ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, Dec 2022

APPLICATION OF MODULAR INVERSE IN RSA ALGORITHM

Shaima Mateen Thange
Assistant Professor, Department of Information Technology, SIES (Nerul) College of Arts, Science & Commerce.
shaimathange@sies.edu.in

ABSTRACT
Multiplicative inverse has a lot of applications in various fields. When we divide a number by another number, we get quotient and remainder. The modulo operation returns the remainder after division. a *mod n gives out the remainder when* a *is divided by n, where* a *is an integer and n is a positive integer. A modular multiplicative inverse of an integer* a *is an integer* b *such that the product* ab *is congruent to 1 modulo n, i.e.* $ab \equiv 1$ *(mod n). Numerous calculations of modulo multiplicative inverses are necessary for a variety of asymmetric cryptographic algorithms such as RSA algorithm.. This paper aims at explaining the concept of modulo inverse and its application in cryptography as well as the various methods for computing the modulus. And the role of modulo inverse in the security of encryption and decryption.*

Keywords: *Modular multiplicative inverse; Public-key cryptography; RSA algorithm.*

INTRODUCTION
Although number theory may not be the "purest" branch of mathematics, it has shown to be one of the most helpful in terms of computer security. The encryption and decryption processes are carried out using the same key in symmetric cryptography, such as that which was available before the 1970s. This calls for the use of a common decryption key amongst the parties involved in encrypting and decrypting the data. As a result, it has been discovered that encryption and decryption can be performed using two separate keys rather than one. The encryption key could be made public without jeopardising the decryption key's security, but the decryption key would still need to be kept a secret. This idea was referred to as public-key cryptography. RSA algorithm is one of those kind. It uses modular multiplicative inverse to find the private key using public key.

METHODOLOGY
The following are the most common methods to compute the inverse modulo n.

(i) Naive Method

This method is useful to find the inverse of a mod n, when $a <$ n and gcd(a, n)=1. We have to multiply a by the elements of the set {1, 2, … ,n -1} and the first of them which gives a product equal to 1 (modulo n) will be the inverse of a.

(ii) Euler's phi function

Euler's phi function ϕ(n) is the number of non-negative integers less than n that are relatively prime to n.

The well-known Fermat's little theorem states that $a^{\phi(n)} \equiv 1$ for a positive integer a such that $a <$ n and gcd(a, n)=1. Hence it gives an explicit formula to compute the modulo inverse.

$$a^{-1} = a^{\phi(n)-1}$$

The RSA Algorithm
The RSA public-key cryptosystem was developed at MIT in 1977 by Ronald Rivest, Adi Shamir, and Leonard Adleman and is based on the aforementioned observations. The value n, also known as the modulus in this cryptosystem, and the value e, also known as the public exponent, make up the public

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, Dec 2022

key. The value d, sometimes known as the private exponent, and the modulus n make up the private key. An RSA public-key / private-key pair can be generated by the following steps:

1. Generate a pair of large, random prime p and q.

2. Compute the modulus n by multiplying p and q.

3. Select an odd public exponent e between 3 and n−1 that is relatively prime to p−1 and q−1.

4. Compute the private exponent d from e, p and q.

5. (n, e) is called as the public key and (n, d) is called as the private key.

The encryption operation in the RSA cryptosystem is exponentiation to the ethpower modulo n:

c = ENCRYPT (m) = me mod n .

The message is the input m, and the ciphertext is the output c. In reality, the message m usually consists of a properly formed key that needs to be distributed. Using a conventional encryption technique and the shared key, the actual message is encrypted. With just one exponentiation, it is possible to encrypt a message of any length using this method.

The decryption operation is exponentiation to the dthpower modulo n:

m = DECRYPT (c) = cd mod n .

As encryption and decryption are inverse processes, the decryption procedure restores the original message m due to the relationship between the exponent e and d.

DISCUSSION

As n is the product of two distinct prime numbers p and q, and e is the public exponent as defined above. Let L = lcm (p−1, q−1) denote the least common multiple of p−1 and q−1. The private exponent d for the RSA cryptosystem is any integer solution to the congruence

$$de \equiv 1 \pmod{L}$$

The value d is the inverse of e modulo L. The requirement that e be relatively prime to p−1 and q−1 ensures that an inverse exists.

CONCLUSION

In this paper, we have discussed the modulo operation and described the most common methods for computing the inverse modulo n as well as the application of inverse modulo in RSA algorithm. The RSA cryptosystem works because exponentiation to the dthpower modulo n is the inverse of exponentiation to the ethpower when the exponents d and e are inverses modulo L. It is challenging to recover m from c without the private key (n, d) or the prime factors p and q. As a result, the fundamental condition for a public-key cryptosystem security can be met even if n and e are made public.

REFERENCES

1. Kaliski, B. (2006). The mathematics of the RSA public-key cryptosystem. RSA laboratories.

2. Bufalo, M.; Bufalo, D.; Orlando, G. A Note on the Computation of the Modular Inverse for Cryptography. Axioms 2021, 10, 116. https://doi.org/10.3390/ axioms10020116.

3. Goshwe, N. Y. (2013). Data encryption and decryption using RSA algorithm in a network environment. International Journal of Computer Science and Network Security (IJCSNS), 13(7), 9.

4. Introduction to Cryptography and Network Security by Behrouz A. Forouzan, McGraw-Hill.

5. Forouzan, B. A. (n.d.). Introduction to Cryptography and Network Security. McGraw-Hill.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, Dec 2022

6. Caldwell, C. (n.d.). prime numbers. Retrieved from ThePrime Pages:https:// primes .utm. edu/glossary/xpage/EulersPhi.html