02/06/2021

20181CSE0621
Sai Ram. K
6-CSE-10

Part-B

Q.5] Given $p = 11$

root = 6.

Let keys $x_a = 4$ $x_b = 6$

- We know $Y_B = a^{x_b} \bmod P$

$Y_A = a^{x_a} \bmod P$

$\Rightarrow Y_A = 6^6 \bmod 11$

$= 46656 \bmod 11$

$= 5$

$\Rightarrow Y_B = 6^4 \bmod 11$

$= 1296 \bmod 11$

$= 9$

$\therefore Y_A = 5 \quad , \quad Y_B = 9$

- We also know,

$K_{AB} = Y_A^{x_B} \bmod P$

$K_{AB} = Y_B^{x_A} \bmod P.$

$\Rightarrow K_{AB} = Y_B^{x_A} \bmod P$

$= 9^4 \bmod 11$

$= 6561 \bmod 11$

$= 5$

20181CSE0621
Sai Ram.

classmate
Date
Page

$$\Rightarrow K_{AB} = Y_A^{X_B} \bmod P$$

$$= 5^6 \bmod 11$$

$$= 15625 \bmod 11$$

$$= 5$$

∴ We obtain shared key = 5