International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 4 Issue 7 July 2017

A Review of Modern Cryptography Techniques with Special Emphasis on RSA

Chandni Vyas[1], Jitendra Dangra[2]
CSE Department, Lakshmi Narain College of Technology & science, Indore, M.P, India[1]
CSE Department, Assistant Professor, Lakshmi Narain College of Technology & science, Indore M.P, India[2]
Chandnivyas02@gmail.com[1], Jitendra.dangra@gmail.com[2]

Abstract: *The backbone of the modern world is electronic communication. Data is transferred from one place to another in almost no time using the electronic medium. But it also exposes the confidential data to the intruder. RSA is the most common and efficient cryptography technique that is used for the purpose of encrypting the content and then sending it over the channel, then than at receivers end the content is decrypted and converted in to original form. Although there are many security mechanisms are available. But there is a continuous need to improve the existing methods.*

The main objective of cryptography is to send information or message in hidden manner from one side to another in such a way that the intruder or attacker cannot crack the content and even unable to feel the presence of secret message. Although many new techniques have been proposed by many researchers to transmit data in encoded form from one side to another. But still it is possible to identify the original message. This paper presents a critical review of modern data encryption and decryption methods.

Keywords: *Diffe and Hellman, Plaintext, Ciphertext, Encription, Decription, Secret key, Public key, Private key.*

1. INTRODUCTION

The concept of public- key cryptography was invented by Whitfield Diffie and Martin Hellman, and independently by Ralph Merkle [1]. Their contribution to cryptography was the notion that keys could come in pairs- an encryption key and a decryption key-and that it could be infeasible to generate one key from the other. Diffie and Hellman first presented this concept at the 1976 National Computer Conference; a few months later, their seminal paper "New direction in cryptography" was published [2].

However, as we all know, communications over open networks are not secure. An effective solution to secure communication over open networks is to apply cryptographic schemes to protect the transmitted messages.

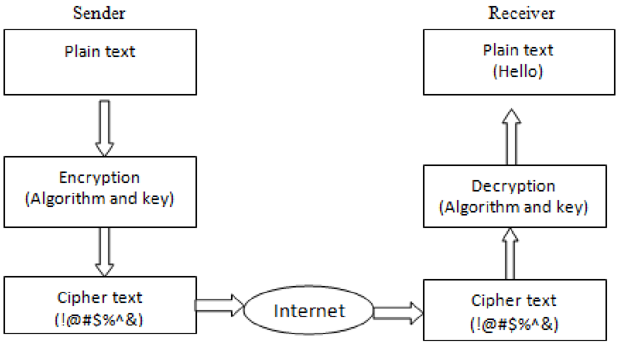

Figure 1 Model of Cryptography

Simply speaking, cryptography is the study of mathematical techniques related to the aspects of information security [3]. There are two categories of key-based cryptographic algorithms: symmetric algorithms and asymmetric algorithms. The same secret key is used to encrypt and decrypt the information in symmetric algorithms [4], as Figure 2 shows.

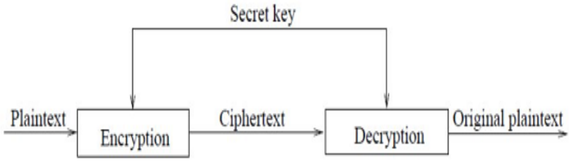

Figure 2: Encryption and Decryption with One Secret Key

In asymmetric algorithms, however, two different keys (namely, public key and private key) are used to encrypt and decrypt information, as shown in Figure 3.

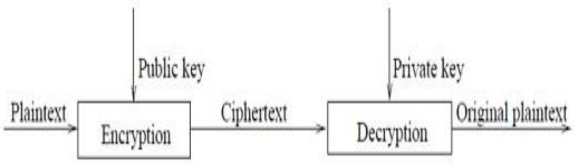

Figure 3: Encryption and Decryption with two keys

As the same (secret) key is used for encryption and decryption in symmetric cryptosystems, it is necessary to transfer the secret key among all communicating parties before secure communication begins. Prior to the birth of asymmetric cryptosystems (also called public-key cryptosystems), the exchange of the secret keys has always been a difficult problem because of the need for a confidential channel. In addition, for each pair of communicating parties, a different pair of the secret keys needs to be generated and shared, so the management of the secret keys had also been an issue [5].

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. Figure 4 shows the components involved in cryptography [6].

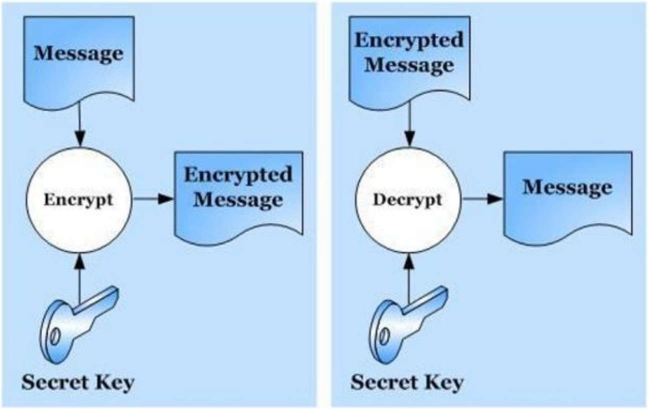

Figure 4: cryptography component

2. LITERATURE REVIEW

In any communication system including internet, satellite and mobile, it is impossible to prevent the important or sensitive information from eavesdropping or losses when the information is broadcasted through the channel (wire or wireless). So security of information has become increasingly important for any application [7].

Cryptography is the science that stands for methods used to transform data and hide its contents far from wrong hands. Cryptography defines a pair of two techniques that which grantees data transformation called encryption and decryption. Encryption is the process of transformation data (plaintext) to be transmitted using algorithm (called cipher), to unreadable form (cipher text).while decryption is the process to convert the encrypted data to the original form [8].

Prime numbers play a very important role in the complexity and security of the public key cryptosystem. RSA is one type of public key algorithm and its security depends on the complexity of factoring (n) value. Any encryption algorithm depends on the length of the key and the computational effort required breaking the key[8].

This is efficient algorithm to attack the RSA Scheme. Obtaining the private key of the RSA scheme is the target of the suggested algorithm by factoring the modulus based on the public key (e, n) of the RSA scheme. The suggested algorithm is very fast due to its treatments for the factorizing problem. It will limited the search for the p & q values especially when the value of n is small, since most of public key encryption schemes select a small encryption n in order to improve the efficiency and reliability of encryption. The suggested algorithm is more efficient than most existed algorithms of attack since it is break the search process and takes less running time [9].

Communication is the basic process of exchanging information. The effectiveness of computer communication is mainly based on the security aspects whether it is through internet or any communication channel. The aim of this paper is based on analyzing the results given by Wiener's, who says that if the private exponent d used in RSA cryptosystem is less than n^.292 than the system is insecure. We will focus on the result given by Weiner's and try to increase the range of private exponent d up to n^0.5. As n is the product of p & q (which are the relative prime numbers). This paper also aims at considering the different factors that affects the performance of encryption algorithms so as to make our information more secure over the network [10].

Yang Ren-er, ZhengZhiwei, Tao Shun, Ding Shilei [11], have presented DES algorithm for encryption along with LBS algorithm so that the hidden information is given a dual protection and the information is compressible and invisible to anyone else. Problem of the research was DES algorithm. Now days it is easily breakable.

Mr. Madhusudhan Mishra, Mr. Gangadhar, Tiwari, Mr.Arun Kumar Yadav [12], the authors has used a new technique. The author has used RSA algorithm for encryption along with F5 algorithm. To hide the encrypted message in the lower image, the author has also used a two tier security layers- first using cryptography key and second using stego key.

Manu Devi, Nidhi Sharma, [13] the proposed system the author has used LBS steganography for image embedding. The author has calculated the PSNR for the better quality of the image and how it is calculated has also been mentioned. The higher the PSNR value, the better is the quality of the stego image. The main aim of the research was developing a new and enhanced technique of hiding the data. The main motive was to make the encrypted message totally unbreakable from the inside.

Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R. [14] has proposed model gives two tier security to secret data. Further our proposed method gives high embedding capacity and high quality stego images using advanced encryption standard (AES) algorithm to encrypt secret message and then pixel value differencing (PVD) with least-significant-bit (LSB) substitution is used to hide encrypted message into true color RGB image.

3. CONCLUSION

Cryptography is a security mechanism which caters the security services of world in perfect manner. In this paper, we have elaborated the notion of cryptography along with the review of various schemes of managing the keys. A review of modern methods is also done in brief. The most of the modern data security techniques have been reviewed. Each of the method has been analyzed with the advantages and the disadvantages. Then a list of common problems in the current version has been identified.

REFERENCES

[1] William Stallings (2006), Cryptography and network Security Principles and Practices Fourth Edition.

[2] Diffie, W.; Hellman, M.1976. New directions in cryptography; Information Theory, IEEE Transactions on , Volume: 22 Issue: 6 , Nov 1976 Page(s): 644 –654 http://cs.unc.edu/~fabian/course_papers/diffie.hellman.pdf

[3] Samir Kumar Bandyopadhyay, Somaditya Roy 2010. Cryptosystem for Information Security, (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 04, 2010, 1419-1422

[4] Kallam Ravindra Babu, Dr. S.Udaya Kumar, Dr. A.Vinaya Babu 2010. A Survey on Cryptography and Steganography Methods for Information Security, International Journal of Computer Applications (0975 – 8887) Volume 12– No.2, November 2010.

[5] Forouzan (2007), Cryptography And Network Security, Special Indian Edition.

[6] Shamir, A. 1984. A polynomial-time algorithm for breaking the basic Merkle - Hellman cryptosystem; Information Theory, IEEE Transactions on , Volume: 30 Issue: 5 , Sep 1984 Page(s): 699 –704

[7] M. E. Hellman, "An Overview of Public Key Cryptography," IEEE Communications Society Magazine, Vol. 16, Nov. 1978, pp.24-32 (Invited Paper).

[8] Prof. Dr. Alaa H Al-Hamami, Bilal S O Al-Kubaysee 2011. A Fast Approach for Breaking RSA Cryptosystem, World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 6, 260-263, 2011

[9] Sachin Upadhyay, Yashpal Singh, Amit Kumar Jain 2012. An Analysis of the Attack on RSA Cryptosystem Through Formal Methods, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012

[10] Prof.Dr.Alaa Hussein Al-Hamami,Ibrahem Abdallah Aldariseh ,"Enhanced Method for RSACryptosystem Algorithm" 2012International Conference onAdvanced Computer Science Applications and Technologies, IEEE 2012.

[11] V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[12] Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June 2011 pp.192-192.