RSA Algorithm and Importance of Prime Numbers in RSA Cryptography

Sukhwinder Singh

Department of Mathematics, SGGS Khalsa College, Mahilpur, India.

Abstract. This paper aims to explain the Rivest, Shamir and Adleman algorithm invented in 1977 used for asymmetric cryptography. In an asymmetric key encryption scheme, anyone can encrypt messages using the public key, but only the holder of the private key can decrypt the message. Security depends upon the secrecy of the private key. Importance of prime numbers in RSA cryptographic system is also explained in this paper.

Keywords: algorithm, cryptography, decrypt, encrypt, key.

Introduction

RSA algorithm is a public key encryption technique and it was invented by Ron Rivest, Adi Shamir and Leonard Adleman in the year 1977. It is an example of asymmetric cryptography. This scheme is useful when two persons who have never met each other want to communicate securely. In this method, one person publish his public key for the world to see. Anybody can encrypt a message using a public key but cannot decrypt it. So when anybody wants to contact that person, his published public key can be used to encrypt the message and sending the data to him. Then, he will use his secret private key to decrypt the message. The idea of RSA is based on the fact that it is difficult to factorize a large number which is the product of two prime numbers. RSA is used in various fields such as e-banking, e-communication and e-commerce etc. RSA is also used in Bluetooth communication.

Main Result

RSA algorithm is based upon the following result:

Let p and q be two different prime numbers and n= pq. Let e be a positive integer such that e and $\phi(n)$ are relatively prime and d be a positive integer such that $de \equiv 1 \pmod{\phi(n)}$. If $M < n$ is any natural number such that $C \equiv M^e \pmod{n}$, then $M \equiv C^d \pmod{n}$.

In this method, a client sends its public key to the server and requests for some data. The server encrypts the data using client's public key and sends the encrypted data. Client receives this data and decrypts it. Since this is asymmetric, nobody else except client can decrypt the data even if a third party has public key of client.

This method begins with the selection of two huge prime numbers p and q (p is not equal to q) where p and q must be 100 or 200 digits long. These two prime numbers help in the formation of public key and private

key. So, these must be kept private. Then, their product n is calculated so that n=pq. The next step is to calculate the Euler's totient function of n

$\phi(n)= \phi(pq)= \phi(p)\phi(q)= (p-1)(q-1)$

Then, a number e is chosen such that $1 < e < \phi(n)$ and $\gcd(e,\phi(n)) = 1$.

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

Private key d is calculated from the numbers e, p and q using the relation $ed \equiv 1 \pmod{(p-1)(q-1)}$

i.e. $ed \equiv 1 \pmod{\phi(n)}$

Suppose a sender wants to send a message say M (in the form of numbers) to the receiver whose public key is (n, e). He use the following syntax to encrypt the message

$$C \equiv M^e \pmod{n}$$

Where C is the message which is sent to receiver. Now, the receiver wants to decrypt the message sent to him. He can use the formula

$$M \equiv C^d \pmod{n}$$

Where d is his private key.

This method can be illustrated with the help of following example:

Suppose a person B wants to send a message to person A. Following steps must be followed for the encryption and decryption of message.

1. A selects two prime numbers p and q. Suppose p=31 and q=41. We are choosing small prime numbers just for better understanding and simplification. In actual practice, the prime numbers to be selected must be reasonably large.

2. Person A calculates n and $\phi(n)$

$n=pq=31\times41=1271$ and $\phi(n)=\phi(pq)=\phi(p)\phi(q)=(p-1)(q-1)=(31-1)(41-1)=30\times40=1200$

3. Person A chooses a number e greater than 1 and less than $\phi(n)$. Also e must be relatively prime to $\phi(n)$. Suppose e=7.

(1271, 7) is the public key which person A tells to Person B and to the rest of the world if he wishes.

4. Suppose B wants to convey a message 'HI' to A.

Then M=89 (8 for H and 9 for I)

B calculates the value of C where $C \equiv M^e \pmod{n}$

$C \equiv 89^7 \pmod{1271}$

C=263

263 is the encrypted message that B sends to A.

5. A wants to decode 263. In order to do so, he must calculate his private key d using the formula ed ≡ 1(mod (p-1)(q-1))

7d ≡ 1(mod 1200)

d = $\frac{1200\times k+1}{7}$ for some integer k where d must be a natural number.

Here for k=2 , d=343 is the private key of A.

In order to decrypt the message, A uses the formula M ≡ C^d (mod n)

i.e. M ≡ 263^{343} (mod 1271)

This can be calculated using binary expansion of 343 i.e. 343=1+2+4+16+64+256

$=2^0+2^1+2^2+2^4+2^6+2^8$

So, $263^{343} = 263^{1+2+4+16+64+256}$

$= 263^1\ 263^2\ 263^4\ 263^{16}\ 263^{64}\ 263^{256}$

$263^{343} \equiv 263^1\ 263^2\ 263^4\ 263^{16}\ 263^{64}\ 263^{256}$ (mod 1271)

M ≡ $263^1\ 263^2\ 263^4\ 263^{16}\ 263^{64}\ 263^{256}$ (mod 1271)

Now, 263^1 ≡ 263 (mod 1271)

263^2 ≡ 535 (mod 1271)

263^4 ≡ 250 (mod 1271)

263^8 ≡ 221 (mod 1271)

263^{16} ≡ 543(mod 1271)

263^{32} ≡ 1248 (mod 1271)

263^{64} ≡ 529 (mod 1271)

263^{128} ≡ 221 (mod 1271)

263^{256} ≡ 543 (mod 1271)

M ≡ 263×535×250×543×529×543 (mod 1271)

M = 89

Using this calculation, Person A can decode the message i.e. HI sent to him by person B.

Validity of the method

The validity of this method depends upon the security of private key. Two prime numbers p and q must be known only to person A and unknown to the rest of the world. If p and q are small, then, n can de factorized easily to get p and q and the private key will be compromised. So, p and q must be taken sufficiently large (at least having hundred digits each).

Also, Euler's totient function of n must not be known to anyone other than person A because if anybody knows n and ϕ(n), he can easily find p and q by the following method

$n = pq$

$\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$

$q = n - \phi(n) - p + 1$

This value of q when substituted in $n = pq$

We get, $n = p[n - \phi(n) - p + 1]$

$n = pn - p\,\phi(n) - p^2 + p$

$p^2 + (\phi(n) - n - 1)p + n = 0$

Which is quadratic equation in p and can be solved to get p.

It is clear that the validity of RSA algorithm is based upon the security of ϕ(n) even if n is known to the entire world. This is possible because Euler's totient function ϕ(n) is calculated using the factorization of n and it is nearly impossible to factorize a number which is the product of two large sized prime numbers. This explains the need of prime numbers in RSA cryptography.

Conclusion

Encryption and decryption are critical security measures that are designed to ensure that communication is processed securely. Using these techniques, information is transferred from one end to the other with proper security. RSA cryptographic system for encryption and decryption of messages and need of prime numbers in RSA cryptosystem is explained in this paper.

References

1. David M. Burton, 1989, Elementary Number Theory, the Second Edition, WCB.
2. Bruce Schneier, 1996, Applied Cryptography, Protocols, Algorithms and Source Code in C, the Second Edition, Wiley.
3. M. Thangavel, P. Varalakshmi, M. Murrali and K. Nithya, An Enhanced and Secured RSA Key Generation Scheme, Journal of Information Security and Applications, Volume 20, February 2015, Pages 3-10
4. Wikipedia. " RSA Cryptosystem."