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 number = 1, 2, 3~~

* Public key $(e) = 5$

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

* Private key:

$ed = 1 \bmod \phi n$
$5d = 1 \bmod 6$
$\therefore d = 5$

* Encryption:

$c = m^e \bmod n$
$c = 6^5 \bmod 14$
$c = 7776 \bmod 14$
$c = 6$ (cipher text)

* Decryption:

$m = c^d \bmod n$
$m = 6^5 \bmod 14$
$m = 7776 \bmod 14$
$m = 6$ (original message)