RSA Cryptography uses the principle of using Private key and Public key to encrypt and decrypt. Here are the following rules –

1) Producer and Consumer will each have a pair of public and private keys.
2) A unique Private key is available with both Producer and Consumer and will not be shared with each other or with anybody else.
3) A unique Public key is available with both Producer and Consumer and will be shared with everybody
4) A message encryptes using one's private key can only be decryptes using their public key.
5) A message encryptes using one's public key can only be decryptes using their private key.

Mathematical calculations required for generating Public and Private keys.

1) A pair of prime numbers – "**p**" and "**q**"
2) Product of the two prime numbers (p and q) = "**N**"
3) "**Φ(N)**" = (p-1)(q-1)
4) "**e**" such that, e is co-prime of N
    a. e is a positive integer
    b. $1 < e < \Phi(N)$
    c. e is not a factor of N
5) "**d**" such that,
    a. $[1+ k (\Phi(N))] / e$
    b. Where $0 < k < e$
    c. $[1+ k (\Phi(N))] \bmod e = 0$

NOTE – My personal secret recipe for finding e – "e is the largest prime number greater than –

1) **Φ(N) / 2 if Φ(N) = even number**
2) **Φ(N) / 3 if Φ(N) = odd number"**

Private key = **(e, N)**
Public key = **(d, N)**

Mathematucal calculations for encryption and decryption

1) Encode the message – convert string to numbers – "**M**"
2) Encrypted message "**A**" = (M^e) mod N (using public key)
3) Decrypted message **M** = (A^d) mod N (using private key)
4) Decode the message – converting numbers to string