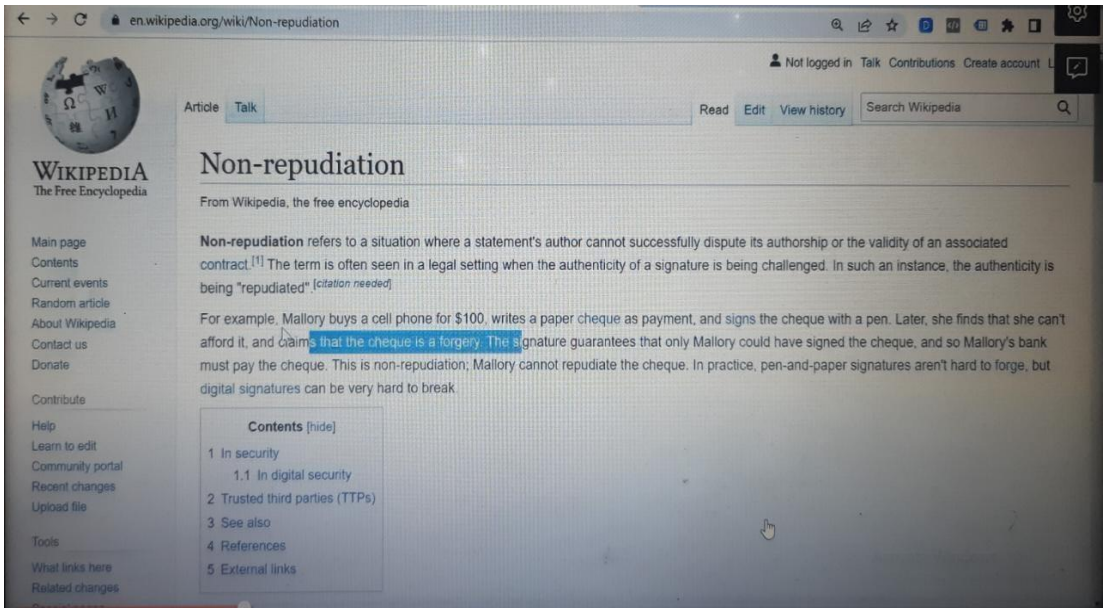
Cryptography Session No.09
Summary 29-07-2022

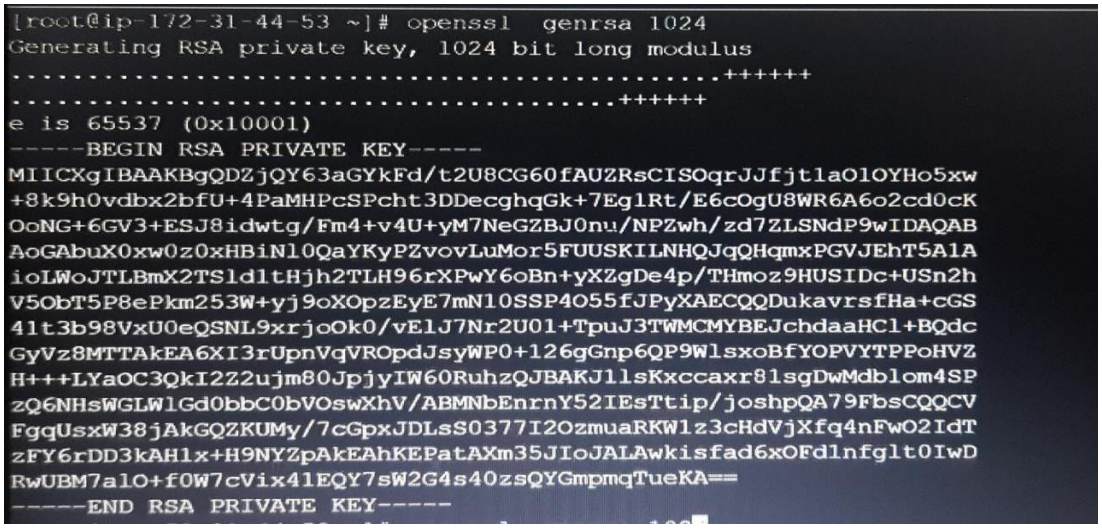
Detailed Discussion on below points –

- In Hybrid Encryption – we have bugs – it can be compromised – to solve this we have to build PKI (Public Key Infrastructure)
- PKI behind the scene uses Digital Signatures
- Digital Signatures can be used to overcome non repudiation issues
- Brief on Non-repudiation

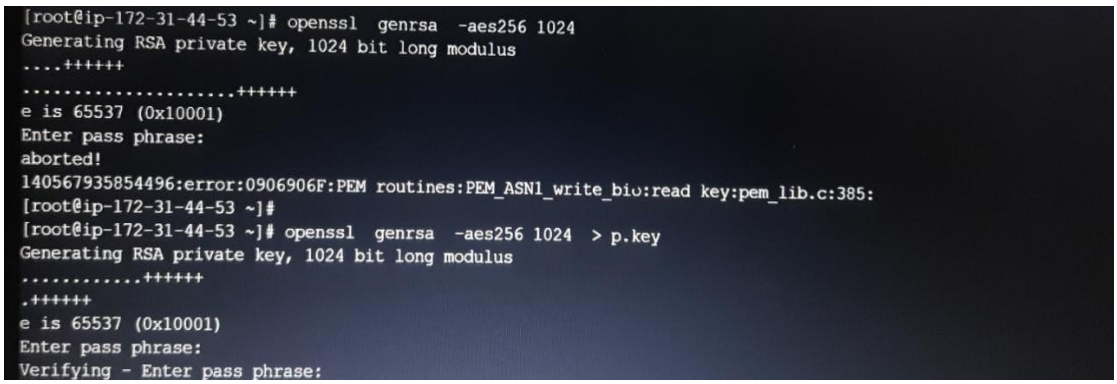


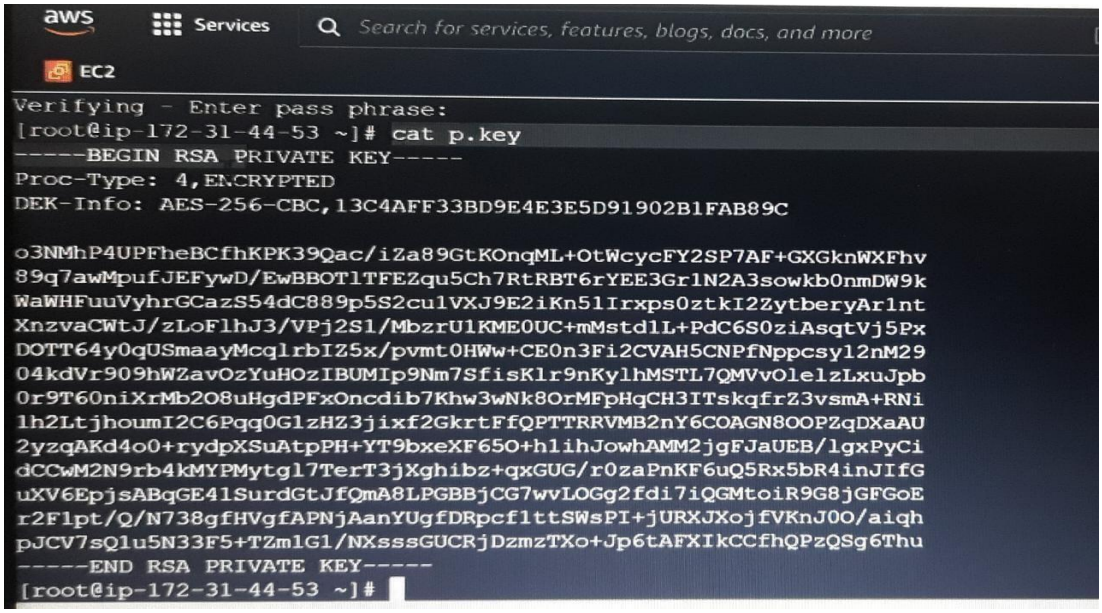
- To implement Digital Signature we use ECDSA (Elliptic Curve Digital Signature Algorithm)- compared to other algorithms like DSA,ECDSA is faster
- To sign a message that is for authenticity we use Private Key
- To verify the message actually signed by real private key we use Public Key.

- To create Private Key- it is the identity- to sign a message

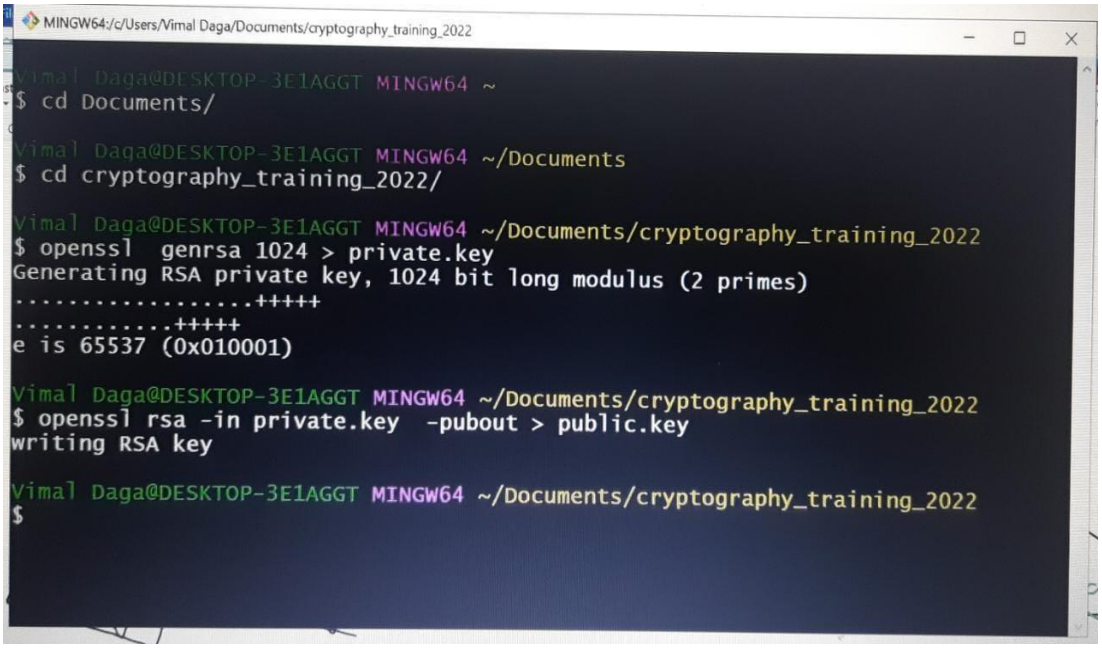


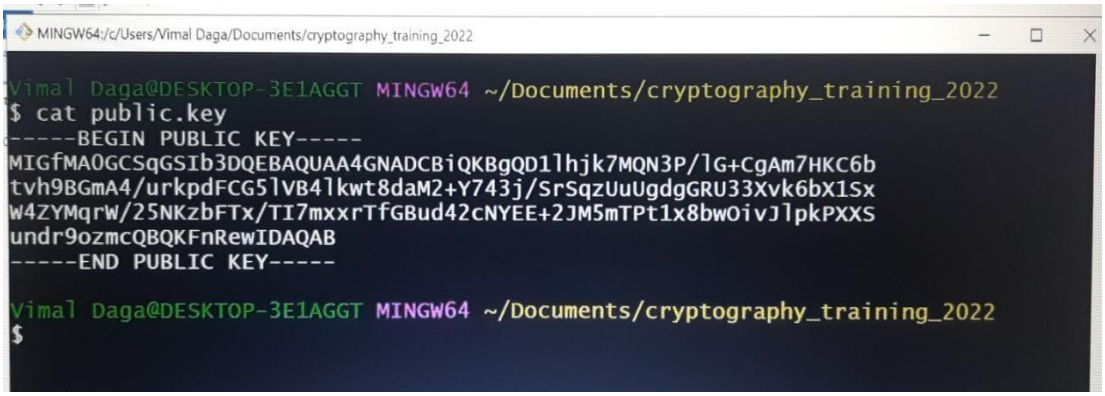
- Private key is sensitive , it can be encrypted using AES algorithm and stored in a file- here private key stored in a encrypted way



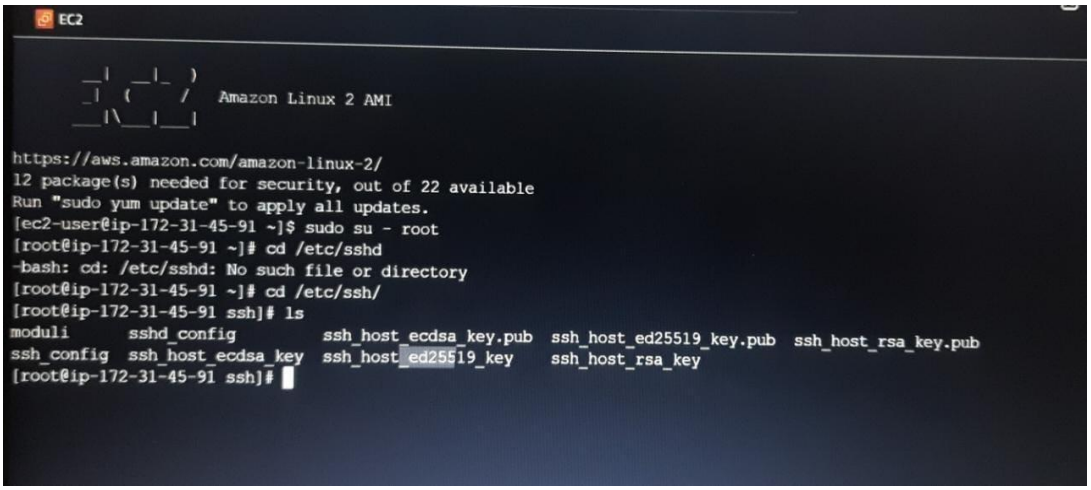


- Public Key is generated from the Private Key and stored in file

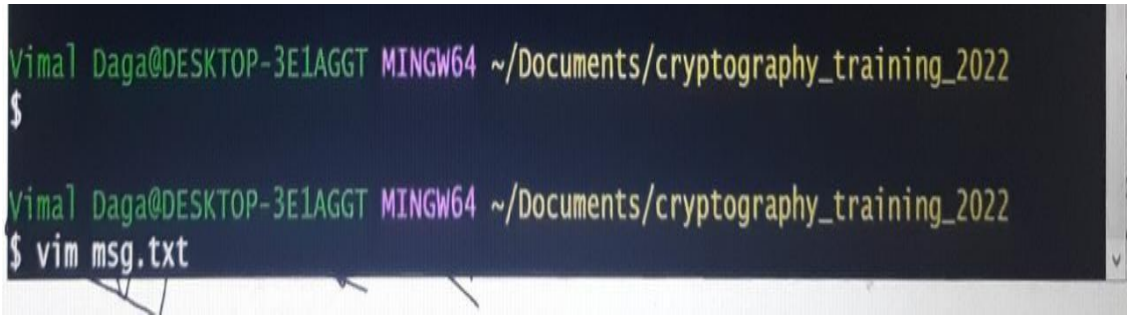


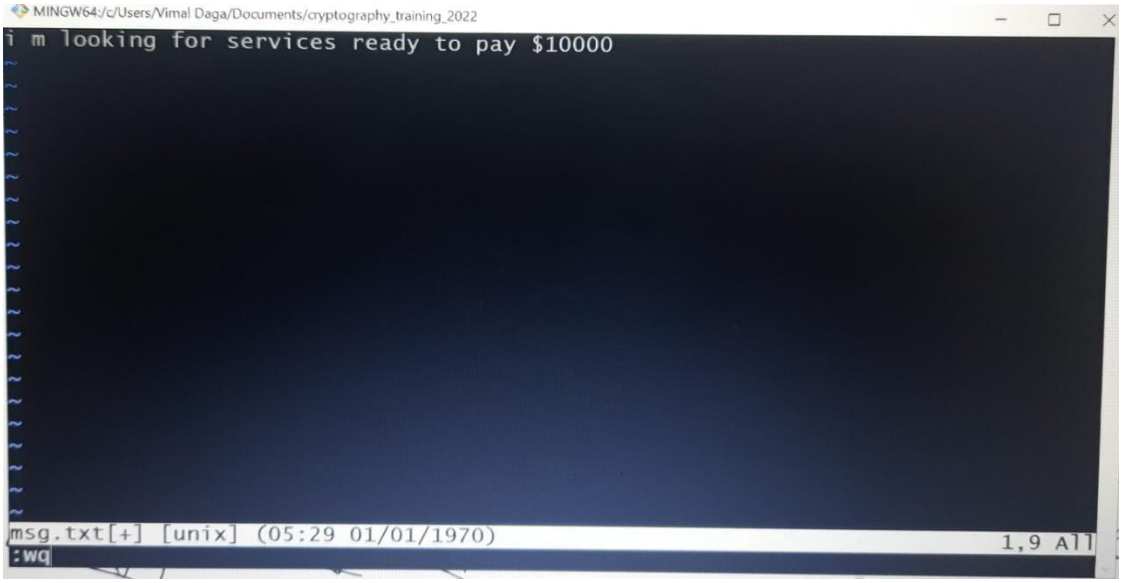


- Some of the servers like SSH – for remote login- automatically creates Private and Public Keys

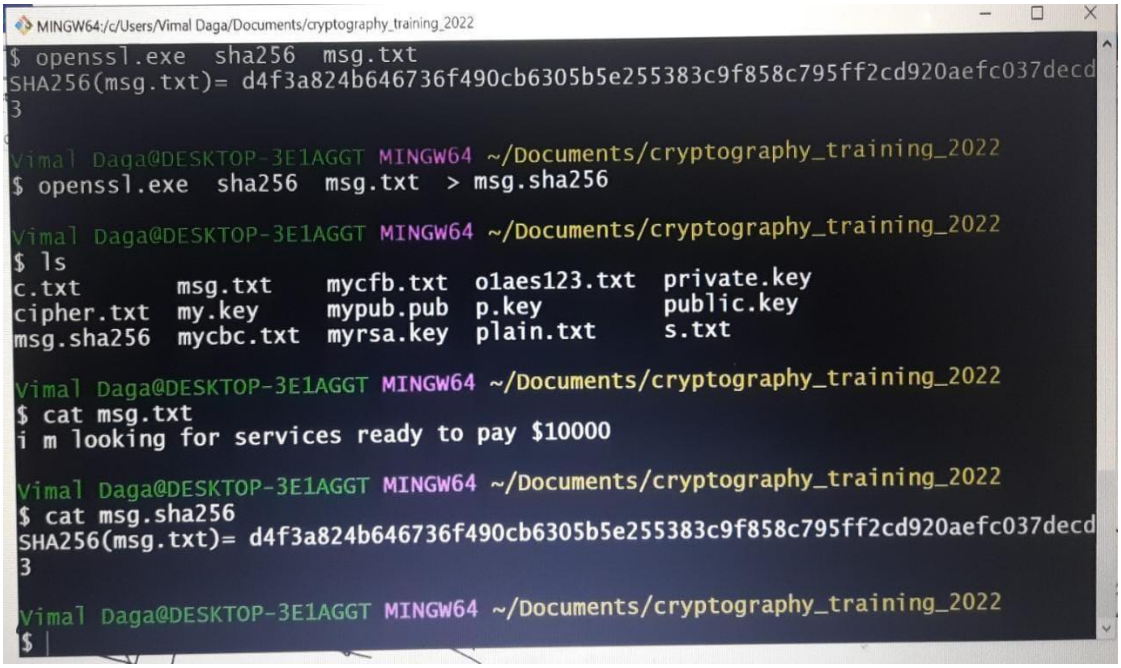


- Sign a message for authenticity

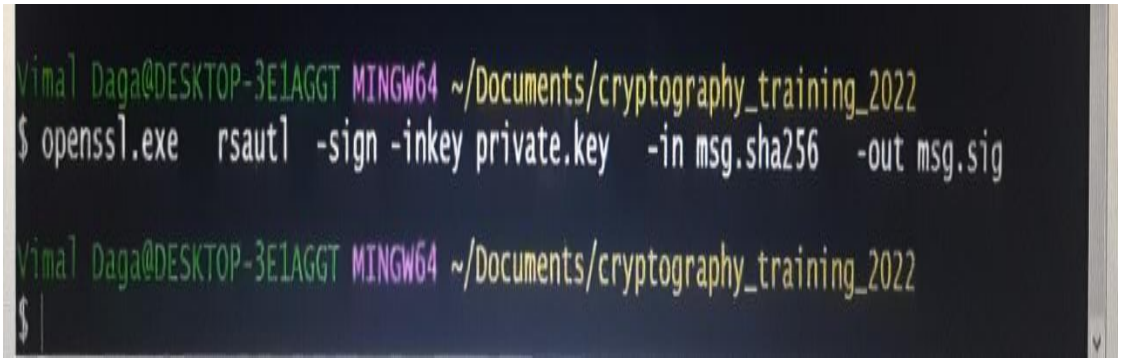


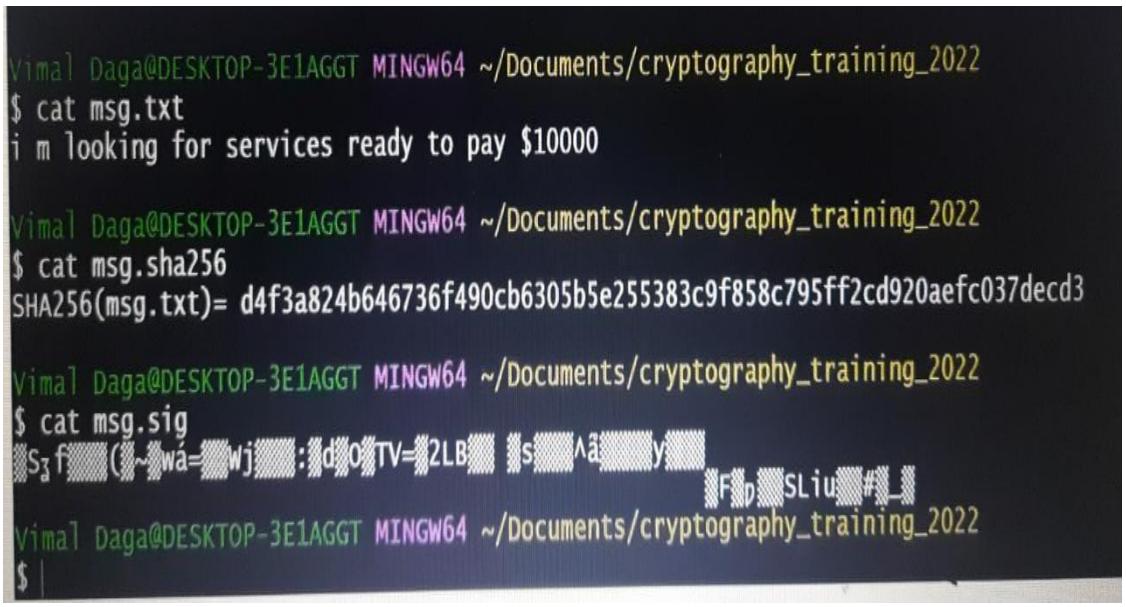


- Create a HASH value of the message-to check integrity of data – so that no one can edit the message

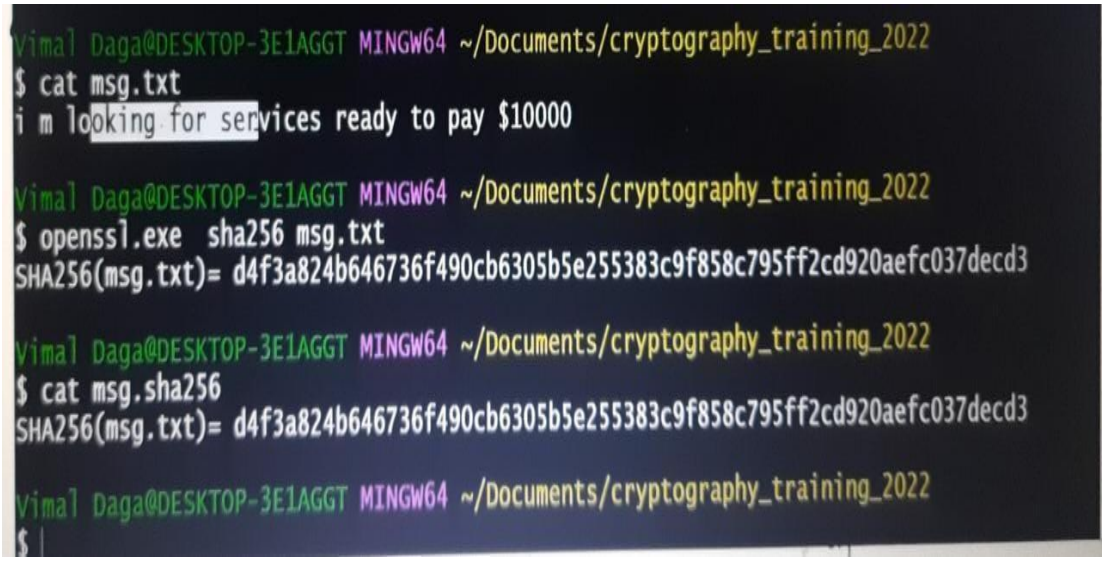


- Sign a message- technically we sign the hash – this creates the signature on the data and we can save it in a file

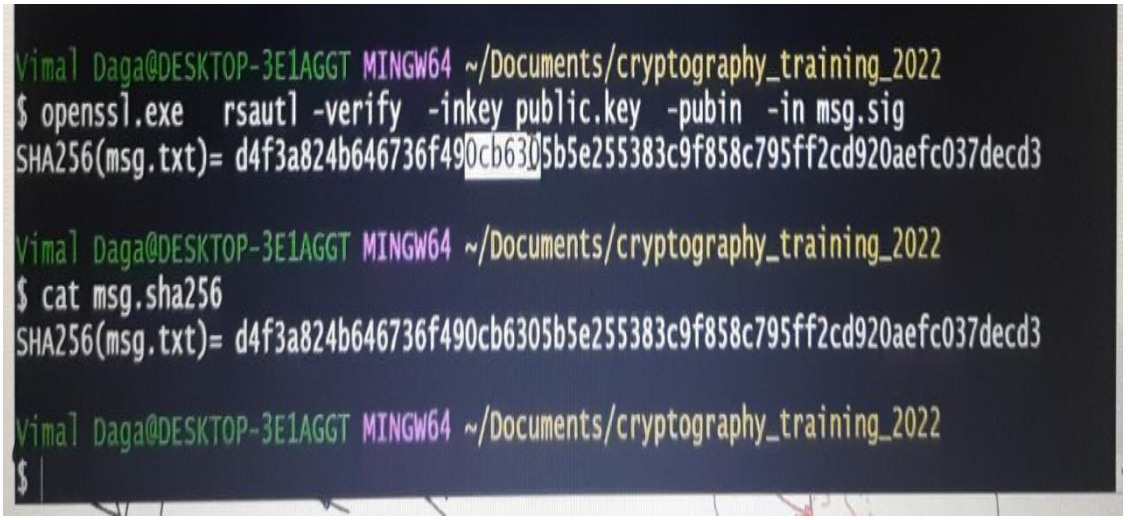




- Before the client using the data- they have to check data integrity using hash – to check whether data is edited or changed at the client end.



- To verify the message actually signed by real private key, we use Public Key- to check hash is sent by actual server



- Brief on PKI (Public Key Infrastructure) – how to excel the Public Key for verification of the Signatures.

Important Links –

Hash13 link for Extra Sessions and session recording - https://learning.hash13.com/

Community Link to post Query, Doubts and share your blogs - https://hash13-community.circle.so/home