bob.key -out bob.csr -sha384

Sign Bob's CSR with the root CA:
openssl x509 -req -in bob.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out alice.crt -days 365 -sha384 -set_serial 03
We got the certificate: