

Understanding RSA Algorithm

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name **RSA** algorithm.

Algorithm

The RSA algorithm holds the following features –

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

You will have to go through the following steps to work on RSA algorithm –

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q , and then calculating their product N , as shown –

$$N = p * q$$

Here, let N be the specified large number.

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than $(p-1)$ and $(q-1)$. The primary condition will be that there should be no common factor of $(p-1)$ and $(q-1)$ except 1

Step 3: Public key

The specified pair of numbers n and e forms the RSA public key and it is made public.

Step 4: Private Key

Private Key d is calculated from the numbers p , q and e . The mathematical relationship between the numbers is as follows –

$$ed = 1 \text{ mod } (p-1) (q-1)$$

The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is (n,e) . To encrypt the plain text message in the given scenario, use the following syntax –

$$C = P^e \bmod n$$

Decryption Formula

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver C has the private key d , the result modulus will be calculated as –

$$\text{Plaintext} = C^d \bmod n$$