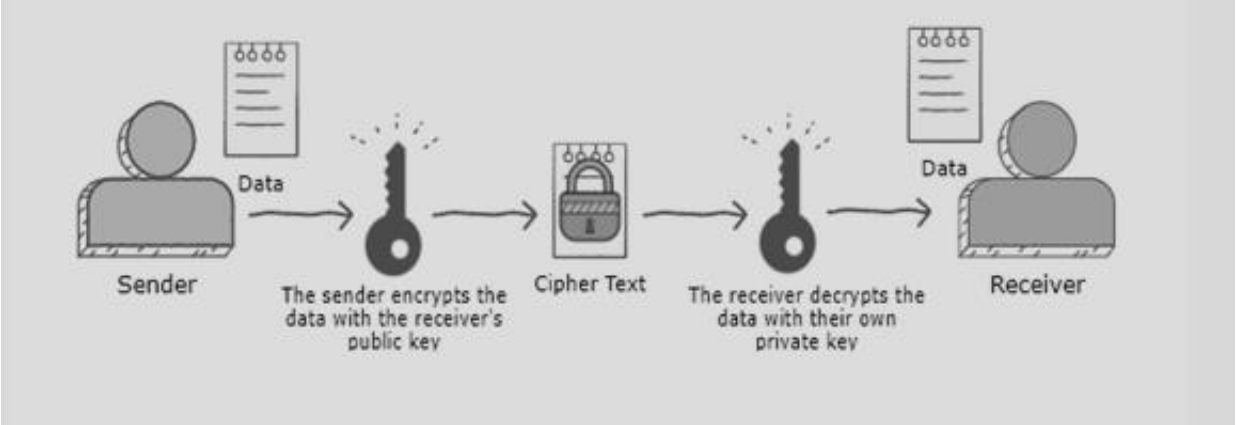
What is the RSA algorithm?

- The **RSA algorithm** is an asymmetric cryptography algorithm this means that it uses a *public* key and a *private* key (i.e two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

- The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.

- The following illustration highlights how asymmetric cryptography works:



Note:

Public key: known to all user in network

Private key : kept secret

- **If public key of user A is used for encryption we have to use the private key of same user for decryption.**

- **The RSA scheme is a block cipher in which the plaintext and cipher text are integer between o and n-1 for some value n.**

An example of asymmetric cryptography :

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client's public key and sends the encrypted data.
3. Client receives this data and decrypts it.

Note:

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.