

Kinza Raza Khan

SE-009

Network & Information Security (CT-460)

Software Engineering.

Ans 1 $p=2, q=7$

$$n = p \times q$$

$$n = 2 \times 7$$

$$n = 14$$

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

$$\phi(n) = (2-1) \times (7-1)$$

$$\phi(n) = 1 \times 6$$

$$\phi(n) = 6$$

~~prime numbers = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100~~

* Public Key $(e) = 5$

$$\cdot \gcd(\phi, e) = \phi x + ey = 1$$

* Private Key:

$$ed = 1 \bmod \phi n$$

$$5d = 1 \bmod 6$$

$$\therefore d = 5$$

* Encryption:

$$c = m^e \bmod n$$

$$c = 6^5 \bmod 14$$

$$c = 7776 \bmod 14$$

$$c = 6 \text{ (cipher text)}$$

* Decryption:

$$m = c^d \bmod n$$

$$m = 6^5 \bmod 14$$

$$m = 7776 \bmod 14$$

$$m = 6 \text{ (original message)}$$