10/27/22 RSA Signatures :-

$$\sigma = M^d \bmod N$$

$$\sigma^e = (M^d)^e \bmod N \quad (e \cdot d \bmod \phi(n) = 1)$$

$$= M \cdot \bmod N = M.$$

11/01/22

$$\sigma = (\sigma_1 \cdot \sigma_2)^e \cdot \bmod N$$

$$= M \bmod N = M.$$

(slide no: 13)

1st change: $H(M) \rightarrow H(S, M)$ ; $S \in \{0,1\}^n$

2nd change: $H(\ldots H(M))$

P.K = (P.K, challenge set)

S.K = (S.K, challenge set).

Schnorr Identification Scheme :-

$$g^x \cdot y^{-c} = g^{cx+k} \cdot g^{-x \cdot c} = g^k = I.$$

11/03/22 (slide no: 24, 25)

DSA's ID scheme :-

Bob's verification :- (step 7 from diagram)

$$g^{\alpha s^{-1}} \cdot y^{x s^{-1}} \stackrel{?}{=} I = g^k$$

$$= g^{\alpha s^{-1}} \cdot g^{\alpha x s^{-1}}$$

$$= g^{s^{-1}(\alpha + \alpha r)}$$

$$= g^{k \cdot (r + \alpha r)^{-1} \cdot (\alpha + \alpha r)} = g^{k}.$$

$\because s^{-1} = k \cdot (\alpha + \alpha \cdot r)^{-1} \bmod q.$

(Slide No: 26)

DSA:

Bob's verification:- (Step 6 from diagram)

$$F\left(g^{H(m)s^{-1}} \cdot y^{r \cdot s^{-1}}\right) \stackrel{?}{=} r$$

$$= F\left(g^{H(m)s^{-1}} \cdot g^{\alpha r s^{-1}}\right)$$

$$= F\left(g^{s^{-1}(H(m) + \alpha r)}\right)$$

$$= F\left(g^{s^{-1}(H(m) + \alpha r)}\right)$$

$$= F\left(g^{\left[k \cdot (H(m) + \alpha r)^{-1} \cdot (H(m) + \alpha r)\right]}\right)$$

$$= F(g^{k}) = r.$$

(Slide No: 33, 34)

Lamport Scheme:-

Ex: $m' = 101$

$\sigma' = (x_{11}, x_{20}, x_{31})$

$A: Sk_A\left[\alpha_{10}, \alpha_{11}, \alpha_{21}, \alpha_{20}, \alpha_{31}\right)$.

$PK_A =$