Volume 8, No. 3, March – April 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A New and More Authentic Cryptographic Based Approach for Securing Short Message

Ekta Agrawal
Research Scholar, Faculty of Computer Science
Pacific Academy of Higher Education & Research University, Udaipur, Rajasthan, India

Dr. Parashu Ram Pal
Professor, MCA
Lakshmi Narain College of Technology, Bhopal, M.P., India

***Abstract*:** In the era of internet & smart phone every day terabytes of data are being generated. Data security over internet during communication is a great challenge. Cryptography is an integral part of data security mechanism over the internet. Cryptography makes information unintelligible to an unauthorized person. Cryptography provides confidentiality and maintains integrity to genuine users. Cryptography is the study of mathematical techniques related to information security aspects such as confidentiality, data integrity, entity authentication, and data authentication. The input to an encryption process is commonly called the plain text, and the output the cipher text. A cryptographic algorithm works in combination with a key a word, number, or phrase to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. In this paper a new approach which provides more authentic and strong encryption and decryption process for short message has been proposed.

Keywords: Cryptography, Security, Privacy, Encryption Algorithm and Decryption Algorithm.

I. INTRODUCTION

Cryptography is the study of mathematical techniques related to information security aspects such as confidentiality, data integrity, entity authentication, and data authentication. Plaintext is the original data before being encrypted and the data of the encryption output is called cipher text or cryptogram [1]. The methods which used to encrypt plaintext are called ciphers. A cryptographic algorithm works in combination with a key a word, number, or phrase to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. Figure 1 shows he encryption process while sending data from one end to another end.

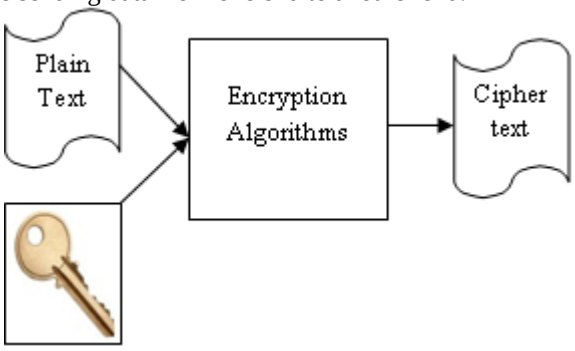

Figure 1: Encryption Process

The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. Cryptography enables user to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. [2]

II. DATA SECURITY ISSUES

Security architecture focuses on security attacks, mechanisms, and services and also shown in Figure 2. These can be defined as follows.

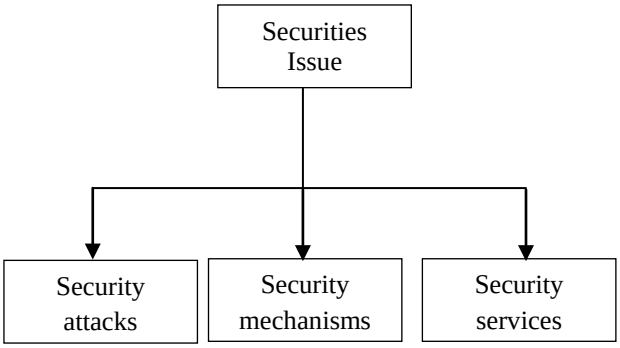

Figure 2: Security Issues

1. Security attack: Any action that compromises the security of information owned by an organization. Security attacks classified in terms of passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation. [3]

2. Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Lists the security mechanisms defined in X.800 are divided into those that are implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service. A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted. Irreversible encipherment mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications. [3]

3. Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. [3]

III. LITERATURE REVIEW

Various papers have been viewed and observed certain parameters to design aspects to more authentic and effective approach for encryption and decryption algorithm for better security.

In 2012 Pratap Chandra Mandal proposed "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish". They provide a fair comparison between four most common and used symmetric key algorithms: DES, 3DES, AES and Blowfish. They used rounds, block size, key size, and encryption/decryption time as parameter. Form the result they show that blowfish is more suitable than AES. [4]

In 2012 Monika Agrawal & Pradeep Mishra proposed "Comparative Survey on Symmetric Key Encryption Techniques". They present a detailed study of most of the symmetric encryption techniques with their advantages and limitations over each other. [5]

In 2013 Dr. T. Bhaskara Reddy proposed "An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding". They considered an image, read its pixels and convert it into pixels matrix of order as height and width of the image. Replace the pixels into some fixed numbers; generate the key using random generation technique. Encrypting the image using this key , performing random transposition on encrypted image, converting it into one dimensional encrypted array and finally applied Huffman coding on that array , due this size of the encrypted image is reduced and image is encrypted again .[6]

In 2013 Obaida Mohammad & Awad Al-Hazaimeh proposed "A New Approach for Complex Encrypting and Decrypting Data". They enhanced security goals by using maintains of the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme. [7]

In 2013 Debasis Das proposed "Design an Algorithm for Data Encryption and Decryption Using Pentaoctagesimal SNS". They presented a new method for data encryption and decryption based on number theory. Data encryption using strange number system (especially using pentaoctagesimal (SNS) can provide real physical security to data .They a better data encryption and decryption strategy offer better security towards all possible ways of attacks [8].

In 2013 Anupama Mishra proposed an algorithm on "Enhancing Security of Caesar Cipher Using Different Methods". He focused on the well-known classical techniques and induces some strength to this classical encryption. He proposed method to show better in terms of providing more security to any given text message. To make it more secure he used some techniques like multiple level Row Transposition Ciphers, encryption with same key at each level and encryption with different key at each level [9].

In 2013 Krishna Kumar Pandey & Vikas Rangari proposed "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security" Proposed work used enhanced symmetric key encryption algorithm, in which same structure of encryption and decryption procedure algorithm is used. The proposed algorithm uses key generation method by random number in algorithm for increasing efficiency of algorithm. [10]

In 2013 Dr. L. Arockiam, and S. Monikandan proposed their approach on "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm". This paper has provided an encryption algorithm to address the security and privacy issue in cloud storage in order to protect the data stored in the cloud. This technique has emphasized on improving classical encryption techniques by integrating substitution cipher and transposition cipher. Both substitution and transposition techniques have used alphabet for cipher text. [11].

In 2014 Prachi Saxena and Sini Shibu proposed "A Novel Approach to Design Time Efficient and Secure encryption Algorithm (T-SEA)". They proposed a new encryption/decryption technique and used the basic security principle for confidential and authenticity. They developed an algorithm with variable key length to improve the security. Results are showing that performance of the proposed concept in terms of efficiency and security [12].

In 2014 Satyajeet R. Shinge & Rahul Patil proposed "An Encryption Algorithm Based on ASCII Value of Data". They presented a symmetric cryptographic algorithm for data encryption and decryption based on ASCII values of characters in the plaintext. The secret key is converted to another string and that string is used as a key to encrypt or decrypt the data. [13]

In 2014 Mitali & Vijay Kumar proposed "A Survey on Various Cryptography Techniques" This represented a fair performance comparison between the various cryptography algorithms on different settings of data packets. They analyze the encryption and decryption time of various algorithms on different settings of data. [14]

In 2014 Surabhi Shah and Megha Singh proposed "A New Encryption Algorithm to Increase Performance & Security through Block Cipher Technique". They designed a system that provides complete authenticity and confidentiality over the open network. They proposed a system which works using new block cipher cryptography along with its comparison to other block cipher algorithm [15].

In 2015 Zaeniah, Bambang Eka Purnama proposed "An Analysis of Encryption and encryption Application by using One Time Pad Algorithm ".Security of data in a computer is needed to protect critical data and information from other parties. One way to protect data is to apply the science of cryptography to perform data encryption. Algorithm One Time Pad uses the same key in the encryption process and a

decryption of the data. An encrypted data will be transformed into cipher text so that the only person who has the key can open that data. The application that implements the one time pad algorithm can help users to store data securely. [16]

In 2017 Ekta Agrawal & Dr. Parashu Ram Pal, "A More Effective Approach Securing Text Data Based on Private Key Cryptography" has observed that the proposed approach takes less time for encrypting given text. [17]

IV. SYMMETRIC ALGORITHM

Symmetric technique has emphasized on improving conventional method of encryption by using substitution cipher. Substitution techniques have used alphabet for cipher text. In this symmetric algorithm, initially the plain text is converted into corresponding ASCII code value of each alphabet. In classical encryption technique, the key value ranges between 1 to 26 or key may be string (combination alphabets). But in symmetric algorithm, key value ranges from 1 to 256. The symmetric algorithm is used in order to encrypt the data of the user in the clouds. Since the user has no control over the data after his session is logged out, the encryption key acts as the primary authentication for the user. [11]
The proposed algorithm will be designed to compare with the symmetric approach given by Dr. L. Arockiam and S. Monikandan. [11]

V. PROPOSED APPROACH

In this section, a new and more authentic cryptographic based symmetric approach is designed for secure short message. In this technique a random number is used as the initial key to add in front of the text, where this key will use for encrypting the given source file using proposed encryption algorithm.

A. Encryption Process

The proposed encryption algorithm works in the following steps:

1. Read the input text.
2. Now add the key in front of the text.
3. Find ASCII code of each text and convert into binary data.
4. Find out One's complement of the previous binary data.
5. Convert binary data and obtain the Decimal value from it.
6. Decimal value is now divided by 4 and finds equivalent ASCII code of the result divide and put it as one character with reminder.
7. Now merge the result with the remainder to got cipher text.
8. Finally got the cipher Return encrypted text.

B. Decryption Process

The proposed decryption algorithm works in the following steps:

1. Read the cipher text.
2. Now split the two digit cipher text into single - single digit.
3. Now multiply the first digit by 4 and add the second digit into the result of multiplication.
4. Convert the result of above steps into binary equivalent.
5. Take the One's complement of the binary equivalent of the result.
6. Find the Decimal value of the previous value which was obtained by complement.
7. Now take the ASCII code of the above result. .
8. Remove the added key from the front of the text to get the plain text.

VI. ARCHITECTURE OF PROPOSED ALGORITHM

The algorithm is used in order to encrypt the data so that the unauthenticated user will not use the secured data. Since the user has no control over the data after sending the data as session is logged out. The key used acts as the primary authentication for the user. Proposed algorithm is shown with the help of flow chart in Figure 3.

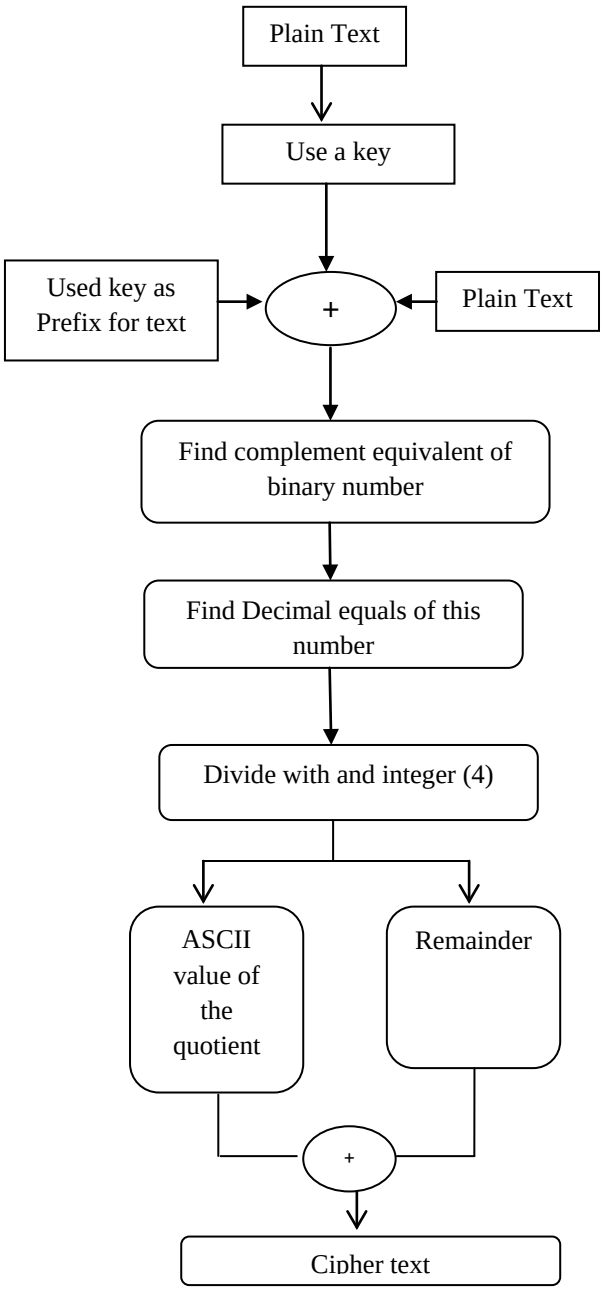

Figure 3: Architecture of Proposed Algorithm

VII. EXPERIMENTAL ANALYSIS

The performance of proposed algorithm is evaluated and also compared it with symmetric key cryptography [8]. The experiments were performed on i3 processor (2.5GHz Intel Processor with 4M cache memory), 2GB main memory and 400 GB secondary memory , and running on Windows 7 . The algorithms are implemented in using C# Dot net frame work version 10.

The simple text file is used which can be created using note pad. The simple text file is taken from a selected location. Figure 4 and Figure 5 shows the encryption process using symmetric approach and proposed approach respectively.

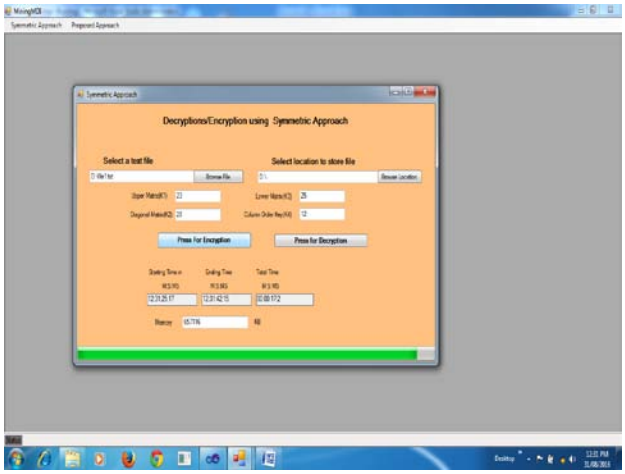

Figure 4: Encryption using Symmetric Approach

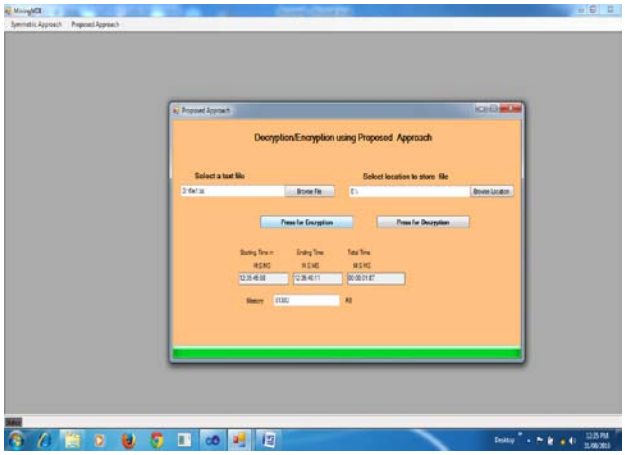

Figure 5: Encryption using Proposed Approach

VIII. COMPARATIVE ANAYSIS

The results are compared on the basis of file size and execution time for encryption. Table 1 shows comparison between symmetric approach and proposed method on the basis of file size and execution time for encryption. Figure 6 shows the comparisons graph for encryption for different file size in symmetric and proposed approach.

Table 1 Execution Time for symmetric approach and Proposed Approach

File Size in KB	Symmetric Approach (in milliseconds)	Proposed Approach (in milliseconds)
10	167	132
50	256	172
100	312	242

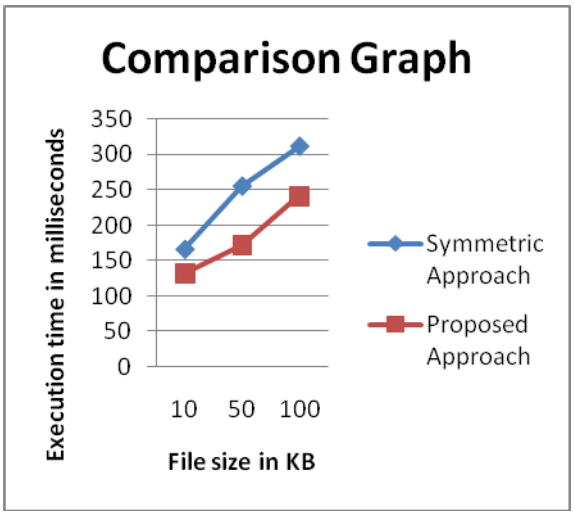

Figure 6: Comparison graph for encryption using symmetric and proposed approach

IX. CONCLUSION

From the experimental analysis it is clear that the proposed approach has been performed as well as compared to the existing approach. Only single key is used for encryption and decryption both. But in the hybrid symmetric approach they have used four key [8]. In this proposed algorithm, the number of keys is minimized as compared with symmetric approach. As the number of keys is minimized so the size of the key should also be reduced. To minimize the execution time in milliseconds, this algorithm is proposed for encrypting and decrypting the text file. On comparing the results of execution time for encryption and decryption for both the approaches, the proposed approach improves the performance and reduces the time required for execution when compared to the symmetric approach. This proposed approach also used simple calculation and operation. The proposed work should be extended in future to implement for special characters.

X. REFERENCES

[1] William, “Cryptography and Network Security Principles and Practice”, Fifth Edition, Pearson Education, Prentice Hall, 2011.

[2] Schneier B., “Applied Cryptography”, John Wiley& Sons Publication, New York, 1994.

[3] A. Kahate “Computer and Network Security” 2nd Edition, Tata Mc-Grew – hill Publisher ltd, 2011.

[4] Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish ", in Journal of Global Research in Computer Science, Vol.3, Issue , 2012

[5] Monika Agrawal & Pradeep Mishra "A Comparative Survey on Symmetric Key Encryption Techniques" in International Journal on Computer Science and Engineering (IJCSE) ISSN: 0975-3397 Vol. 4 No. 05 May 2012.

[6] Dr. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti, "An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding" IJCTA | Nov-Dec 2013 .

[7] Obaida Mohammad Awad Al-Hazaimeh "A New Approach for Complex Encrypting and Decrypting Data" in International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013.

[8] Debasis Das , U. A. Lanjewar , S. J. Sharma"Design an Algorithm for Data Encryption and Decryption Using Pentaoctagesimal SNS"*International Journal of Computer Trends and Technology (IJCTT)*,V6(2):84-88 December Issue 2013 .ISSN 2231-2803.www.ijcttjournal.org. Published by Seventh Sense Research Group.

[9] Anupama Mishra proposed an algorithm on "Enhancing Security of Caesar Cipher Using Different Methods" in International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[10] Krishna Kumar Pandey & Vikas Rangari "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security in International Journal of Computer Applications (0975 – 8887) Volume 74– No. 20, July 2013.

[11] Dr. L. Arockiam & S. Monikandan "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm" in International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), ISSN : 2278 – 1021 (Online) and ISSN: 2319-5940 (Print) Vol. 2, Issue 8, August 2013.

[12] Prachi Saxena and Sini Shibu proposed "A Novel Approach to Design Time Efficient and Secure encryption Algorithm (T-SEA)" in IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. VI (Feb. 2014), PP 29-34

[13] Satyajeet R. Shinge & Rahul Patil "An Encryption Algorithm Based on ASCII Value of Data". (IJCSIT) in International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234.

[14] Mitali, Vijay Kumar & Arvind Sharma "A Survey on Various Cryptography Techniques" in International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Web Site: www.ijettcs.org Email: editor@ijettcs.org Volume 3, Issue 4, July-August 2014.

[15] Surabhi Shah and Megha Singh proposed "A New Encryption Algorithm to Increase Performance & Security through Block Cipher Technique" in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 9, September 2014 ISSN: 2277 128X.

[16] Zaeniah & Bambang Eka Purnama "An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm" in International Journal of Advanced Computer Science and Applications, Vol. 6, No. 9, 2015

[17] Ekta Agrawal & Dr. Parashu Ram Pal, "A More Effective Approach Securing Text Data Based on Private Key Cryptography" in International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC) ISSN: 2321-8169, Volume: 5 Issue: 3, March 2017.