International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 4, May-June 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Image Cryptography using RSA Algorithm

Shivam Kumar[1], Dr. Ganesh D[2]

[1]Student, [2]Assistant Professor,
[1,2]Department of MCA, School of CS& IT, Jain University, Bangalore, Karnataka, India

ABSTRACT

Cryptography is a process used for sending information in secret way. Goal of this process is to provide protection for information but in different 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. But to make it more secure we are going to perform 2 bit rotation due to which it is more secure as compared to existing algorithm. After applying the 2 bit rotation we perform the permutation of that image that will give us encrypted image.

KEYWORDS: *Cryptography algorithms encrypted permutation*

How to cite this paper: Shivam Kumar | Dr. Ganesh D "Image Cryptography using RSA Algorithm" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-4, June 2021, pp.835-837, URL: www.ijtsrd.com/papers/ijtsrd42408.pdf

IJTSRD42408

I. INTRODUCTION

The Rivest-Shamir-Adleman (RSA) was publically described in 1977, which is used by modern computers to encrypt and decrypt the messages. It is an asymmetric cryptographic algorithm. As two different keys are used in this algorithm hence the name asymmetric. One key is shared to anyone therefore it is also called public key cryptography. Public key cryptography is largely used for authentication, non-repudiation, and key exchange. Cryptography is a technique or method for securing communications by using codes, so that the third parties cannot use that sensitive information and only intended users can read and process it.

National Bureau of Standards (NBS) algorithm. Most importantly, RSA implements a public-key cryptosystem, as well as digital signatures. RSA is motivated by the published works of Diffie and Hellman from several years before.

Modern cryptography algorithms offer more security than the ancient ones and can be divided into 3 categories, namely secret key, public key and hash functions. The focus of this paper is public key cryptography (PKC) algorithm.

II. LITERATURE REVIEW

This chapter is going to present some of the past work done in the field of public key cryptography with respect to RSA algorithm. This one includes the modifications done in the original methods along with about the attacks tried over it. Hung-Min Sun et al. have proposed a modified approach based on the same same format of public key cryptography. The authors have used the same format followed in the original version. Process of providing authentication was achieved here through blind signatures. Security issue was addressed in this work by increasing complexity in the process but it reflects in the larger execution time. Ravi Shankar Dhakar et al. made some modifications in the original steps. These corrections have begun from the very first step in the original process by having four different prime numbers in the place of only two. By this way both the public and private key had more components than the original. This approach straight away addressed the issue off actoring attacks but again failed to provide quicker execution time. Zulkarnain Md Ali et al. have taken both RSA algorithm and Elgamal crypto systems together to propose a new procedure as an alternative to RSA algorithm. This approach has increased the complexity over the process of providing security especially to counter factoring attacks. Instead of integer factorization discrete logarithm problem was chosen to counter the above said attacks. So this approach stands out as an alternate to the original algorithm to have a wider acceptance. Aayush Chhabra et al. proposed another modified version of RSA algorithm which has gained some attention among the researchers. The procedure was modified in the key generation part. Thus this approach too tried to address the factoring attacks. Since some modifications brought the security enhancement from the original, this work also stands as the modified RSA algorithm but the novelty on addressing other issues was not considered in this approach. In order to speed up the decryption process, this proposed approach tried to combine both of these approaches. This work also tried to show that the proposed one was less vulnerable to various attacks on RSA. The results showed that the time taken for decryption process was lesser than the approach which used Chinese Reminder Theorem which one was traditional one. This

proposed approach brought the significant advantage from the former approach.

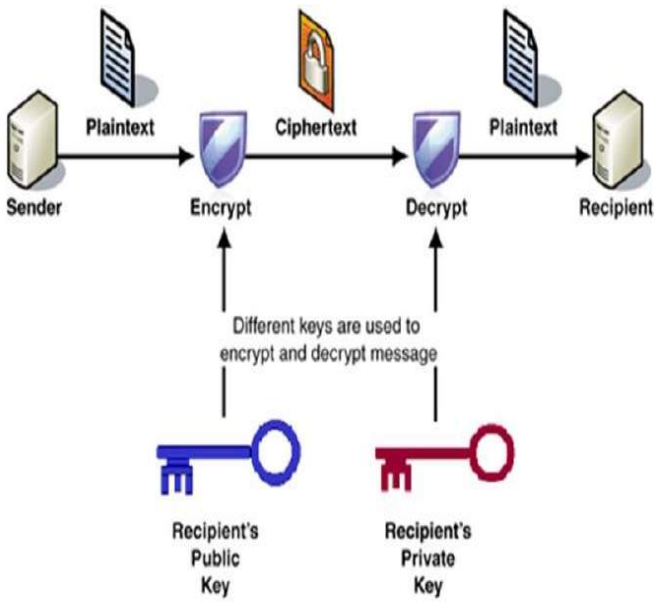
III. CURRENT USAGE OF RSA

Looking at where RSA is being used today, let's take the example of Pretty Good Privacy in short PGP, a freeware created by Phil Zimmerman, providing encryption and authentication for e-mail and file storage applications across multiple platforms and it uses RSA algorithm for its key transportation [14], [15]. Many cloud service providers also use PKC for authentication. One example is Googles G Suite, a brand of cloud based services that has been rated as excellent on PGMags review in February 2017, has about 3 million paid customers including large companies such as Whirlpool and Pice Water house Coopers taking advantage of a collaboration ready office suite, a website, shared calendars, mail services, chat, video conferences, social media, real-time document collaborations, and many more. Firstly, data access is enabled through Hypertext Transfer Protocol Secure (HTTPS) encrypted tunnels, then it uses Perfect Forward Secrecy (PFS), for which Google made headlines in 2011 for being the first to enable this feature [18], which scrambles data as it moves between their and other companies servers and it uses SSL (Secure Sockets Layer)/TLS (Transport Layer Security) for connectivity where the 256-bit TLS looks at the encryption enforcement policy which rejects all inbound and outbound mail from other mail servers if they don't use TLS [19]. A common operation in IT is RSA signature verification and many protocols such as SSH, Open PGP, S/MIME and SSL/TLS rely on it [20]. SSL certificates are used to protect the online users' private and sensitive data. In its bids to up defenses against the growth in cryptanalysis, Google has upgraded the length of all its SSL certificates RSA encryption keys from 1024 to 2048 bits for validation and key exchange in 2013.

IV. DESIGN ARCHITECTURE

The encryption is starting on the RSA algorithm with the selection of two large prime numbers, along with an auxiliary value, as the public key. The prime numbers are keep in secret. The public key is used to encrypt a message, and private key is used to decrypt a message or information.

The RSA algorithm is encrypt the original image and decrypts the image by the different keys.



V. WORKING OF RSA

The RSA involves four steps for the complete process which are key generation, key distribution, encryption, and decryption. All steps are mentioned below.

RSA is an algorithm is using in the modern computer environment to encrypt and decrypt the data in transform. The RSA algorithm is also called as an asymmetric cryptographic algorithm. Asymmetric cryptosystem means two different keys are using in the encryption and decryption. In the two keys one key is using for encryption and the second key is using for decryption. This RSA algorithm is also called as the public key cryptography. Because one of the secret key can be given to everyone which means public. The other key must be kept private.

The RSA algorithm consists of three manor steps in encryption and decryption. The steps are following as :-

5.1 Key Generation:-Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key.

1. Generating the RSA modulus (n)
2. Finding Derived Number (e)
3. Forming the public key
4. Forming the private key

5.2 Key Distribution: If a message is sent from one end to the other using RSA, one person will have the public key which is used for encryption(n, e) and other person will have the private key which will be used for decryption (d) and won't be distributed.

5.3 Encryption: Message is encrypted using a public key (n, e). To encrypt the first plaintext P, this is modulo n.Mathematical step for encryption is –

$$C = Pe \bmod n$$

Ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n.

5.4 Decryption: Message is decrypted using private key by the receiver. The receiver has received a ciphertext.

$$Plaintext = Cd \bmod n$$

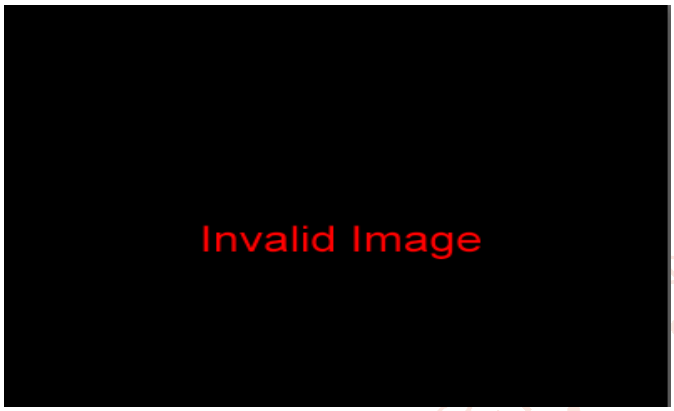
APPLICATIONS OF IMAGE CRYPTOGRAPHY

Core banking is a set of services providing by the group of networked bank branches. Bank customers may access their funds and perform the simple transactions from the member branch offices. The major issue in core banking is the authenticity of the customer. An unavoidable hacking of the databases on the Internet, it is always quite difficult to trust the information in Internet. To solve this problem of authentication proposing an algorithm based on image processing and image cryptography.

The internet multimedia applications is become popular. The valuable multimedia content such as the image is vulnerable to unauthorized access while in storage and during transmission over a network.

The image processing applications have been commonly found in the Military communication, Forensics, Robotics, Intelligent systems etc.

VI. RESULT



VII. CONCLUSION

Though, RSA is most used algorithm these days, still it has some limitations which are getting replaced by further versions of RSA. In today's digital world the most important thing is to encrypt the image due to various types of attacks and misusing of the same. Image encryption using RSA is proved to be efficient enough and highly securable. Even though RSA is the most used cryptography algorithm today, it has certain limitations which need to be taken into consideration for RSA to continue to be the best and research has to be done into making RSA quantum resistant. There is a need now more than ever for studies to be conducted in the area of quantum encryption methods resistant to quantum computers as it will soon replace the current encryption systems. Development of qCrypt isn't enough, but it's a start. However, we need more research into quantum resistant encryption systems. Development of qCrypt isn't enough, but it's a start. However, we need more research into quantum resistant encryption systems.

VIII. RECOMMENDATIONS

While the strength of RSA lies in the large prime number based keys, it's also causing RSA to be slower compared to other algorithms in terms of key generation. One example is the JSCAPE MFT Server, a platform independent server that consolidates all file transfer processes into a single easy to use application which requires users to choose between two supported key algorithms: RSA or digital signature algorithm (DSA) during the process of generating a public-private keypair in PGP [33]. Generally encryption happens at client end while decryption on the server side. Let's say that in the JSCAPE server the client side machine is slower and server more powerful then RSA is used for server keys as it has smaller computational requirements for encryption, thereby encrypting faster, however, if server is slower than DSA is used as there is a need for server keys that have smaller computational requirements for decryption, thus impacting the start of the session only. Even though he wasn't able to have a functional quantum computer of the necessary size to crack RSA encryption yet, Chuangs experiment points out the threat that such a computer poses to cryptographic systems [9]. In line with this comes the news of the Ireland's top young scientist and technologist of 2017, Shane Curran, a 16 year old student at Terenure College, who anticipated the impact quantum computing will have on current cryptographic methods and created qCrypt, a quantum-encrypted data storage solution is resistant to attacks by quantum computers

References

[1] https://ieeexplore.ieee.org/document/6021216/figures#figures

[2] https://www.tutorialspoint.com/cryptography/public_key_encryption.htm

[3] http://www.ijcset.net/docs/Volumes/volume5issue9/ijcset2015050902.pdf

[4] http://www.isg.rhul.ac.uk/static/msc/teaching/ic2/demo/42.htm

[5] https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[6] https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

[7] https://www.di-mgt.com.au/rsa_alg.html