Research Journal of Computer and Information Technology Sciences ______________________ISSN 2320 – 6527
Vol. **8(1),** 9-12, June **(2020)** *Res. J. Computer and IT Sci.*

Short Communication

Development of "RSA" Encryption Algorithm for Secure Data Transmission

Abhishek Guru*[1] and Asha Ambhaikar[2]
[1]Department of Computer Science Kalinga University Naya Raipur, India
[2]Kalinga University Naya Raipur, India
abhishekguru0703@gmail.com

Available online at: www.isca.in
Received 27th November 2019, revised 13th May 2020, accepted 10th June 2020

Abstract

Data transmission using insecure network need to be secure by using various methods. There are various cryptographic techniques are available to ensure data transmission very secure. In this paper we will try to increase the data security by modifying the RSA encryption algorithm using a pair of even numbers in the combination of private key and public key by using this the factorization and complexity of variables are increased. This new technique helps to provide max data security over the network. Our proposed scheme where we use even numbers in RSA encryption algorithm provides more efficiency and reliability and also increases the level of data security over the network.

Keywords: RSA algorithm, even number, complexity, public and private key.

Introduction

In traditional communication systems, securing the tract meant securing the information. With the arrival of network and development in packet switching techniques, securing the tract are neither probabilistic nor effective. This increases the ponderability of Cryptography. The cryptography involves creating written or generated codes that allow information to be kept secure. In a cryptography the information is converted into unreadable format which is called ciphertext or cyphertext which is cannot be understand by unauthorized user only a person who having a key can able to decode the information into original format which is called plaintext.[1] RSA encryption algorithm is public-key cryptography and is considered as one of the great handsel in the field of public key cryptography. It is suitable for both decryption and encryption. The RSA is more secure from multiple attacks, But the fault of the RSA are low speed, request for key deposit, and unsuited for global system.[2] The RSA algorithm was developed by Rivest, Adi Shamir and Leonard in 1978[3].

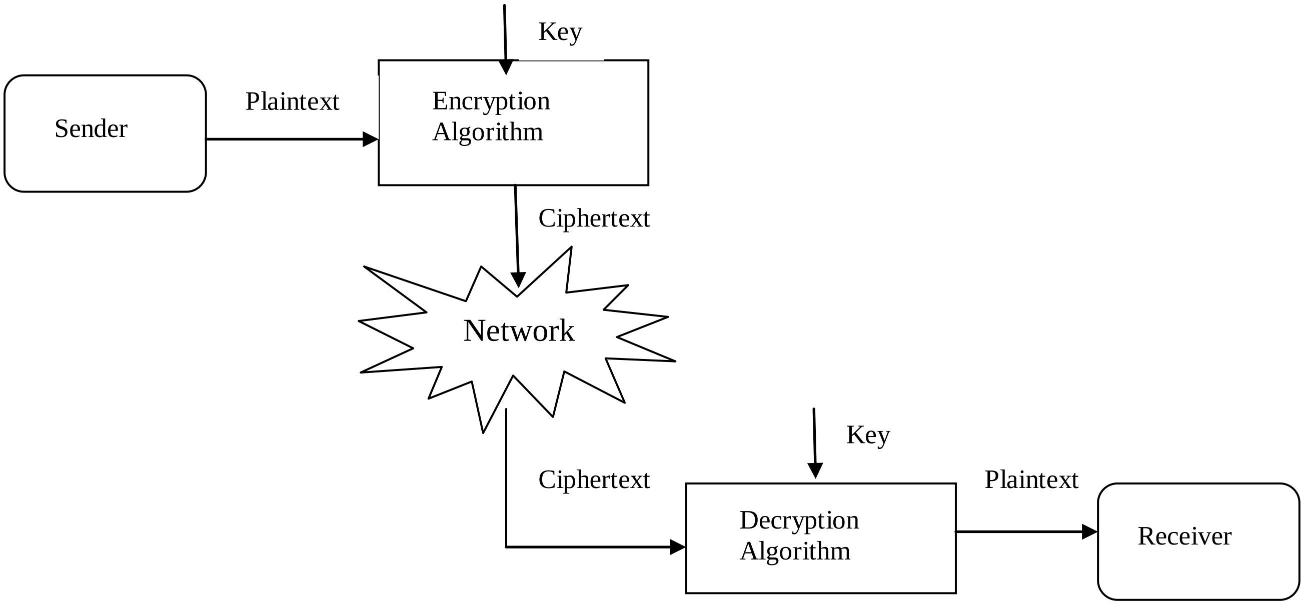

Figure-1: Cryptography.

Purpose of Cryptography

The main purpose of cryptography is to secure data or information from cyber crimes. Cryptography has numbers of security features that's why is it is widely used today. Following are some goals of cryptography[4]. i. Authentication: This is a process of proving identity. In this we verify the message security. Authentication is of two types Peer entity authentication and Data origin authentication. ii. Privacy: Privacy means protection against unauthorized manifestation of information. It may be applied to whole message. Privacy provides the conservancy of transmitted data from dormant attacks. iii. Integrity: It assures the receiver that the received original message which has not been exchanged. iv. Non-repudiation: Sender or receiver cannot deny for a transmitted message. When a message is sent, the receiver can verify that the sender in fact sent the message.

Basic Terminology of Cryptography[5]

Plaintext: The original information which is used into the algorithm as input.

Encryption algorithm: Process where we change plaintext into cipher text.

Cipher text: Cipher text is the encrypted form the message depends on the key and plaintext.

Decryption algorithm: The process in which we change Cipher text into plain text is known as decryption.

Key: It also plays as input to the encryption algorithm.

Classification of Cryptography: Cryptography can be classified into two key encryption groups - Symmetric and Asymmetric key encryption.

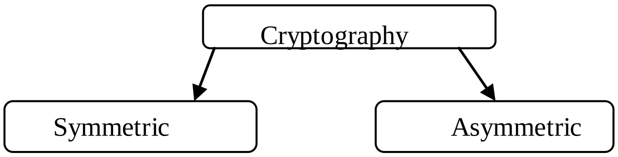

Figure-2: Classification of Cryptography

Symmetric Cryptography: In the symmetric key encryption user uses the same key to encrypt and decrypt the data or information. Symmetric key cryptography is faster than the asymmetric key cryptography. It is used to provide confidentiality of the messages. The following symmetric algorithms such as DES, 3DES, Blow Fish, IDEA, TEA, CAST 5, AES, RC6, Serpent, Two Fish and MARS are described in details according to their overview of architecture and security.[6]

Asymmetric Cryptography: A key can be divided into two parts in asymmetric cryptography, a public key and a private key. The public key is open to everyone and the private key must be kept secret. There are two main use cases of asymmetric cryptography secrecy and authentication.

RSA: RSA is an asymmetric cryptographic which is based on prime numbers. This algorithm works on a public and private key system, the public key is available to everyone to encrypt the information and the person who have private key can able to decrypt the original information.

Methodology

In this paper we modify the RSA algorithm which is based on even numbers. This algorithm is helps to get the max data security over the network by increasing the factorization of the variables. In this paper we will use JAVA IDE to get the Public Key and Private Key.

RSA algorithm: Here is the main RSA algorithm technique; In this first we take two different prime numbers p and q, then

Calculate: $n=p*q$
Calculate f(n) : $f(n)=(q-1)(p-1)$
Select 'e' such that: $1<e<f(n)$ and GCD (e, f(n))=1
After that Determine 'd'
e mod (f(n)) $(e * d) \bmod f(n) = 1$
'd' is the private key

For Encryption: Use following: $C=m^e \bmod n$
Now for Decryption: To decrypt the message: $M= c^d \bmod n$.
Where c= cipher text, n= p*q and d is the private key.

The above is a normal RSA algorithm which is used widely for encrypt and decrypt the data or information. In which we use two prime numbers.

Now below is an example where we use even numbers to encrypt the information. In this example first we select two even numbers, than calculate the value of 'n' by multiplying those variables which is n= (p*q), after that we calculate function of 'n'by subtracting those variable by 1(one) and multiply which is f(n)= (p-1)*(q-1).

Than we select 'e' which we will use to get the ciphertext but the 'e' must be a number which is 1<e<f(n), After that we get public key=(n,e), than we calculate the 'd' which is use for private key so the 'd' multiplicative of e(mod f(n)), now we have private key=(n,d). After getting both keys (public and private key) we have to put a massage in a formula to get the ciphertext which is: $C=M^e \bmod n$.

Here C= ciphertext, M=message or data. After calculating we get our ciphertext which is sent to network. To decrypt the ciphertext into original message we have: $M=C^d \bmod n$

Here M= message or data, C=ciphertext. After calculating this we get the original message which is sent by the first user but here we are using even number so there is some changes in the formula to get the original message i.e.

$M = \sqrt{C^d} \bmod n$

This process can be understood by an example which is given below:

Example: Below is RSA algorithm where we use two even numbers
First we select two even numbers and calculate n=p*q
Which is: n=10*12, n=120

After calculating n we calculate the function of 'n' f(n)=(p-1)(q-1)
i.e. f(120) = (10-1) (12-1)=99 f (n)=99

Now we select a number for 'e' which must be 1<e<99
f(n) cannot be divisible by e Let e=2

Select d, e(mod f(n)) which is d= 50 ,Now we have public key (n = 120,e = 2) Private key is (n = 120,d = 50)

In the side of A; if given message m = 5
Then Encryption of the given message can be performed like: $C= 5^2 \bmod 120 = C = 25$ here 'C' represents cipher text which is sent by A to B.

Now In the side of B the decryption process can be done like:
$M = 25^{50} \bmod 120 = 25$
So here we got the plain text M=25 which is not original message sent by A
So here we apply the modified formula to calculate the message value i.e.
$M = \sqrt{C^d} \bmod n$, $M=\sqrt{5^{50}} \bmod 120$

After calculation we got plain text M=5 which is original message sent by the A to B

Conclusion

Cryptography plays very important role in the field of data security. The RSA encryption algorithm is very good encryption algorithm there may some disadvantages on it but many researchers try to reduce the drawbacks of RSA encryption algorithm .In this paper we use even numbers in the place of prime numbers in RSA encryption algorithm where we saw that the even number increases the data security by increasing the factorization of even numbers to achieve the original message and there may be some changes in the formula i.e. $M = \sqrt{C^d} \bmod n$. The complexity of the calculation of M by using the modified formula provides more security and also secure our data over the network.

References

1. Joseph Amalraj and J. John Raybin Jose (2016). A Survey Paper on Cryptography Techniques. *International Journal of Computer Science and Mobile Computing*, 5(8), 55-59.
2. Rejani R. and Deepu. V. Krishnan (2015). Study of Symmetric Key Cryptography Algorithms. *International Journal of Computer Techniques*, 2(2).
3. Rivest Adi Shamir and Leonard (1978). The RSA Algorithm https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf , access on 11 Nov 2019.
4. Ivy, B. P. U., Mandiwa, P., & Kumar, M. (2012). A modified RSA cryptosystem based on 'n' prime numbers. *International Journal of Engineering and Computer Science*, 1(2), 63-66.
5. Sarita Kumari (2017). A research paper on Cryptography Encryption and Compression Techniques. *International Journal of Engineering and Computer Science*, 6(4), 20915-20919.
6. Abood, O. G., & Guirguis, S. K. (2018). A survey on cryptography algorithms. *International Journal of Scientific and Research Publications*, 8(7), 410-415.
7. B, Padmavathi and S. Ranjita Kumari, (2013). A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique. *International Journal of Science and Research*, 2(4).
8. Gurpreet Singh Supriya (2013). A Study of Encryption Algorithms (RSA,DES,3DES and AES) for Information Security. *International Journal of Computer Application*, 67(19).
9. Venkat Prasad K. and S. Magesh (2017). A Survey on Encryption Algorithms Using Modern Technique. *International Journal of Pure and Applied Mathematics*, 117(16).
10. Vanjara P. A. (2012). Analysis and design of cryptography algorithms. *International Journal of Computer Applications & Information Technology*, 1(2), 12-15.
11. Nitin jirwan, Ajay Singh and Sandip Vijay (2013). Review and Analysis of Cryptography Technique. *International Journal of Scientific & Engineering Research*, 4(3).
12. Manisha Vishwakarma (2013). Comparative study of Cryptography Algorithms. *International Journal of Advanced Research in Computer Science*. 4(3).
13. Suguna, S., Dhanakoti, V., & Manjupriya, R. (2016). A Study on Symmetric and Asymmetric Key Encryption Algorithms. *International Research Journal of Engineering and Technology (IRJET)*, 4(3), 2395-0056.
14. Shivani Sharma and Yash Gupta (2017). Study on Cryptography and Techniques. *International Journal of Scientific Research in Computer Science*, 2(1).
15. Maqsood, F., Ahmed, M., Ali, M. M., & Shah, M. A. (2017). Cryptography: A comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications*, 8(6), 442-448.
16. Swapnil Chaudhari, Mangesh Pahade, Sahil Bhat, Chetan Jadhav & Tejaswini Sawant (2018). New Hybrid Cryptography Algorithm. *International Journal for Research & Development in Technology*, 9(5).

17. Arpit Agrawal and Gunjan Patankar (2016). Design of Hybrid Cryptography Algorithm for Secure Communication. *International Research Journal of Engineering and Technology*, 3(1).

18. S. Pavithra and E. Ramadevi (2012). Study and Performance Analysis of Cryptography Algorithms. *International Journal of Advanced Research in Computer Engineering and Technology*, 1(5).

19. Hardik Gohel (2015). Design and Development of Combined Algorithm Computing Technology to Enhance Web Security. *International Journal of Innovation and Emerging Research in Engineering*, 2(0).

20. Sarthak R Patel, Khushbu Shah and Gaurav R Patel (2014). Study on Improvements in RSA Algorithm. *International Journal of Engineering Development and Research*, 1(3).