02/06/2021

20181CSE0621
Sai Ram
6-CSE-10.

Part-C.

Q.2] Let the numbers be $p = 11$, $q = 17$

Step1: To calculate n

$$n = p \times q$$
$$= 11 \times 17$$
$$n = 187$$

Step2: Calculate $\phi(n) = (p-1)(q-1)$

$$= (11-1)(17-1)$$
$$= 10 \times 16$$
$$\phi(n) = 160$$

Step3: Choosing 'e'

$1 < e < \phi(n)$ & $\gcd(\phi(n), e) = 1$

We get $e = 7$ i.e. $\gcd(160, 7) = 1$

hence $e = 7$

Step4: Calculating, $d = e^{-1} \bmod \phi(n)$

$$de = 1 \bmod \phi(n)$$
$$7 \cdot d = 1 \bmod 160$$
$$7 \cdot d \bmod 160 = 1$$

$\boxed{d = 23}$ $[161 \bmod 160 = 1]$

2018ICSE0621
Sai Ram.

Step5: Public key = {e, n}

Encryption key = {7, 187}

Step6: private key = {d, n}

Decryption key = {23, 187}

Hence we obtain,

- Encryption :-

$$C = M^e \bmod n$$
$$C = 8^7 \bmod 187$$
$$\boxed{C = 134}$$

Here, M -> Plain text c -> Cipher text.

- Decryption :-

$$M = c^d \bmod n$$
$$M = 134^{23} \bmod 187$$
$$\boxed{M = 8.}$$

Here, M -> Plain text C -> Cipher text

Hence, by applying RSA for encryption & decryption we get

=> $\boxed{\begin{array}{l} C = 134 \\ M = 8 \end{array}}$