10/25/22: Key Encapsulation Mechanism (KEM):-

Encryption $E_{(PK)}(K) \rightarrow c$. (Randomized Encapsulate)

Public key

$D_{(SK)}(c) \rightarrow K$. (Deterministic Decapsulate)

decryption key

shared key

Data Encryption Mechanism (DEM):-

$E_K(M) \rightarrow C$ (Randomized)

$D_K(c') \rightarrow M$. (Deterministic).

Public-key Cryptography-2:-

ElGamal:-

$C = \{c_1, c_2\}$

$c_1 = g^y$;

$c_2 = h^y \cdot m = g^{xy} \cdot m$.

$$\frac{h^y \cdot m}{g^{xy}} = \frac{g^{xy} \cdot m}{g^{xy}} = m.$$

(or)

we can also do, $m \leftarrow \frac{c_2}{(c_1)^x} = \frac{g^{xy} \cdot m}{(g^y)^x} = m.$

Diffie - Hellman Key Exchange:-

$S_{KA} \in Z_p$

$S_{KB} \in Z_p$

(From the slide No: 6)

Step-6: Alice: $\left(g^{SK_B}\right)^{SK_A} \bmod p.$

Step-7:- Bob: $\left(g^{SK_A}\right)^{SK_B} \bmod p.$

10/27/22 **Diffie - Hellman man in the middle Attack:-**

$K_2 = g^{SK_A \cdot SK_2} \pmod p$

$K_1 = g^{SK_1 \cdot SK_B} \pmod p$

ELGamal Signatures:-

(From slide No: 13, diagram)

Step: 10 to 12:- $V_1 = g^h \bmod p$

$$V_2 = \left(P_{KA}^{S_1} \cdot (S_1)^{S_2}\right) \bmod p$$

$$= \left(\left(g^{SK_A}\right)^{S_1} \cdot \left(g^K\right)^{K^{-1}\left(h - SK_A \cdot S_1\right)}\right) \bmod p$$

$$= \left(g^{SK_A \cdot S_1} \cdot g^{K \cdot K^{-1}} \cdot g^{\left(h - SK_A \cdot S_1\right)}\right) \bmod p.$$

$$= \left(g^{SK_A \cdot S_1} \cdot g^{h} \cdot g^{-SK_A \cdot S_1} \right) \bmod p$$

$$= g^{h} \bmod p.$$