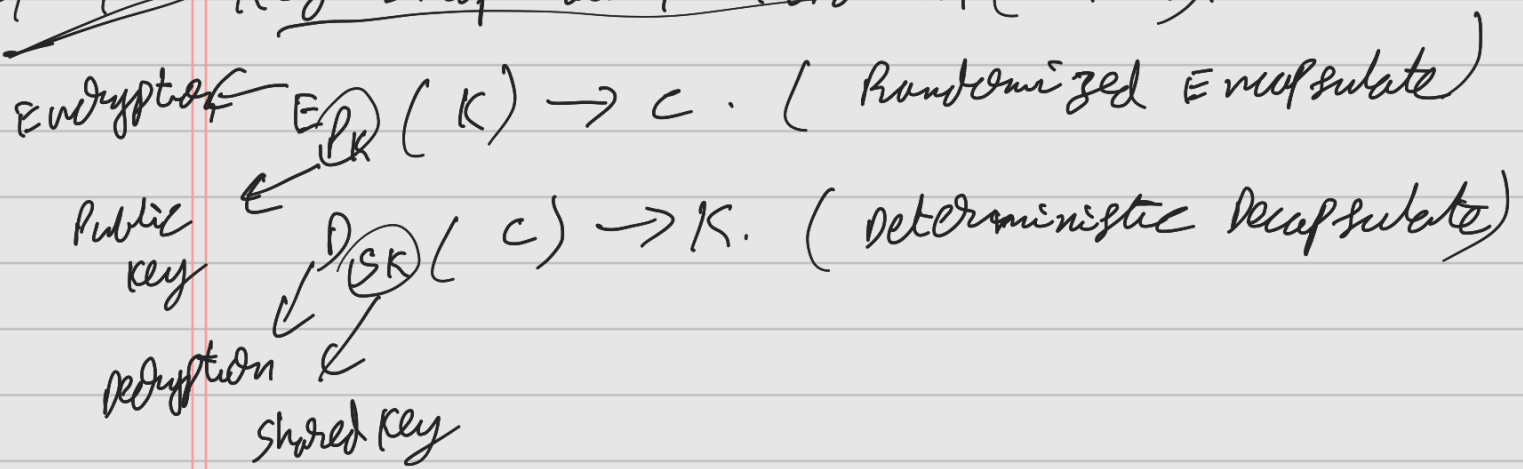


10/25/22: Key Encapsulation Mechanism (KEM):-



Data Encryption Mechanism (DEM):-

$$E_K(M) \rightarrow C \quad (\text{Randomized})$$

$$D_K(C') \rightarrow M. \quad (\text{Deterministic})$$

Public-Key Cryptography-2:-

ElGamal:-

$$C = \{c_1, c_2\}$$

$$c_1 = g^x;$$

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

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

(or)

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

Diffie - Hellman Key Exchange:-

$$S_{KA} \in \mathbb{Z}_P.$$

$$S_{KB} \in \mathbb{Z}_P.$$

(From the slide no: 6)

Step-6:

Alice:
$$\left(g^{S_{KB}} \right)^{S_{KA}} \mod P.$$

Step-7:- Bob:
$$\left(g^{S_{KA}} \right)^{S_{KB}} \mod P.$$

10/27/22

Diffie - Hellman Man in the middle Attack:-

$$K_2 = g^{S_{KA} \cdot S_{K_2}} \mod P$$

$$K_1 = g^{S_{K_1} \cdot S_{KB}} \mod P$$

ElGamal Signature:-

(From slide no: 13, diagram)

Step: 10 to 12:-
$$V_1 = g^h \mod P$$

$$V_2 = (r_{KA}^{S_1} \cdot (S_1)^{S_2}) \mod P$$

$$= \left((g^{S_{KA}})^{S_1} \cdot (g^K)^{K^{-1}} (h - S_{KA} \cdot S_1) \right) \mod P$$

$$= (g^{S_{KA} \cdot S_1} \cdot g^{K \cdot K^{-1}} \cdot g^{(h - S_{KA} \cdot S_1)}) \mod P.$$

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

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