Rebecca Dias TECMPNA
182027 19

Ans:- (1) Digital certificate is an electronic file that is used to identify people and resources over a insecure network channel. Digital certificate also enable secure confidential communication between sender and receiver using encryption.

(2) For example when we travel to another country, our passport provides a way to establish our identity and gain entry. Digital certificate provide similar identification in the electronic world.

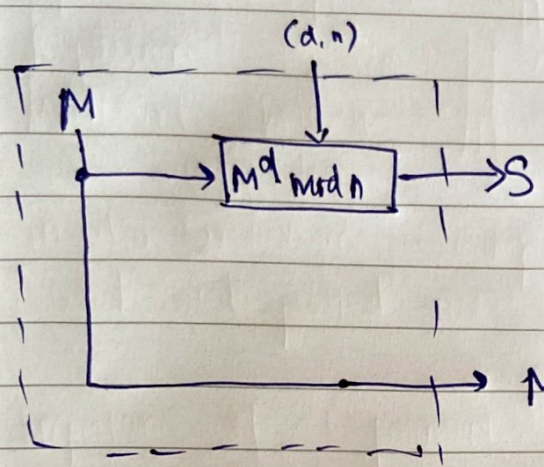
(3) The role of certification Authority (CA) is to issue certificates with authorized digital signatures. Much like the role of passport office, the role of the CA is to validate the certificate owners identity and to "sign" the certificate so that it cannot be tampered by unauthorized user.

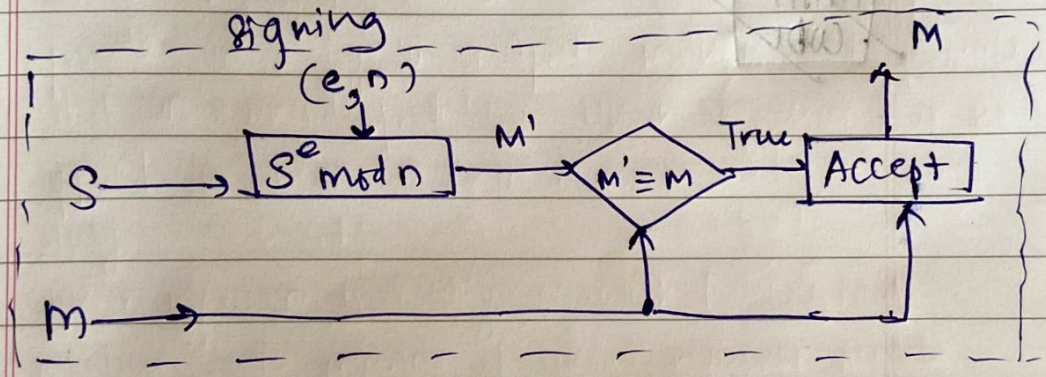
(4) X.509 defines structure of digital certificate RSA Digital signature scheme

1) The idea of RSA can also be used for signing and verifying a message.
2) Also known as RSA Digital Signature Scheme.
3) The digital signature scheme changes the role of private and public key
4) Here, the private and public key of the sender is used.

5) Sender uses her own private key to sign the document
6) Receiver used the senders public key to verify it

M : Message
S : signature.





Verifying

7) Key generation in the RSA digital signature scheme is exactly the same as key generation in RSA
8) Sender selects 2 prime numbers p and q
9) Calculate $\phi(n) = (p-1)(q-1)$
10) Sender then chooses e, calculates d such that $e*d = 1 \bmod \phi(n)$

Sender keeps d and announces n and e