Key Generation

1. Select two prime numbers: 23, 31
2. N = 23*31 = 713
3. Phi(N) = (23-1) *(31-1) = 660
4. e has to be in the range of {1…659} and e is coprime with 713 and 660

   713 = 23 * 31
   660 can be divided by 2,3,5…

   So, 713 and 660 both have no common factors with the value 91

   E = 91

5. d = (k*Phi(N)-1)/e
   [k can be any integer value for which the answer of d is also an integer]
   = (4*660-1)/91 = 29

23*31 = 713

Phi (713) = Phi(23) * Phi(31)
= (23 -1) * (31 -1)
= 660

Coprime: does not share any common factors.

14 is coprime with 15 and 23

Phi function refers to how many integers are less than or equal to N that do not share any common factors with N.

7 = 7 * 1

7 can be divided by 7

How many integers are less than or equal to 7? => 7

So, Phi(7) = 6

For every prime number, the phi function will be (Prime number - 1)

Public Key {3,3127}
Private Key {2011 ,3127}

m^e (mod N) = C

We have to encrypt the message "Hi"

Hi = 89

89^3(mod 3127) = 1394

Where m = 89, e = 3, N = 3127

c^d (mod N) = m

1394^2011(mod 3127) = 89

So, using the value of the private key, d; Alice can easily decrypt the ciphertext