**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**
**IMPACT FACTOR: 5.258**

***IJCSMC, Vol. 5, Issue. 4, April 2016, pg.380 – 383***

# Mathematical Review of RSA Algorithm

**Sumit Suri[1], Yashpal Singh[2]**

[1]Computer Science Department Ganga Institute of Technology and Management, India

[2]Computer Science Department Ganga Institute of Technology and Management, India

[1] sumitsuri292@gmail.com; [2] yashpalsingh009@gmail.com

***Abstract— with the growing usage of Computer Systems in modern e-commerce applications the need of Security has been increased to a greater extent. One of the area related to security systems is Cryptography [1], which deals with the Encoding the plain information to some encoded format so that it can only be read after decoding. Formally the process of Encoding and Decoding is referred to as Encryption and Decryption. Mathematics Number Theory is the backbone of the various Encryption and Decryption Techniques. Most of the encryption and decryption techniques have strong Mathematical Basis. This paper details the review of mathematical Foundation of the most commonly used Asymmetric Key Algorithm the RSA.***

***Keywords— RSA – Rivest-Shamir-Adleman, Prime Numbers, Symmetric Key, Asymmetric key, Encryption, Decryption***

## I. INTRODUCTION

Gone are the days when the Security was a 'should have' Feature in the Software systems. With the growing use of the software system in financial applications like e-commerce the need of secure transaction is a 'must have'. Cryptography is a technique which is used to encrypt the message into some non readable form so that it can be transferred securely over a medium without the fear of losing integrity. Cryptography make use of 'Keys' applied to a text or Image which convert the text /image into some non readable format. Application of the same or a different 'Key' to this non readable encoded form generates the original Form. This can be depicted graphically as in the fig-1 below in context of Text.

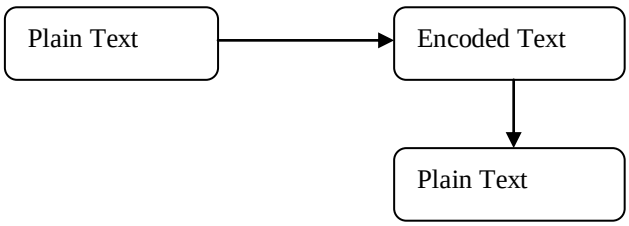


Fig. 1 Encryption and Decryption Process

 

The way the 'Key' is applied to the plain text broadly classifies the encryption/decryption into two categories Symmetric and Asymmetric Key Technique.

Symmetric Key Algorithms uses same key for the Encryption and Decryption. This is faster approach but suffers from major problem of 'Key Distribution' and 'Required Number of Keys'.

Asymmetric Key Algorithms on the other hand make use of different key for Encryption and Decryption. The key used for encryption is publically known to everybody but the decryption key is only known to the legitimate receiver who is able to decrypt the message successfully. This technique allows less number of keys required to establish number of connections. Also the process of Key Distribution is not a problem with this approach. RSA [2] Algorithm is one of the very frequently used asymmetric key algorithms.

## II. DESCRIPTION OF RSA ALGORITHM

Various attempts made to solve the problems of symmetric key cryptography lead to the development of one of the most practical asymmetric key algorithm known as RSA algorithm. The RSA [2] is named after the initials of three scientists Ron Rivest, Adi Shamir and Len Adleman. The algorithm was based on the framework developed by Diffie and Hellman [3]. This section provides a detailed step wise description of how the two keys are generated – Public and Private keys – and using them the task of encryption and decryption is performed.

Prime Numbers [6] – are the basis of RSA algorithm. A prime number may be defined as a number which is divisible by one and by itself. For example 5 is a prime number. The smallest Prime number is 2.

Steps to Generate the Keys are explained as:

1. At first step two very large random prime numbers are selected. We call them P1 and P2.
2. The product of these two prime numbers is calculated. We will call the product as M.

$$M = P1 * P2$$

3. The Public Key – the key used to encrypt is then calculated as the number such that it is not a factor of the product (P1 -1) AND (Q-1). We will call this key as E (encryption Key).
4. The Private Key – the key used to decrypt is chosen such that is satisfies the following relation.

   $D * E \bmod (P1-1) * (P2 -1) = 1$

Here D is the Private Key – or decryption key.

Once the keys are available they can used in the following way to do the encryption and decryption.

*Encryption Step*:

Consider the Plain Text – P to convert this to encrypted text or cipher text following formula is applied.

$$C = P^E \bmod M$$

*Decryption Step*:

Consider the Cipher Text – C to convert it back to Plain Text the following formula is applied.

$$P = C^D \bmod M$$

## III. ILLUSTRATION WITH AN EXAMPLE

In this section we will illustrate the various steps using a simple example [4].Consider the two prime numbers:

$$P1 = 47 \text{ and } P2 = 17$$

$$M = P1*P2 = 119$$

After applying bit of Mathematics we can see that E = 5 or any other number as well.

$$D * 5 \bmod 98 = 1$$

After bit of mathematics we can see that D=77 will hold the above equation.

Given the Plain Text – 12

Encryption is applied to the given text resulting in the encrypted text as follows:

$$12^5 \bmod 119 = 3$$

At the receiver end the decryption is applied on the cipher text as

$$3^{77} \bmod 119 = 12$$

 

The value 12 is decoded using the decryption key.

Here we have taken a simplified example where the numeric equivalent number of text is considered as 10. The same can be applied to a large textual message by taking the ASCII value of each character and applying the encryption and decryption on that value.

## IV. MATHEMATICAL THEORY OF ALGORITHM

The RSA Algorithm is dependent on following truths and observation in the Mathematical Number Theory [5].

### *A. Prime Numbers can be generated easily*

We can generate the Prime numbers of given length in relatively easier manner. For example this can be done by generating large numbers and checking whether it is a prime or not.
From implementation perspective JAVA provides inbuilt functions to generate the numbers fairly easily, for example BigInteger.probablePrime [7].

It may be noted here that to check the Prime property of number we could find the factors of that particular number but this approach is not easy but a much time consuming one. Rather there are additional properties of Prime Numbers which are exploited to find whether a number is Prime or Not.

It is recommended to use very large prime numbers for the purpose of RSA Algorithm e.g. more than 150 digits.

### *B. The multiplication is a very easy operation*

Most of the available Computation Systems today can complete the multiplication in relatively short time – if we refer the time complexity of multiplication operations it is generally assumed to be of 'Constant Time'.

### *C. Factoring Operation is a Hard Operation*

If we are given a large number it is not a trivial operation to recover two prime factors of the number. This is topic of research in current mathematics to find quicker ways to be able to do the factoring but this has not been established whether a quick method can be devised. Also this has also not established whether a quick method can never be devised so we may have a quicker method in future. Mathematically on a modern computer it will take years to crack a number sized 1024 bits. This is the major reason for the effectiveness of the RSA Algorithm.

### *D. Mod and Exponentiation is easy*

The mod with exponentiation is easy operation for example given C, P, E and M it is easier to compute

$$C = P^E \bmod M$$

This operation is called as Modular Exponentiation.

### *E. The reverse operation of Modular Exponentiation i.e. Modular Root Extraction is easy given the Prime Factors.*

### *F. The Modular Root Extraction is hard if we are not having the Prime Factors.*

## V. SECURITY OF RSA ALGORITHM

RSA algorithm is considered very much secure as the computation requirement to obtain the Decryption key is a hard problem. Though it is one of the strongest algorithms but still there can be attacks. In real life no encryption technique may be regarded as a fool proof and able to withstand each and every attack. Brute Force techniques may sometimes able to break a code.

RSA algorithm's security is due to the hard nature of the Prime Factoring operation. It has been observed that despite of many attempts to find a quicker way to have factors. So the problem of cracking the RSA can be visualized as hard as factoring a large number n. It must be mentioned here that finding factor to be hard is not proven as yet – but also no method has been devised as yet for the same.

## VI. ADVANTAGES

1. The primary advantages of using RSA or any other asymmetric key scheme is to avoid the problem of key distribution. The encryption can be done by any party using the known public key. The decryption key or the Private Key is the secret key which is required to be known only to the receiver party. This is a

 

major problem with the symmetric key approaches e.g. AES as same key is required to be used and both the parties should be aware of the key. This creates the problem on how to exchange the key.

2. Another advantage is that that the number of keys required is smaller. For instance only with one pair of keys a receiver can get encrypted messages from any number of senders. Whereas in symmetric scheme the keys required is of the order of 2n.
3. Digital Signature [8] is one other application where this algorithm can be applied. In digital signature scheme the encryption is done using sender's Private Key. And can be decrypted using the sender's Public Key. This way the message can be decoded by anyone – but this does ensures that message is authenticated to have come from the legitimate sender. Hence the digital signature scheme does not achieve the confidentiality but the authentication. Another aspect of security is non-repudiation which is also achieved using the digital signature scheme. Digital Signature scheme is gaining the same status as the paper signature now days and is even being applied to financial transactions.

## VII. LIMITATIONS

One of the major limitations of the asymmetric key approach is the speed of operation. It is observed fact that symmetric key algorithms are inherently faster than the asymmetric ones. To overcome this limitation usually the combination of both these schemes is implemented. The approach is termed as Digital Envelop.

In addition using RSA Algorithm some common pointers must be taken care of so that it is not vulnerable to attacks.

a. If we choose small prime numbers then the factoring of their product will become easier for a computer making the algorithm vulnerable to attacks. So it is recommended to use large prime numbers.
b. It is also recommended to use the prime numbers which are not very close to each other. The definition of 'being close' is relatively vague as no set rule is there to establish what difference can be considered as close

## VIII. THE FUTURE

Though the RSA algorithm is proven and not breakable as yet but in context of cryptography if something has never been broken as yet does not guarantee that it will never be broken. The security of RSA is dependent on one observation that Factoring is time intensive operation. If in future someone is able to devise a efficient algorithm for factoring the RSA breaking might become trivial. With the advancement of heuristic search techniques and alternate problem solving techniques this might be feasible so attempts should be made to make the scheme more secure. This is also the area of research to find alternative techniques to RSA.

## ACKNOWLEDGEMENT

We wish to acknowledge Dr. Yashpal Singh and other staff members for Computer Science Department of Ganga Institute of Technology and Management for providing guidance from time to time on the subject.

## REFERENCES

[1] Articles Available [Online]: https://en.wikipedia.org/wiki/Cryptography.
[2] Articles Available [Online]: https://en.wikipedia.org/wiki/RSA_%28cryptosystem%29.
[3] Articles Available [Online]: http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange
[4] Atul Kahate, Cryptography and Network Security, 3rd ed., Mc Graw Hill Education.
[5] Articles Available [Online]: https://nrich.maths.org/4352.
[6] Pages Available [Online]: http://empslocal.ex.ac.uk/people/staff/mrwatkin/zeta/tutorial.htm.
[7] Oracle Docs Available [Online]:https://docs.oracle.com/javase/7/docs/api/java/math/BigInteger.html
[8] Pages Available [Online]: http://www.icg.isy.liu.se/courses/tsit03/forelasningar/cryptolecture08.pdf

 