IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 1 ISSUE : 3 Print / Issue Publication Date: 08-Oct-2016

ISSN : 2455-2143

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 100-102
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

APPLYING RSA ON ASCII VALUE FOR ENCRYPTION AND DECRYPTION OF DATA

Abishek Kumar
B. Tech, CSE,
G.L.B.I.T.M
Gr. Noida, U. P., India

Ashish Kumar
B. Tech, CSE,
G.L.B.I.T.M
Gr. Noida, U. P., India

Manu Sharma
Asst. Professor, Dept. of CSE,
G.L.B.I.T.M
Gr. Noida, U.P., India

ABSTRACT - Cybercriminals are becoming more sophisticated and collaborative with every coming year. They are highly skilled and equipped with very modern tools; they often use 21st century tools to take on 20th century systems. So the prime concern of today's web based world is security. Each communication medium over the network must be secured for the proper transmission of hush-hush data and from unintended or unauthorized access, change or destruction. So it requires a high level of protection, for that there are several cryptography algorithms but all of them do not satisfy the required demand. Hence this paper with reference to RSA algorithm and additional steps is expected to provide safekeeping of information. By the use of ASCII value based RSA (AVBRSA); one height of safety is increased to the data because it performs two level of encoding. The beauty of this scheme is that it transforms the text of the message into a large number and then it is further concealed to make it unreadable.

KEYWORDS - Public key Cryptosystem, RSA, private key, public key, encryption, decryption, AVBRSA

I. INTRODUCTION

In today's computer centric world, security is the prime concern i.e. required to transmit confidential information over the network. Each and every application demands confidentiality which can be achieved using cryptography. Cryptography is derived from the Greek word kryptos, meaning hidden [4]. It is the art and science of writing secret messages or the study of various ways to disguise messages in order to avoid the interception from an unauthorized interceptor. It is a discipline that helps us to store and transmit data in unreadable form so that only those for whom it is intended can read and process it [2]. It includes techniques such as microdots, merging text with images, and other ways to hide information in storage or transit. It is most often associated with scrambling plaintext into encoded text (encryption), then back again (decryption). Encryption can be defined as the process of converting plaintext into cipher text using algorithms and key. The size of the cipher text is proportional to the size of plaintext. The primary purpose is to protect the confidentiality of digital data stored on computer systems or transmitted via the Internet or other computer networks; it is the most effective way to achieve data security. Cipher text is the result of encryption performed on plaintext using an algorithm, called a cipher [12]. This text is unreadable until it has been converted into plain text (decrypted). Decryption can be defined as the process of converting encoded text into the plaintext using algorithms and key. It is generally the reverse process of encryption. An authorized user can only decrypt data because it requires a secret key or password, this provides authentication.

Cryptographic systems can be broadly classified into symmetric key systems and asymmetric key systems. The public key cryptography is also called as the asymmetric key cryptography [3]. This system uses a different key for both encryption and decryption. It requires each user to have two keys – a public key and a private key (secret key). The sender of the data encrypts the message using the receiver's public key. The receiver then decrypts this message using his/her private key [11]. The public and private keys are always in pairs, it is difficult to derive at the private key from the public key which is shared [5]. That is why this method is considered to be more secure than the symmetric method. RSA adopted public key cryptography algorithm which is considered as one of the most secure cryptographic algorithm. The use of RSA on American Standard Code for Information Interchange (ASCII) value can add one more level of protection to the data as the original data is modified by using the ASCII value [10]. By applying ASCII value based RSA (AVBRSA) method data becomes ambiguous for the unauthorized person or it can be said that data will become bogus for the eavesdropper. This approach will give enhancement to the public key cryptosystem. AVBRSA includes grouping of data so that each group consist of few characters and applying some steps on the ASCII value of each characters of a group to make it more secure. This method helps in increasing the level of protection by increasing the complexity of the data. It also decreases the possibilities of finding the actual data by the attacker because it increases the number of possible combination for the original data.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 100-102
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

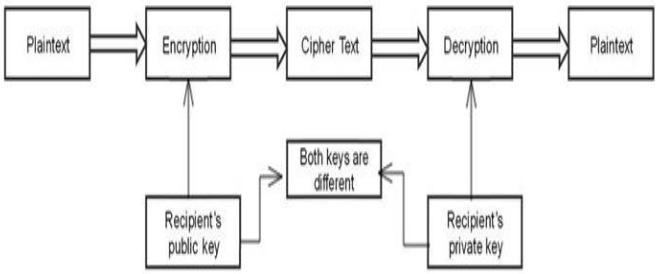

Fig1: Life cycle of Public key cryptography

II. CLASSICAL METHODOLOGY

Traditional ciphers are the earliest and simplest types of ciphers in which a character is used as a unit of data to be encrypted [8]. It of two types namely substitution ciphers and transposition ciphers. Substitution ciphers operate on the principle of substitution of one symbol with the other. If the symbols are alphanumeric characters (such as A, B, etc.), then such characters are replaced by another characters. For example, A can be replaced by C or B by Z etc. The symbols in the digit form (0, 1, 2, etc.) are also replaced by another digits. The types of substitution ciphers are mono-alphabetic and poly-alphabetic. In mono-alphabetic substitution, a character in the plaintext is always replaced by some other text regardless of its position in the text. For example if A in the plain text is to be changed by Z, then every A in the plaintext will always be changed to Z regardless of its position. In poly-alphabetic substitution, each character is replaced by a group of characters to obtain the cipher text. Hence, the relation between each character in the plaintext to the character in the encoded text is one-to-many. Transposition ciphers retain their plaintext form, but change their positions when unreadable text is created. The plaintext is arranged in the form of a two dimensional table and columns are interchanged as per key. But this is not very secure because it is possible to be cracked by trial and error method.

2.1 Deviation in Classical Methodology

The major problem with simple substitution ciphers is that the frequencies of letters are not masked at all. In the case of small message, the cipher text is easily deciphered by anyone willing to try deciphering with different key values. The main problem with substitution cipher and transposition cipher is that the actual letters are not changed, so frequency counts reveal not only trends in letter repetition but the actual plaintext letter that the cipher text is linked to (because they are the same letter). Generally speaking, having the plaintext and encoded text letters line up exactly with each other always leads to easily deciphered messages. Another disadvantage of this method of derangement is that the last letters of the alphabet (which are mostly low frequency) tend to stay at the end.

III. PREVAILING METHODOLOGY

The traditional ciphers use a character or a symbol as the unit of encryption or decryption. But the modern ciphers use a block of bits as the unit of encryption or decryption. This means that both the plaintext and cipher text are blocks of bits. It uses the power of computing to provide message secrecy, message integrity (the message has not been changed) and sender authentication (the sender is who he claims to be) [7]. The basis for modern ciphers is the one-way mathematical function.

3.1 Anomaly

Public key cryptography for encryption is a very slow process [1]. And in case of block cipher if the data is corrupted due to noise the complete block is lost. This technique is also not applicable when the size of data is not known beforehand. The key size of RSA is 1024 bits which are not used any more for web sites because it has been cracked by the cryptanalyst.

IV. ASCII VALUE BASED RSA

The most widely used RSA is based on arithmetic modulo of product of two large prime numbers and it is also known that factorizing of a very large number into prime factors is not feasible, there is no known algorithm for finding such factors. So the only method is by trying every possible key [6] that makes it secure.

The proposed technique is based on ASCII value that uses RSA algorithm to increases the level of security of the data. The ASCII Value Based RSA **(AVBRSA)** increases the number of steps for encryption and decryption of data that leads to increase the complexity of the data. And so it becomes strenuous for the eavesdropper to crack the data, hence data becomes more protected.

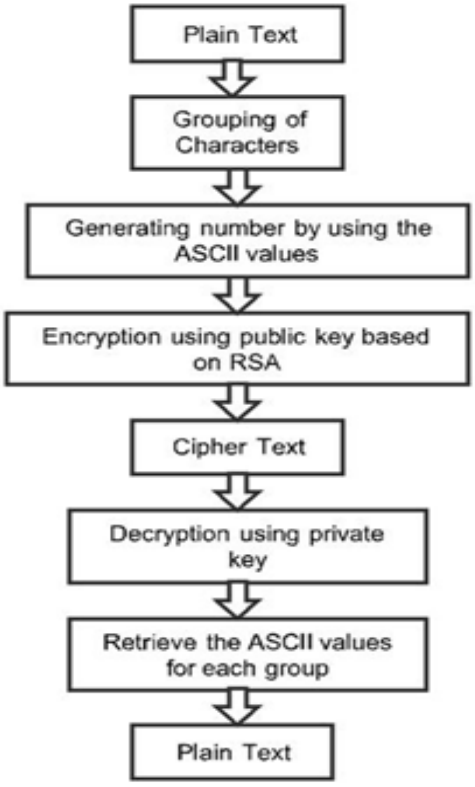

Fig2: ASCII Value Based RSA

The above depicted flow chart describes the AVBRSA technique in which the plaintext or the message is grouped such that each group consist of few characters. After grouping the characters of the message, ASCII content of each group is calculated. In order to generate the number some mathematical operation are performed on the ASCII content of each group. Further this number is encrypted using the public key and RSA algorithm to produce the cipher text. Cipher text is the unreadable text that is constructed by the encryption algorithm. Now this text is transferred to the recipient that is then decrypted using the decryption algorithm and the private key to breed the number. Again some mathematical calculations are done to retrieve the ASCII content of each group and finally the original plaintext can be recovered. The beauty of this scheme is that two levels of encryption and decryption is performed which enhances the security of a data.

V. FUTURE SCOPE AND CONCLUSION

In the paper we analyse that the process of encryption and decryption is performed by using AVBRSA algorithms on characters of data, further it can be used for a complete text file. It also enhances the complexity of cipher text as well as the security of data. In future we will apply and implement these processes for secure communication over the network. Finally conclude that RSA becomes prolific to characters with AVBRSA technique in terms of protection.

VI. REFERENCES

[1] 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*, pages 60-63,2005.

[2] R. Rivest, A. Shamir and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, February 1978, pages 120-126.

[3] William Stallings,"Cryptography and Network Security", *ISBN 81-7758-011-6*, Pearson Education, Third Edition, pages 42-62,121-144,253-297.

[4] 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.

[5] Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma, "Modified RSA Encryption Algorithm (MREA)", Second International Conference on Advanced Computing & Communication Technologies, 2012.

[6] Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek, "Dual RSA and Its Security Analysis", IEEE Transactions on Information Theory, Vol. 53, No. 8, Aug. 2007.

[7] Sattar J Aboud, Mohammad A AL-Fayoumi, Mustafa Al-Fayoumi and Haidar S Jabbar, "An Efficient RSA Public Key Encryption Scheme", Fifth International Conference on Information Technology: New Generations, 2008.

[8] Shamir A. (1984): 'Identity based cryptosystems and signature schemes', Advances in CryptologyCrypto, Lecture Notes in Computer Science, Springer- Verlag, 1 96, pp. 47-53.

[9] Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma,"Modified RSA Encryption Algorithm (MREA)"-978-0-7695-4640-7/12, IEEE2012

`

[10] Akansha Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", *International Journal on Computer Science and Engineering*, vol. 4, no. 9, pp: 1650- 1657, September 2012.

[11] Yunfei Li, Qing Liu, Tong Li, Design and Implementation of an Improved RSA Algorithm, 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies

[12] B. Schneier, Applied cryptography, second edition, NY: John Wiley & Sons, Inc., 1996.

[13] Vikas Agrawal , Shruti Agrawal , Rajesh Deshmukh "Analysis and Review of Encryption and Decryption for Secure Communication", ISSN (Online): 2347-3878, Volume 2 Issue 2, February 2014

[14] Hardik Gandhi, Indra Rajput, Vinit Gupta "A Research on Enhancing Public Key Cryptography by the Use of MRGA with RSA and N-Prime RSA", IJIRST, Volume 1, Issue 12, ISSN (Online): 2349-6010, May 2015

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143