International Journal of Applied Research 2018; 4(6): 170-174

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2018; 4(6): 170-174
www.allresearchjournal.com
Received: 23-04-2018
Accepted: 24-05-2018

Charru Kalra
PG Student, Department of Computer Science Engineering (CSE) Prannath Parnami Institute, Chaudharywas, Hisar, Haryana, India

Correspondence
Charru Kalra
PG Student, Department of Computer Science Engineering (CSE) Prannath Panamá Institute, Chaudharywas, Hisar, Haryana, India

Image to text encryption and decryption using modified RSA algorithm

Charru Kalra

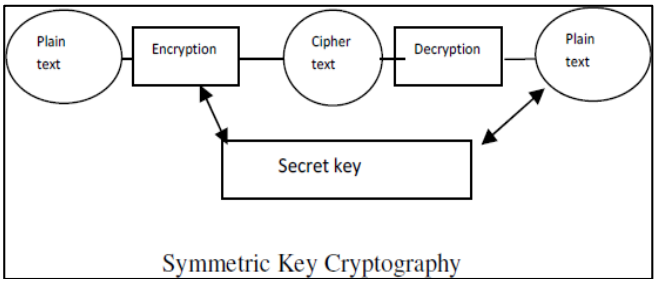
Abstract
Security is required to transmit confidential information over the network. Security is also demanding in wide range of applications. Cryptographic algorithms play a d very important role in providing the data security over malicious attacks. RSA encryption algorithm is Public key cryptography is also called as asymmetric key cryptography. This paper presents the literature review of methods of implementation of RSA algorithm and modified RSA algorithm.

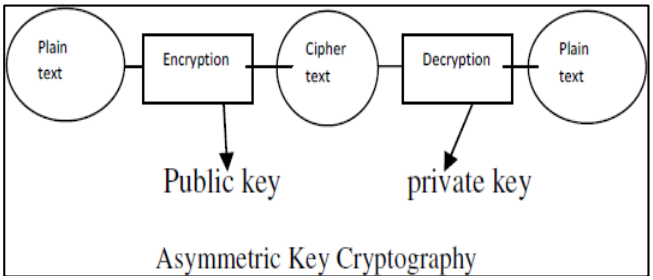
Keywords: Encryption, decryption, public key cryptography, pairwise RSA

1. Introduction
In the today's era the internet provides communication between people and facilitates for electronic payment, military communication and many others. This cause a major concern for privacy, identify theft, security etc. cryptography is a standard way of safe the data over the medium. Cryptography has been developed from the Greek word crypto which means is hiding the information person who study and discover cryptography are called cryptographers and study of cryptography is name by cryptanalysis. Cryptography is a part of secret information,it is science and art of protecting theinformation over the medium. It is process of convert readable text to unreadable text. By using the cryptography we can help this fickle information by private document on over computer network. In a distributed network cryptography become important part of secure communication,there are three type of cryptography algorithm: symmetric key cryptography, Hashing, Asymmetric key cryptography. An algorithm for cryptography that uses the same keys for both encryption of normal text and decryption for cipher text is called symmetric key cryptography,e.g. Data Encryption standard(DES) and Advance Encryption standard(AES).To solve the key distribution problem Maryam Ahmed developed the concept of public key cryptography in 1976.

2. Public Key Cryptosystem
In this cryptosystem, we have two different types of keys: one is the public key and second is the private key. Public key is publicly known and private key is kept secret. The system is called asymmetric system. If data encrypted by the public key so it can only decrypted by the private key. In public key cryptosystem, no need to share the secret data between two parties. So there is less chance of data stolen & manipulation and data is more secure.

3. RSA Cryptosystem
RSA algorithm is the first practicable public-key cryptosystems and is mainly used for secure data transmission. In cryptosystem, the encryption key is public and the decryption key is secret. In RSA, this asymmetry is based on the factoring the product of two large prime numbers that is called factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who is the founder of this algorithm and discovered in 1977.





It involves three steps

- Key Generation
- Encryption
- Decryption

Key Generation

In this, we need keys that are public and private. We will generate public and private key by using following steps. Public key is visible to both sender and receiver. But the private key is kept secret and not visible to end user.

Steps are

1. Choose two distinct prime numbers p and q.
2. For security purposes, these prime numbers p and q should be chosen at random, and must be of similar bit-length.
3. Compute n = pq. n is used as the modulus for both the public and private keys. It length is expressed in bits which is key length.
4. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p + q - 1)$, where φ is Euler's totient function.
5. Choose an integer e such that $1 < e < \varphi n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and φ(n) are co-prime. Where e is the public key exponent. And having a short bit-length and small Hamming weight results such as: 216 + 1 = 65,537. However, if the value of e is small.
6. Determine d as $d \equiv e{-}1 \pmod{\varphi(n)}$;i.e., d isthe multiplicative inverse of e (modulo φ(n)).

Decryption

$m \equiv cd \pmod n$

4. The Security of the RSA Cryptosystem

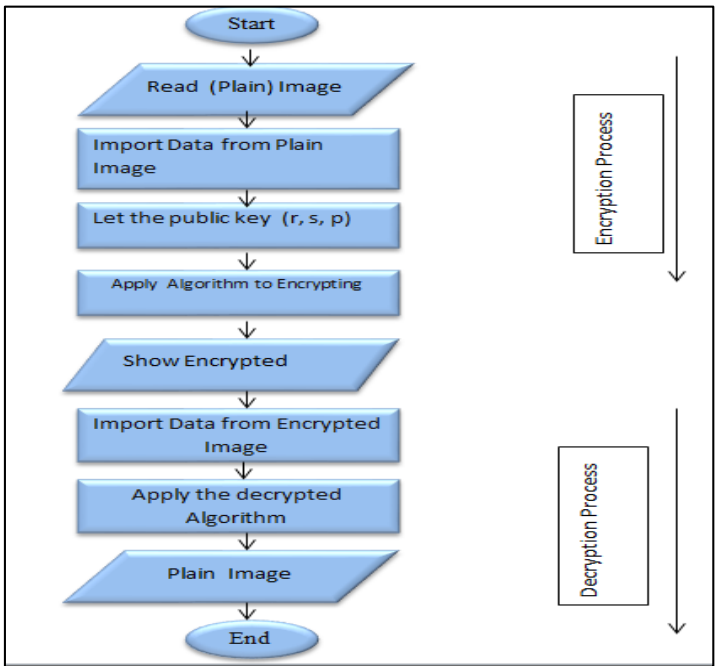
The security of the RSA cryptosystem relies on the integer factorization problem to find the secret key (**d**, R), which many cryptologists try to recover. If anyone can get the factors p and q of R, then it is so easy to find φ (R) and **d** and since e is known. Many studies showed that if R is a large composite number, then it is hard to obtain the prime factors of R Thus, hacking or cracking the RSA cryptosystem by factoring R would not be easy, and it is a conjecture in mathematics. Nevertheless, there might other ways to obtain d. It can be obtained by finding φ(R) from R, such that find $\varphi(R) = \varphi(pq) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$. Then p and q, that factorize R, can be found easily. Note that finding φ(R) is not easier that factoring R. Moreover, when p and q both have approximately 300 decimal digits, R=pq has approximately about 600 decimal digits. Using the fastest factorization algorithm to factor an integer of this size, more than millions of years of computer time are required to factor it.

5. Image Decryption

To decrypt the cipher image, the private key **a** and **X** are necessary to be known by the receiver. The process as the following (done by MATLAB):

1. Import to data (Y) from the encrypted image.
2. Restore the plain image M, such that $M \equiv [\, Y\ ((X)a)\text{-}1] \pmod p$
3. Obtain the original image (decrypted image).

The following flow chart shows the image Encryption and Decryption process:



Literature Review

Recently, there have been significant research works on Spam Detection. This section covers the literature survey of the work of the paper.

V. Kapoor [1] tells about cryptography is the art and science of achieving security by encoding message to make them non readable to secure data or information transmits over the network. In this paper introduced modified RSA approach based on multiple public keys and n prime number. RSA algorithm is mostly used in the popular implementation of public key cryptography. In public key cryptography two keys are developed in RSA one keys is used for encryption data and other corresponding key used for decryption. No other key decrypt the data. Even if it is efficient algorithm it is vulnerable to other person. With the help of all brute force attacks can obtain private keys. In this research paper new approach we used n prime number and multiple public keys. Which is not easily crack able. In here implementation RSA algorithm,using some mathematical logic integer factorization and discrete logarithm problem.

Sunita [2] discuss about cryptography is a process used for sending information in secret way. Goal of cryptography is to provide the protection for information but in various way. In this paper our motive to represent a new method for protection that is generated by combination of RSA and 2 bit rotation mechanism of cryptography. There are many algorithms exist for this process. For cryptography there are algorithms like RSA, IDEA, AES, and DES but here we are using only one algorithm from these that is RSA which is enough to implement combined process using 2 bit rotation. The encrypted image is used as input for network for further implementation. RSA encrypt image with 1 bit
rotation. In 1 bit rotation only 1 bit is shifted and at decrypt side shifted bit are reversed.

Karrar Dheiaa Mohammed AlSabti [3] The need of making important information that is being exchanged between two persons by unsecure websites has intersted cryptoligists to create and modify some secure cryptosytems to secure these information from getting hacked or cracked. In this paper, a strategy in the public key cryptosystem called RSA Cryptosystem is used to be applied over gray and color images with the help of MATLAB Program. Even the RSA cryptosystem is a well- known secure cryptosystem, we use MATLAB to use this cryptosystem over gray and color images. That would be generating two algorithms for the encryption and decryption. These algorithms are applied over the plain image and cipher image after reading them in the matrices forms. However, the image is partitioned into blocks that are n x m matrices. Since the RSA cryptosystem is a secure public key cryptosystem since its security based on the difficulty of the factoring problem, which is factoring a positive integer R into a product of two primes, we apply this cryptosystem over images using MATLAB with increasing the number of the primes in R. This gives the modified RSA cryptosystem has a higher security than the RSA cryptosystem, because decrypting any encrypted images requires factoring the large integer composed of the product of many large primes, and it requires knowing the size of the blocks that are formed from plain matrix. Therefore, this approach of encrypting and decrypting images using RSA cryptosystem with some modifications more immune against any attacks in the transmission of images in all agencies in the era of the information technology.

Dr. U. S. Bhadade [4] discuss about Security is required to transmit confidential information over the network. Security is also demanding in wide range of applications. Cryptographic algorithms play a d very important role in providing the data security over malicious attacks. RSA encryption algorithm is Public key cryptography is also called as asymmetric key cryptography. This paper presents the literature review of methods of implementation of RSA algorithm and modified RSA algorithm.

Hayder Raheem Hashim [5] tells about need of exchanging messages and images secretly over unsecure networks promoted the creation of cryptosystems to enable receivers to interpret the exchanged information. In this paper, a particular public key cryptosystem called the ElGamal Cryptosystem is presented considered with the help MATLAB Program to be used over Images. Since the ElGamal cryptosystem over a primitive root of a large prime is used in messages encryption in the free GNU Privacy Guard software, recent versions of Pretty Good Privacy (PGP), and other cryptosystems. This paper shows a modification of the this cryptosystem by applying it over gray and color images. That would be by transforming an image into its corresponding matrix using MATLAB Program, then applying the encryption and decryption algorithms over it. Actually, this modification gives one of the best image encryptions that have been used since the encryption procedure over any image goes smoothly and transfers the original image to completely undefined image which makes this cryptosystem is really secure and successful over image encryption. As well as, the decryption procedure of the encrypted image works very well since it transfers undefined image to its original. Therefore, this new modification can make the cryptosystem of images more immune against some future attacks since breaking this cryptosystem depends on solving the discrete logarithm problem which is really impossible with large prime numbers.

Dipali B. Khairnar [6] Main goal of Pair wise RSA Encryption Algorithm is secure transmission of confidential information over network. RSA encryption algorithm is Public key cryptography is also called as asymmetric key cryptography. Public key cryptosystem use key pair one use as public other use as private or secret key and private key cryptosystem use same private key for encryption and decryption. For encryption and decryption RSA encryption algorithm use key pair one key use for encryption which called as public key and other key use for decryption called as private key. In this paper, we have done an efficient implementation of Pair wise RSA algorithm using key pairs and using Euclidean algorithm rather than sending the e value directly as a public key. Because it avoid mathematical attacks and brute force attack. In this paper key size increased 512bit to 1024 bit in Pairwise RSA which provide highest security in the network.

Ravi Shankar Dhakar [7] The algorithms (RSA & MREA) have many important parameters affecting its level of security and speed [10]. By increasing the modulus length it is caused of increasing the complexity of decomposing it into its factors. This also increases the length of private key and hence difficulty to detect the key. Another parameter is modular multiplicative inverse. Where the modular multiplicative inverse is new factor of private key, so it will be more difficult to choose by trying all possible private keys for brute force attack hence the security also increases

as well as difficulty of detecting the private key. The RSA and MREA parameters are changed one parameter at a time and the others are kept fixed to study the relative importance [7].

Rajan. S. Jamgekar [8] The algorithms (RSA & MREA) have many important parameters affecting its level of security and speed. By increasing the modulus length it is caused of increasing the complexity of decomposing it into its factors. This also increases the length of private key and hence difficulty to detect the key. Another parameter is modular multiplicative inverse μ where the modular multiplicative inverse μ is new factor of private key, so it will be more difficult to choose μ by trying all possible private keys (brute force attack) hence the security also increases as well as difficulty of detecting the private key. The RSA and MREA parameters are changed one parameter at a time and the others are kept fixed to study the relative importance. The results vary depending on type of file and size of file [11].

A. Anagaw Ayele [9] RSA Encryption algorithm provide single public key, Less communication overload, More vulnerable to brute force attack, less security, The Public key is sent once. As compare with RSA Modified RSA provide Use two public key, High communication overload, less vulnerable to brute force attack, more security, The Public key is sent separately twice [6].

Allam Mousa [10] The 1024bit InKeSi SRNN implementation the methodology for computing the modular exponentiation is used. This is chosen because it can achieve an appreciable decrease of covered area and sometimes increase the time- performance comparing with other methodologies. The senders encrypt the message with Public Key of InKeSi SRNN algorithm and then the data is signed with the Private Key of InKeSi SRNN algorithm. The verification of digital signature is started after this process with the help of Public key at the recipient side. The decryption of the digital signature is done in this process which eventually results in the generation of message [5].

Conclusion

With the implementation of RSA algorithm using 2 bit rotation, we reach a conclusion that for better security of any text or image. In this work there choose an image and apply RSA algorithm on it. Then we got encrypted image and applies the 2 bit rotation algorithm on encrypted image and after that we apply Hill Cipher algorithm for better security. Then got an encrypted image which is very difficult to decrypt by any other person. So, the conclusion is that the, image is more secure.

References

1. Kapoor V. Institute of Engineering and Technology, DAVV, Indore, India," Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and 'n'prime, 1(2)
2. Sunita Bhagat Phool Singh Mahila Vishwavidhalaya, Khanpur Kalan, Sonepat, Image Encryption/Decryption using RSA Algorithm. 2017; 5(5):1-14.
3. Karrar Dheiaa Mohammed Al Sabti. University Of Kufa, Iraq. A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB" ISSN 0973-1768 2016; 12(4):3631-3640
4. Sarika Y Bonde, Dr. Bhadade US, SSBT. College of Engineering & Technology Bambhori, Jalgaon, (M.S) (India), Implementation of RSA algorithm and modified rsa algorithm 2017, 5.
5. Hayder Raheem Hashima, Irtifaa Abdalkadum Neamaa. Image Encryption and Decryption in A Modification of ElGamal Cryptosystem in MATLAB
6. Dipali B Khairnar, Sandeep Kadam, Dr. Patil DY. College of Engineering, Ambi University of Pune, Maharashtra, India, Secure RSA: Pair Wise Key Distribution using Modified RSA Algorithm. 2016; 6(4).
7. Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma. Modified RSA Encryption Algorithm (MREA), Second International Conference on Advanced Computing & Communication Technologies, 978-0-7695-4640- 7/12 $26.00 © 2012 IEEE, 2012.
8. Rajan S, Jamgekar, Geeta Shantanu Joshi. "File Encryption and Decryption Using Secure RSA, International Journal of Emerging Science and ngineering (IJESE) ISSN: 2319–6378, 2013; 1(4),
9. Anagaw Ayele A, Dr. Vuda Sreenivasarao. A Modified RSA Encryption Technique Based on Multiple public keys" International Journal of Innovative Research in Computer and Communication Engineering. 2013; 1(4).
10. Sheela K, George E, Dharma Prakash Raj. InKeSi-Increased Key Size Method in SRNN Public Key Cryptography Algorithm, IJCSMC, 2013; 2(8).
11. Maryam Ahmed, Baharan Sanjabi, Difo Aldiaz, Amirhossein Rezaei, Habeeb. "Diffie- Hellman and Its Application in Security Protocols" International Journal of Engineering Science and Innovative Technology (IJESIT) 2012; 1(2).
12. Golle P, Staddon J, Gagne M, Rasmussen P. A Content-Driven Access Control System, Proc. Symp. Identity and Trust on the Internet, 2008, 26-35.
13. Rangarajan A Vasudevan, Sugata Sanyal. Jigsaw-based Secure Data Transfer over Computer Networks Information Technology: Coding and Computing,. Proceedings. ITCC 2004. International Conference on 2004**,** 1
14. Wuling Ren, Zhiqian Miao. College of Computer and Information Engineering, Zhejiang Gongshang University, A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication Second International Conference on Modeling, Simulation and Visualization Methods, 2010.
15. Neal R Wagner. The Laws of Cryptography with Java Code, Technical Report, 2003, 78-112.
16. Allam Mousa. Sensitivity of Changing the RSA Parameters on the Complexity and Performance of the Algorithm, ISSN 1607 – 8926, Journal of Applied Science, Asian Network for Scientific Information, 2005, 60-63.
17. Atul Kahate. Cryptography and Network Security, ISBN-10:0-07-064823-9, Tata McGraw- Hill Publishing Company Limited, India, Second Edition, pages 38-62,152-165,205-240.
18. Gagandeep Shahi, Charanjit Singh. Cryptography and its two Implementation Approaches International Journal of Innovative Research in Computer and Communication Engineering. 2013; 1(3):668-672.
19. Rupali Verma, Maitreyee Dutta, Renu Vig. FPGA Implementation of RSA based on Carry Save Montgomery Modular Multiplication‖, IEEE International Conference on Computational Techniques

in Information and Communication Technologies (ICCTICT), 2016, 1-6

20. Narander Kumar, Priyanka Chaudhary, - Implementation of Modified RSA Cryptosystem for Data Encryption and Decryption based on n Prime number and Bit Stuffing‖, International Conference on Information and Communication Technology for Competitive Strategies (ICTCS- 2016), March 04-05, Udaipur, India, 2016, 1-6.