Report

Q) What are limitations of self-signed certificate? What are they useful for?

A:  It is an identity certificate that is signed by the same entity whose identity it certifies. ]

Limitations:

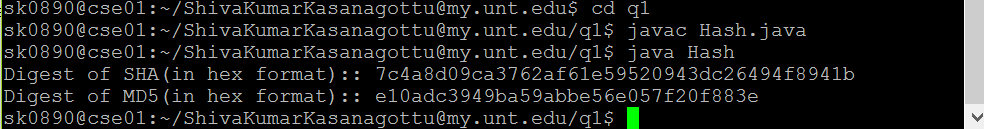
* Other parties do not have trust on these self-signed certificate.
* Needs lot of maintenance for renewal, replacement of certificate.
* They use weak hash and cipher technologies which are not qualified for present security policy.
* The advantage of no need for PKI(Public key Infrastructure) makes it unsupportive at situations were PKI is needed and makes it an disadvantage.

Useful for:

* They are useful in situations were no PKI is not needed.
* They are automatically created during installation process.

Q1)

Running of function Hash

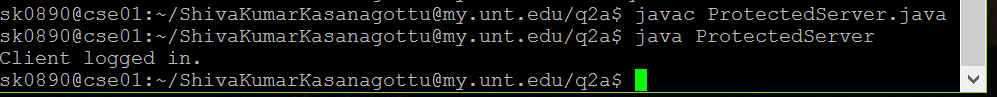


Q2)

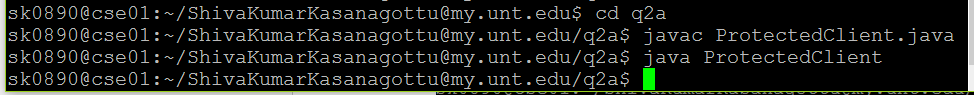
a)

Running of function:

First compile and run ProtectedServer.java file

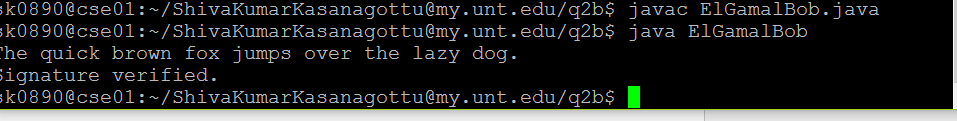


Next compile and run ProtectedClient.java

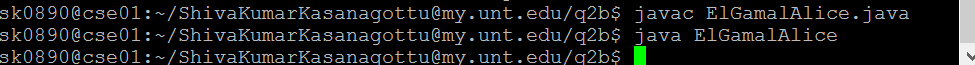


b)

first run ELGamalBob.java

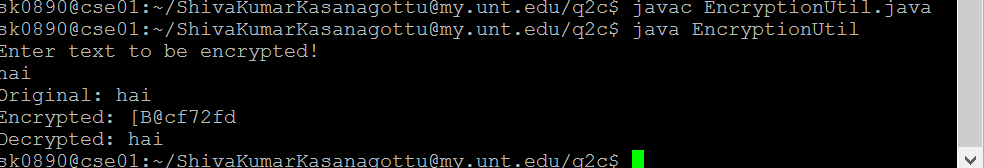


Later run ELGamalAlice.java



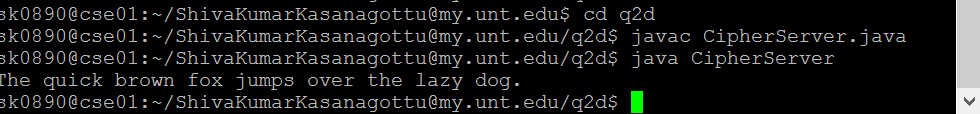
c)

run EncryptionUtil.java

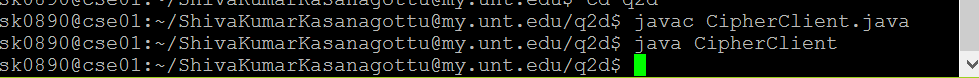


d)

first run CipherServer.java



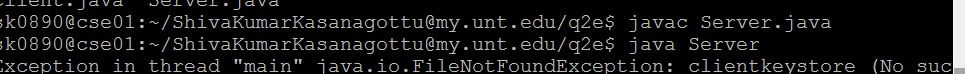
Later run CipherClient.java



e)

first generate keystore and certificate using commands:

Later run Server.java



Now run client.java

