The public Key encryption algorithm is also called the Asymmetric algorithm. Asymmetric algorithms are those algorithms in which sender and receiver use different keys for encryption and decryption. Each sender is assigned a pair of keys:**Public key & Private key**

The **Public key** is used for encryption, and the **Private Key** is used for decryption. Decryption cannot be done using a public key.

RSA is the most common public-key algorithm, named after its inventors **Rivest, Shamir, and Adelman (RSA).** RSA encryption algorithm is a type of public-key encryption algorithm.

**RSA algorithm uses the following procedure to generate public and private keys:**

* Select two large prime numbers, p and **q**.
* Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.
* Choose a number **e** less than **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n),  
  **gcd (e,d(n)) =1**
* If **n = p x q,** then the public key is <e, n>. A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C. **C = me mod n**Here**, m** must be less than **n**. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
* To determine the private key, we use the following formula to calculate the d such that:  
  **De mod {(p - 1) x (q - 1)} = 1  
  Or De mod φ (n) = 1**
* The private key is <d, n>. A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.  
  **m = cd mod n**