RSA Algorithm in Cryptography

Difficulty Level : Medium • Last Updated : 05 Jan, 2021

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

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.

Since this is asymmetric, nobody else except browser can decrypt the data even if a

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 in the near future. But till now it seems to be an infeasible task.

Let us learn the mechanism behind RSA algorithm :

> Generating Public Key :

- Select two prime no's. Suppose **P 3 and Q = 59.**

- An integer.
- Not be a factor of n.
- **1 < e < Φ(n)** [Φ(n) is discussed below],
  Let us now consider it to be equal to 3.

- Our Public Key is made of n and e

>> Generating Private Key :

- We need to calculate Φ(n) :
  Such that **Φ(n) = (P-1)(Q-1)**
  so, Φ(n) = 3016

- Now calculate Private Key, **d** :
  d = (k*Φ(n) + 1) / e for some integer k
  For k = 2, value of d is 2011.

Now we are ready with our – Public Key (n = 3127 and e = 3) and Private Key(d = 2011)

Now we will encrypt **"HI"** :

- Convert letters to numbers : H = 8 and I = 9

- Thus **Encrypted Data c = 89^e mod n.**
  Thus our Encrypted Data comes out to be 1394

  Now we will decrypt **1394** :

- **Decrypted Data = c^d mod n.**
  Thus our Encrypted Data comes out to be 89
  8 = H and I = 9 i.e. "HI".

Below is C implementation of RSA algorithm for small values:

```
// Returns gcd of a and b
int gcd(int a, int h)
{
    int temp;
    while (1)
    {
        temp = a%h;
        if (temp == 0)
          return h;
        a = h;
        h = temp;
    }
}

// Code to demonstrate RSA algorithm
int main()
{
    // Two random prime numbers
    double p = 3;
    double q = 7;

    // First part of public key:
    double n = p*q;

    // Finding other part of public key.
    // e stands for encrypt
    double e = 2;
    double phi = (p-1)*(q-1);
    while (e < phi)
    {
        // e must be co-prime to phi and
        // smaller than phi.
        if (gcd(e, phi)==1)
            break;
        else
            e++;
    }

    // Private key (d stands for decrypt)
    // choosing d such that it satisfies
    // d*e = 1 + k * totient
    int k = 2;  // A constant value
```

```
    // Encryption c = (msg ^ e) % n
    double c = pow(msg, e);
    c = fmod(c, n);
    printf("\nEncrypted data = %lf", c);

    // Decryption m = (c ^ d) % n
    double m = pow(c, d);
    m = fmod(m, n);
    printf("\nOriginal Message Sent = %lf", m);

    return 0;
}
// This code is contributed by Akash Sharan.
```

Output :

```
Message data = 12.000000
Encrypted data = 3.000000
Original Message Sent = 12.000000
```

This article is contributed by **Mohit Gupta_OMG** 🙂. If you like GeeksforGeeks and would like to contribute, you can also write an article using contribute.geeksforgeeks.org or mail your article to contribute@geeksforgeeks.org. See your article appearing on the GeeksforGeeks main page and help other Geeks.

Please write comments if you find anything incorrect, or you want to share more information about the topic discussed above.

Like 69

Previous Next

RECOMMENDED ARTICLES

Page : 1 2 3

01 Classical Cryptography and Quantum Cryptography
29, Apr 19

02 Custom Building Cryptography Algorithms (Hybrid Cryptography)
06, Sep 18

03 How to solve RSA Algorithm Problems?
12, Nov 18

04 Difference between RSA algorithm and DSA
22, May 20

05 RSA Algorithm using Multiple Precision Arithmetic Library
19, Mar 18

06 How to generate Large Prime numbers for RSA Algorithm
26, Jun 20

07 One Time Password (OTP) algorithm in Cryptography
31, Jan 19

08 Shamir's Secret Sharing Algorithm | Cryptography
07, May 20

▲

Vote for difficulty

Current difficulty : Medium

Easy Normal Medium Hard Expert

Improved By : aniketbote

Article Tags : cryptography, number-theory, Computer Networks

Practice Tags : number-theory, cryptography, Computer Networks

Improve Article Report Issue

Writing code in comment? Please use ide.geeksforgeeks.org, generate link and share the link here.

Load Comments

GeeksforGeeks

5th Floor, A-118,
Sector-136, Noida, Uttar Pradesh - 201305

feedback@geeksforgeeks.org