CLASS ASSIGNMENT

SOHAM SHINDE
2019BCS0054

Q1. Here $p = 13$
$q = 7$

$n = pq = 13 \times 17 = 91$

$e = 35$

$\phi(n) = (p-1)(q-1) = 12 \times 6 = 72$

Here $(d * e) \bmod \phi(n) = 1$

$(d * 35) \bmod 72 = 1$ —— (1)

for $d = 35$ condition (1) is true

so private key is 35.

Q2. I and II

I for this

Encrypted text = $(\text{plain text})^{e} \bmod n$

Plain text = $(\text{Encrypted text})^{d} \bmod n$

III for this

$(d * e) \bmod \phi(n) == 1$

Similar to $cd = 1 \bmod f(n)$

Q.3. given $q = 7$

Smallest primitive root $a = 3$

Privat key A = 2 = X_A

Private key B = 5 = X_B

$Y_A = a^{X_A} \mod q = 3^2 \mod 7 = 2$

$Y_B = a^{X_B} \mod q = 3^5 \mod 7 = 5$

Secret keys :-

$K_{AB} = Y_B^{Y_A} \mod q = 5^1 \mod 7 = \cancel{2}\ 4$

$K_{AB} = Y_A^{Y_B} \mod q = 2^5 \mod 7 = \cancel{5}\ 4$

∴ value of common secret vale = 4

Q4. given $q = 17$

$a = 5$

$X_A = 4$; $X_B = 6$

$Y_A = (5)^5 \mod 17 = 13$

$Y_B = (5)^6 \mod 17 = 2$

$K_{AB} = Y_B^{Y_A} = (2)^4 \mod 17 = 16$

$K_{AB} = Y_A^{Y_B} = 13^6 \mod 17 = 16$

∴ Common secret key = 16