# RSA Key Generation: Public and Private Keys Explained

For the given two prime numbers, $p = 7$ and $q = 11$, Find the value of modulus (n), totient $\phi(n)$, encryption exponent (e) and decryption exponent (d) and mention the public key and private key.

Solution:
$n = p \times q = 7 \times 11 = 77$
$\phi(n) = (p - 1) \times (q - 1) = (7 - 1) \times (11 - 1) = 6 \times 10 = 60$

Suppose, $e = 7$ (You can pick any number which satisfy two conditions,
**i) $1 < e < \phi(n)$, ii) $\gcd(e, \phi(n)) = 1$)**

To find the value of d, we need to perform gcd of e & $\phi(n)$ first. Then, we can find the value of d by using a backtracking approach.

Here is the calculation of $\gcd(e, \phi(n))$ or $\gcd(7, 60)$ or $\gcd(b, a)$

$a = q \times b + r$
Here,
a = big number
b = small number
q = quotient
r = remainder

$60 = 8 \times 7 + 4$ ………….. (i) [a = 60, b = 7, q = 8 & r = 4]
$7 = 1 \times 4 + 3$ …………….(ii) [a = 7, b = 4, q = 1 & r = 3] #here a is the b of previous step and b is the r of previous step
$4 = 1 \times 3 + 1$ ……………..(iii) [a = 4, b = 3, q = 1 & r = 1]
$3 = 3 \times 1 + 0$ ……………..(iv) [a = 3, b = 1, q = 3 & r = 0]

Since, $r = 0$ at steps (iv), the value of $b$ is gcd of 7 & 60.

To find the value of $d$, we need to backtrack from the step (iii) because this step has remainder 1. **Remember, $(e \times d) \bmod \phi(n) = 1$, must satisfy.**

From step (iii), we can write
$1 = 4 - 1 \times 3$
Now, we're going to replace 3 using the step (ii),
$\Rightarrow 1 = 4 - 1 \times (7 - 1 \times 4)$
$\Rightarrow 1 = 4 - 1 \times 7 + 1 \times 4$
$\Rightarrow 1 = 2 \times 4 - 1 \times 7$
Now, we're going to replace 4 using the step (i),
$\Rightarrow 1 = 2 \times (60 - 8 \times 7) - 1 \times 7$
$\Rightarrow 1 = 2 \times 60 - 16 \times 7 - 1 \times 7$
$\Rightarrow 1 = 2 \times 60 - 17 \times 7$

$2 \times 60$ is divisible by 60. So, $-17 \times 7$ is the reason for the remainder 1. Here, $e = 7$, so $-17$ can be $d$.

For eliminating negative value, we can add 60 ($\phi(n)$) with $-17$.

So, $d = -17 + 60 =$ **43** which satisfy the condition **$(e \times d) \bmod \phi(n) = 1$.**

**Public Key: (modulus: 77, encryption exponent: 7)**
**Private Key: (modulus: 77, decryption exponent: 43)**