

## Week – 8

### Activity – 1

$$p = 5$$

$$q = 7$$

$$n = 5 \times 7$$

$$n = 35$$

$$\phi(n) = (5-1) \times (7-1)$$

$$\phi(n) = 4 \times 6$$

$$\phi(n) = 24$$

$$e = 5$$

**Public Key: ((e, n) = (5, 35))**

**Private Key: (d = 5)**

### Encryption:

Compute ( $C = M^e \pmod n$ ):

$$[ C = 5^5 \pmod{35}]$$

Calculating ( $5^5$ ): [ $5^5 = 3125$ ]

Now compute ( $3125 \pmod{35} = 89.28$ )

$$3125 - (89 \times 35 = 3115) = 3125 - 3115 = 10$$

$$\mathbf{C = 10}$$

### Decryption:

Compute ( $M = C^d \pmod n$ ):

$$[ M = 10^5 \bmod 35 ]$$

Calculating (  $10^5$  ): [  $10^5 = 100000$  ]

Now compute  $(100000 \bmod 35) = 2857.14$

$$100000 - (2857 * 35 = 99995, 100000 - 99995 = 5$$

$$\mathbf{M = 5}$$

## Activity – 2

$$\mathbf{p = 11}$$

$$\mathbf{g = 2}$$

Prey

$$B = g^b \bmod p = 2^8 \bmod 11$$

$$2^8 = 256$$

$$256 = 23.27$$

$$256 - (23 * 11 = 253) 3$$

$$\mathbf{B = 3}$$

$$s = A^b \bmod p = 9^8 \bmod 11$$

$$( 9^8 )$$

$$9^2 = 81 \bmod 11 = 4$$

Then,  $( 9^4 = 4^2 = 16 \bmod 11 = 5 )$ .

$$[ 9^8 = 9^4 \times 9^4 = 5 \times 5 = 25 \bmod 11 = 3 ]$$

$$\mathbf{s = 3}$$

**Partner name: Sidrah shaikh**

**P=11**

**G =2**

**Private key = 8**