Question 12

Find keys d and e for the RSA cryptosystem where p=7 and q=11.

SOLUTION

To find d and e, we need to follow the steps to generate a simple RSA key.

Step 1 - Choose two prime numbers 'p' and 'q'.
Here p = 7 and q = 11. (Given).

Step 2 - Calculate the value of 'n', where n = p * q.
Here n = 7 x 11 = 77.

Step 3 - Calculate the value of 'PHI', where PHI = (p - 1)(q - 1).
Here PHI = (7 - 1)(11 - 1).
PHI = 6 x 10.
PHI = 60.
We also need to find the factors of PHI.
The factors of PHI are 1,2,3,4,5,6,10,12,15,20,30,60.

Step 4 - The public component 'e' is generated such that the greatest common divisor of e and PHI is 1 i.e. (e is relatively prime with PHI).
Here the smallest value of 'e' is = 7.

Step 5 - The private key component 'd 'is the inverse of e modulo (PHI).
Here, $d = e^{-1}$ mod(PHI).
$d = 7^{-1}$mod(60).

We can find the value of d using the Euclidean Algorithm.
60 = 7 x 8 + 4
7 = 4 x 1 + 3
4 = 3 x 1 + 1
Now, since we get GCD of Integer and Mod as '1', we can apply the extended Euclidean Algorithm.
1 = 4 + 3(-1)
1 = 4 + (7 + 4(-1))(-1)
1 = 4 + 7(-1) + 4
1 = 4(2) + 7(-1)
1 = [60 + 7(-8)](2) + 7(-1)
1 = 60(2) + 7(-16) + 7(-1)
1 = 7(-17) + 60(2)
7^{-1} x 1 = (-17) + 60(2)

Taking mod(60) on both sides:
7^{-1} x 1mod(60) = (-17) mod(60) + 120 mod(60)
7^{-1} mod(60) = (-17) mod(60) + 0
7^{-1} mod(60) = 43. [Since -17mod(60) = 43mod(60) = 43]

We get d = 43.

Step 6 - We can now find the Private Key and The Public Key.

Private Key (n,e) - (77,7).
Public Key (n,d) - (77,43).

ANS: The keys d and e for the RSA cryptosystem, where p = 7 and q = 11 are,
d = 43.
e = 7.