RSA Algorithm

- RSA algorithm is an asymmetric encryption method used by modern computers to encrypt and decrypt the messages.
- It was presented in the year 1977.
- RSA stands for the three researchers Rivest, Shamir and Adleman.
- RSA is a public-key algorithm.

Principle

- It is extremely difficult to factor a product into its original primes

  Example : It is easy to find the product of two prime numbers 29 and 31 but it is not easy to find the prime factors of 899.

Algorithm

Input : (a) Two prime numbers: p & q

(b) Message M to encrypt

Output : (a) Possible values of d and e

(b) Encrypted Message

1. $n \leftarrow p*q$
2. $z \leftarrow (p-1)(q-1)$
3. find e co-prime to z
4. find d Ɔ de mod z = 1
5. Public Key $K_u \leftarrow (e,n)$
6. $C \leftarrow M^e \bmod n$
7. Private Key $K_r \leftarrow (d,n)$
8. $M \leftarrow C^d \bmod n$

Example

- p=3 and q=11
- 3 x 11 = 33. So n=33.
- (p-1) x (q-1) = 2x10 = 20
- z = 20
- Choose e such that it is less than Z and it is also a co-prime to Z. In this case e=7. It is co-prime to 20 and also less than that.
- Choose d such that (d*e) mod 20 = 1.

- Take d=3, it will be 3*7 i.e. 21. Also verify that 21 mod 20 = 1.

- **Public key Ku = (e,n) = (7, 33)**
- **Private key Kr = (d,n) = (3, 33)**

- **Encryption**

  Message m=24

  24^7 mod 33 = 18 *(Encrypted Message)*

- **Decryption**

  18^3 mod 33 = 24 *(Original Message)*

Applications of RSA

- Secure Data transmission