08/2/22: Modes of Symmetric Encryption:-

Mode 1: Electronic Code Book (ECB).

Mode 2: Cipher Block Chaining (CBC).

How to verify if the public key's used for encrypting a message is true (or) not.

CA: $Sign_{SK_{CA}}(PK_B) \longrightarrow (cert_B, PK_B)$

Alice: $verify_{PK_{CA}}(cert_B, PK_B) \stackrel{?}{=} True.$

Symmetric key Cryptography:-

(PK_A, SK_A) Alice

(PK_B, SK_B) Bob

1) secret key K

2) DO $EP_{KB}(K) \rightarrow C$

3) send C →

4) DO $DS_{KB}(C) \rightarrow K$

5) DO $E_K(M) \rightarrow C'$

6) send C' →

MAC (Message Authentication Code):

Alice → Bob

$C, Tag \xrightarrow{} C', Tag'$

$D_K(C') \rightarrow M'$

$Mac(K, M') = Tag''$

$Tag'' \neq Tag'$.

08/25/22

Hash Functions:-

Digital Signature: → used to provide Authenticity.

→ It is based on public-key cryptography