**RSA (Rivest-Shamir-Adleman) Algorithm**

Overview:

RSA Algorithm is an asymmetric cryptographic algorithm. The meaning of Asymmetric is that it works on two different keys.

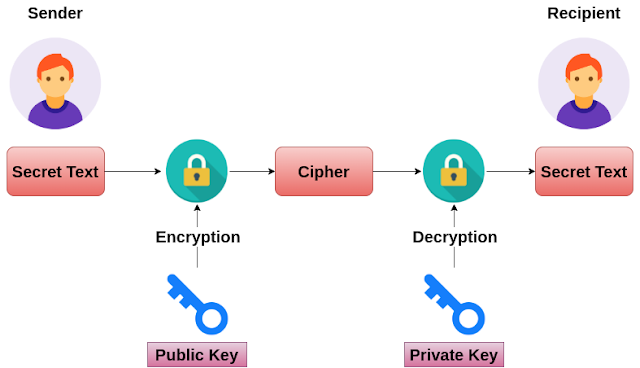
1. Public Key
2. Private Key

The public key is given to everyone, but the private key is kept private. A client sends its public key to the server and requests some data then the server encrypts the data using client’s public key and sends the encrypted data. RSA algorithm is considered secure and is widely used for secure data transmission. The idea of RSA is based on the fact that it is difficult to factorize a large integer The public key consists of two numbers where one number is a multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So, if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken soon. But till now it seems to be an infeasible task.

Advantages:

1. RSA algorithm is considered to be very secure and is widely used for secure data transmission.
2. RSA algorithm is a public-key cryptographic algorithm , which means that it uses two different keys for encryption and decryption.
3. RSA algorithm is used for secure key exchanges which means two party can exchange a secret without actually sending the key over the network.
4. RSA Algorithm can be used for digital signatures which means the sender can sign a message using their private key and receiver can verify that using the sender’s public key.

Schematic Diagram:



Class Diagram :

Graphical user interface, text

Description automatically generated