ISSN: 2455 - 9172

EIJO Journal of Engineering, Technology And Innovative Research (EIJO–JETIR)

Einstein International Journal Organization (EIJO)

Available Online at: www.eijo.in

Volume – 4, Issue – 2, March – April -2019 , Page No. : 12 - 18

Enhancement of Asymmetric RSA Algorithm for Cryptographic System

[1]Dr. Himanshu Arora, Department of CSE, Arya College of Engineering & Research Centre, Jaipur, Rajasthan, India

[2]Shilpi Mishra, Department of CSE, Arya College of Engineering & Research Centre, Jaipur, Rajasthan, India

[3]Smita Sankhla, Department of CSE, Arya College of Engineering & Research Centre, Jaipur, Rajasthan, India

[4]Pradeep Jha, Department of CSE, Arya College of Engineering & Research Centre, Jaipur, Rajasthan, India

Abstract

A cryptosystem is a pair of algorithms that accept a key and convert the plaintext into encrypted text and vice versa. In this process two types of algorithms are used symmetric and asymmetric algorithm. In the symmetric algorithm both the sender and receiver key are same but in the asymmetric algorithm the sender and receiver key are different that makes this type of algorithms more secure. In the asymmetric algorithm RSA is the one of the most popular algorithm. In this paper present the enhancement of Asymmetric RSA algorithm which is used in the cryptographic System. The security of the RSA system is based on the premise that many decomposing factors are difficult. In RSA, if we can factor the module (n) in its prime numbers, we can also get the private key. So in this paper a customized RSA algorithm is offered called Dual Modulus Digital Logarithmic Algorithm (DMDLA). The DMDLA algorithm uses dual module digital logarithmic encryption and decryption, so it is safer than the RSA algorithm.

Keywords: RSA Algorithm, DMDLA Algorithm, Encryption, Decryption, Cryptography.

Introduction

The communication over internet is not secure for sending and receiving confidential information. To keep the information safe and secure, users would like to have a secure private connection link/connection protocol with the other party. Cryptography is the technique used for protecting the information from any third parties. It provides the way in which data can be encoded to prevent third party usage there by keeping the information safe. Thus only intended receiver can identify the real message [2]. Public key cryptography relies on the use of a public key and a private key. The public key is normally and freely distributed without compromising the private key, which is to be normally kept secret by its owner. The public key is used to encrypt plaintext messages and to verify signatures; the private key is used to sign messages and to decrypt the cipher texts to obtain the plaintext messages [1]. Since digital imaging plays an important role in multimedia technology, maintaining user privacy becomes even more important. To ensure such security and privacy for the user, it is very important to encrypt the image to protect against unauthorized access. Encryption of images and video is used in various fields, including Internet communications, multimedia systems, medical imaging, telemedicine and military communications. Color images are transmitted and stored in large quantities via the Internet and wireless networks that use the rapid development of multimedia and network technologies. Cryptography has played an important role in security, and this is the battlefield for mathematicians and scientists from Shannon since 1949. Several cryptographic algorithms are now offered as AES, DES, RSA, IDEA, etc [3].

Modern cryptography can be classified broadly into two types:-

A. Symmetric key cryptography

In the form of encryption, there is only one key and the private key is used to encrypt and decrypt data between the sender and receiver.

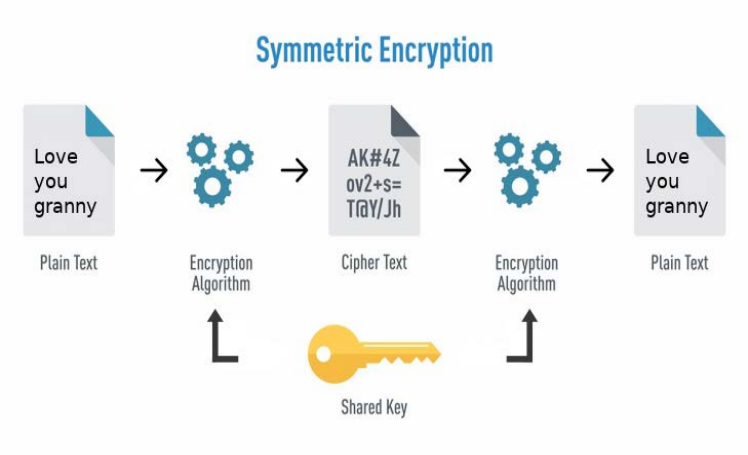

Figure 1 : Symmetric Key Cryptography

B. Asymmetric key cryptography

In this type of encryption, there are two types of keys: the public key and the private key. Both are used in encryption and decryption. The public key is available to everyone.

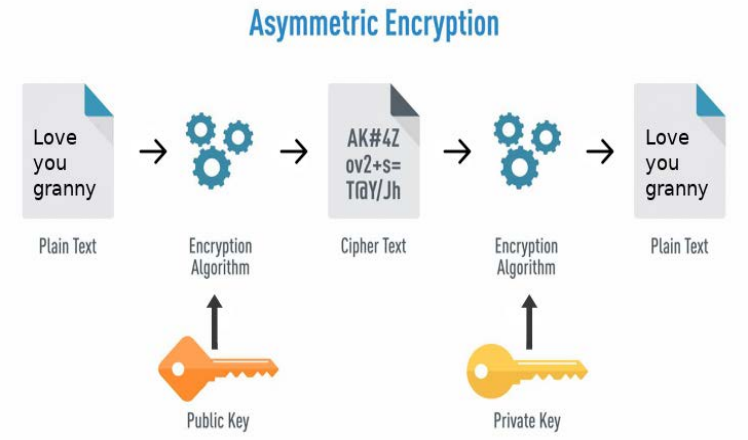

Figure 2: Asymmetric Key Cryptography

RSA Algorithm

Public-key cryptography is also called asymmetric. It requires the use of a private key (a key that only its owner knows) and a public key (a key that both know). Public key cryptography is a fundamental technology and widely used throughout the world. It is the approach used by many cryptographic algorithms and commonly used for the distribution of software, financial transactions and in other critical security areas where it is important to protect against counterfeits and falsifications.

RSA is the most popular asymmetric digital image encryption algorithm. RSA (named for Rivets, Shamir and Adelman, who first described it publicly) is the first known algorithm for both signing and encryption, and was one of the first major advances in public-key cryptography. It uses a pair of keys, one of which is used to encrypt the digital image in such a

way that it can only be verified with the other key of the pair [4]. The keys are generated through a common process, but cannot be generated in a viable manner among them. The security of RSA depends solely on finding the prime factors that are used in the process of encrypt and decrypt, the digital image and is based on the assumption that factoring a large number is difficult. "Multiplying two large prime numbers is a one-way function. It is easy to multiply the numbers to obtain a product, but it is extremely difficult to factor the product and retrieve the two large prime numbers that have been multiplied previously. it is known as a factoring problem. " In this research, the security of the existing algorithm is improved whenever no one finds a way to solve this problem in a reasonable amount of time. RSA will be a secure encryption algorithm.

DMDLA Algorithm

A customized version of RSA algorithm called Dual modulation with discrete logarithm algorithm (DMDLA). By using an competent implementation of DMDLA algorithm, performance of the algorithm is analyzed by changing different parameters of the algorithm.

This algorithm has the following advancement

- Encryption of two Private keys using Dual modulus concept.
- Decryption of two Public keys using Dual modulus concept.
- Three different Random numbers are used to generate the encryption and decryption key

DMDLA algorithm is similar to RSA algorithm with some modification. DMDLA algorithm is based on discrete logarithm problem with the factorization problem. This modification increases the security of the cryptosystem. It uses an extremely large number having two prime factors (similar to RSA Algorithm). In addition to this, three natural numbers are used. These natural numbers introduce discrete logarithm problem thereby increasing the security of the cryptosystem [5].

Comparison of RSA And DMDLA Algorithm

DMDLA algorithm is an advance extension of RSA algorithm. The comparison between RSA & DMDLA algorithm in term of sign & design time comprising of key generation time, digital signature creation time & digital signature verification time which is directly related to performance & security concerns. The security of the RSA algorithm lies in factorization as there is no proper way to factorize the prime numbers effectively. No specific process is designed to integer factorization problem. As long as no one finds a way, RSA will be safe and will be one of the best encryption algorithm in use. So, to enhance the performance the security of RSA, a new algorithm is developed called Dual modulation with discrete logarithm algorithm (DMDLA).

This modification enhances the security of the algorithm [6]. Security of DMDLA algorithm depends on both factorization as well as discrete logarithm problem [7]. Therefore, one has to solve both the problems to break DMDLA algorithm. In this algorithm an extremely large number is there which has four prime factors. In addition to this, three natural numbers are used. These natural numbers introduce discrete logarithm problem thereby increasing the security of the cryptosystem [8].

Changing the Size of Prime Number: As the given table and mentioned graph shows up that when the value of prime numbers is increased,

Table 1: Changing Prime No Size with Constant Chunk Size and Public Key Size

Prime Number Size	Total Execution Time (ms)DMDLA	Total Execution Time (ms) RSA
128	2730	1886
256	3013	2401
512	4763	6740
1024	16267	21510

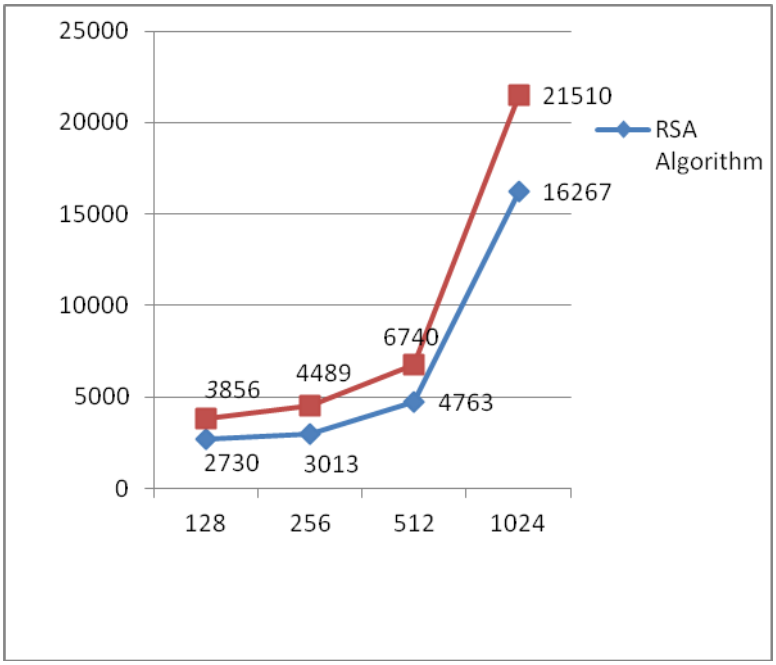

Figure 3: Changing Prime No Size with Constant Chunk Size and Public Key Size in RSA and DMDL Algorithm

Changing the length of the Public Key Size: The Public Key Size is increased, the overall execution time which comprises key generation time, digital signature creation time and digital signature verification time changes at random with the execution time.

Table 2 : Public Key Size V/S RSA, DMDLA Algorithm Execution Time

Public Key Size (bits)	DMDLA Total Execution Time (ms)	RSA Total Execution Time (ms)
128	16267	21510
256	18080	23463
512	16694	21981
1024	14586	16362

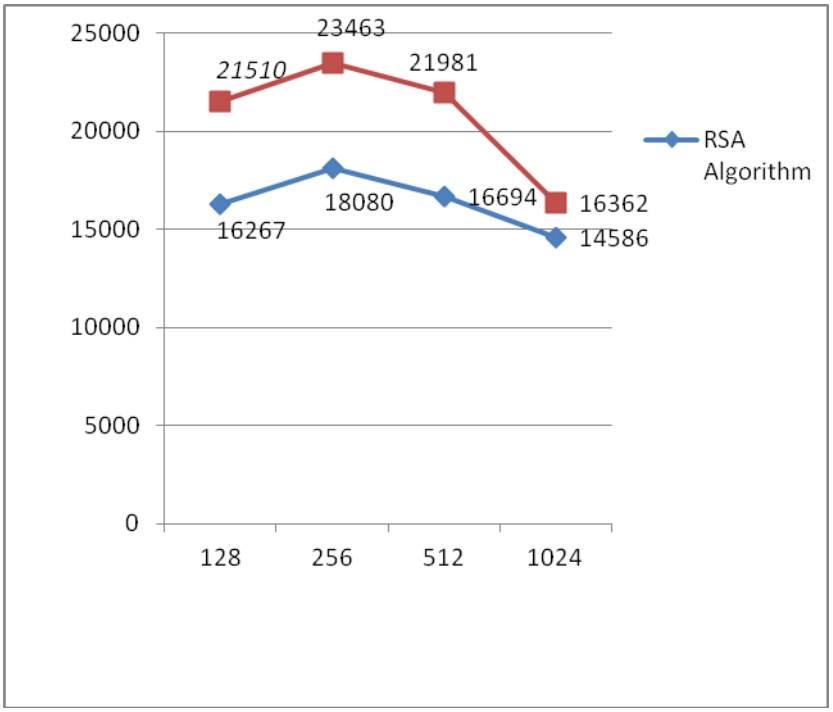

Figure 4: Public key Size V/s RSA, DMDLA algorithm execution time, taking Average bit size of Prime No. 1024 bits, size of chu**nk 64 bits & Random Number 16 bits.**

Changing the length of the message to be processed (chunk size): The chunk size is the number of characters to be processed at a time, either in encryption or decryption process. Here the message is divided into sub blocks each of length equal to chunk size. To illustrate the importance of this parameter, the message is taken long enough and the chunk size is allowed to vary in both the signature creation/signature verification process. The effect of changing the chunk size gives the results as shown in table and graph.

Table 3 : Chunk Size V/s RSA, DMDLA algorithm execution time

Chunk Size (bits)	DMDLA Total Execution Time (ms)	RSA Total Execution Time (ms)
64	23836	16362
128	18786	13401
256	14547	10337
512	9456	6542

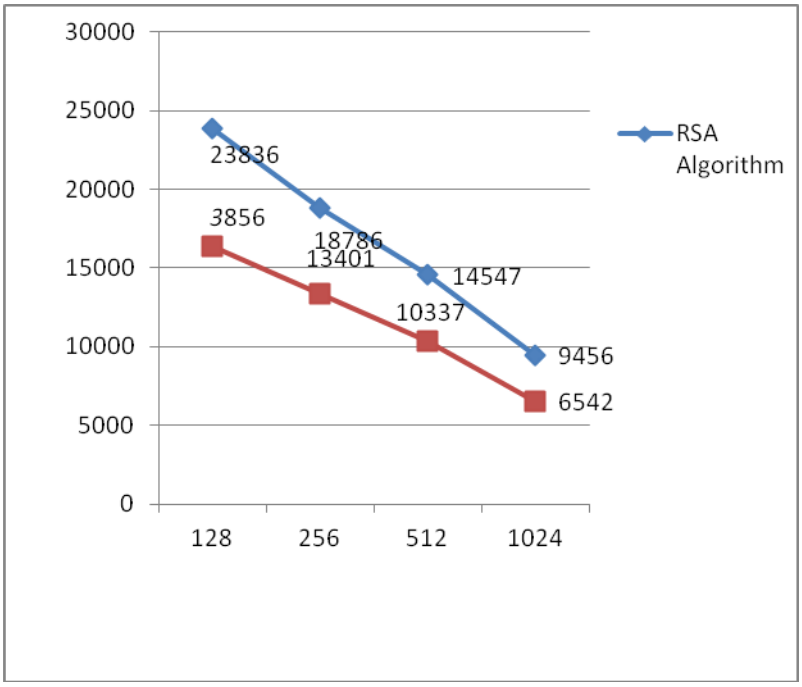

Figure 5: Chunk Size V/s RSA, DMDLA algorithm execution time

Conclusion

Most popular used public key algorithm is RSA. Asymmetric cryptosystems use two different keys, so you can use one to encrypt data and decrypt with the other key. The keys are generated by a general method, but they cannot be easily generated from each other. The security of the RSA system is based on the premise that many decomposing factors are difficult. In RSA, if we can factor the module (n) in its prime numbers, we can also get the private key. So in this paper a customized RSA algorithm is offered called Dual Modulus Digital Logarithmic Algorithm (DMDLA). The DMDLA algorithm uses dual dual module digital logarithmic encryption and decryption, so it is safer than the RSA algorithm. It has also been shown here that the dual module and numerical logarithmic problem play an important role in increasing the complexity of factorization compared to a single RSA applied module. The DMDLA algorithm uses double encryption and decryption using private and public double keys as well as three natural numbers. These natural numbers increase the security of the encryption system due to discrete logarithmic nature to provide security against various cyber attacks. Hence if an person or interloper detects a single key of DMDLA cryptosystem even then it is not possible to recognize the key.

References

1. Soram Ranbir Singh, Ajoy Kumar Khan and Soram Rakesh Singh, "Performance Evaluation of RSA and Elliptic Curve Cryptography", IEEE 2nd International Conference on Contemporary Computing and Informatics (ic3i), PP-302-306, 2016.
2. Aiswarya P M, Archana Raj, Dona John, Liya Martin and Sreenu G, "BINARY RSA ENCRYPTION ALGORITHM", IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), PP-178-181, 2016.

3. Prasenjit Kumar Das, Mr. Pradeep Kumar and Manubolu Sreenivasulu, "Image Cryptography: A Survey towards its Growth", Advance in Electronic and Electric Engineering, Volume 4, Number 2, pp. 179-184, 2014.
4. Aniati Murni, “Image Processing”, class handouts, Faculty of Computer Science, University of Indonesia, Jakarta, 2000.
5. Wen-bi Rao, Quan Gan “The Performance Analysis of Two Digital Signature Schemes Based on Secure Charging Protocol”, International Conference on Wireless Communications, Networking and Mobile Computing, vol.-2, pp. 1180 - 1182, Sept. 2005.
6. Qing Liu, Yunfei Li, Lin Hao and Hua Peng, "Two Efficient Variants of the RSA Cryptosystem", International Conference On Computer Design And Appliations (ICCDA 2010), Volume-5, PP-250-253, 2010.
7. Yunfei Li, “Design and Implementation of an Improved RSA Algorithm”, International Conference on E-Health Networking, Digital Ecosystems and Technologies, vol.-1, April 2010.
8. Aiswarya P M, Archana Raj, Dona John, Liya Martin and Sreenu G," Binary RSA Encryption Algorithm", IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), PP-178-181, 2016.
9. Soram Ranbir Singh, Ajoy Kumar Khan and Soram Rakesh Singh, " Performance Evaluation of RSA and Elliptic Curve Cryptography", IEEE International Conference on Contemporary Computing and Informatics (ic3i), PP-302-306, 2016.