iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IX **Month of publication:** September 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Improved Cryptography Algorithm to Enhanced Data Security

Charru[1], Paramjeet Singh[2], Shaveta Rani[3]

[1]*M.Tech Scholar,* [2]*Assistant Professor,* [3]*Assistant Professor*

[1,2,3]*CSE Dept., GZS PTU Campus, Bathinda, India*

Abstract: ***The high growth in the evolution of networking and wireless networks leads to grant communication anywhere at any time. Security of data and telecommunication can be done by a technique called cryptography. In this paper we have developed a new cryptography algorithm based on exclusive-OR operation to enhanced data security. Security is measured by computing number of decryption steps required to accomplish the decryption process. Higher the number of decryption steps to decrypt the ciphertext to get original message shows higher level of security. All the simulation has been conducted using visual C# to implement the proposed algorithm. Experimental results show that proposed algorithm results in maximum security.***

Keywords: Ciphertext, Cryptography, Decryption, Encryption, Plaintext, Security, XOR.

I. INTRODUCTION

Cryptography is derived from Greek meaning “hidden or secret”, and “writing”, or “study” respectively; is the science of protecting information by encoding it into an unreadable format. Cryptography is a method of storing and transmitting data in a form that only intended user can read and process it. Encryption algorithms are in used today may be symmetric or asymmetric.

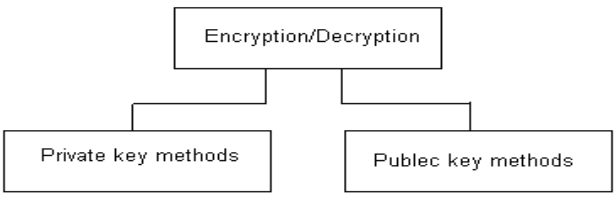


Figure 1: Methods of Enryption/Decrption

In symmetric key encryption method the secret key is used and it should be make available to sender and receiver both and no one else. Symmetric key encryption algorithms are DES, 3DES, Blowfish, RC2, RC5 and AES et al. In asymmetric key encryption the key used is not secret. The key is public that can be shared by anyone but the decryption key should be made available to the receiver only. Asymmetric key encryption algorithms are RSA, Digital signature algorithm, Diffie Helman, ElGamal, ECC et al.

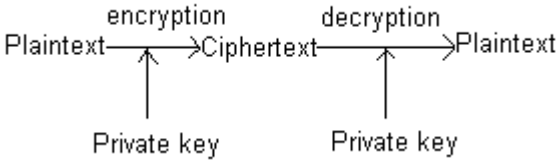


Figure 2: Private key encryption Method

Encryption is considered as the subset of cryptography. Encryption is the actual process of applying cryptography. A system that provides encryption and decryption is referred to as a cryptosystem and can be created through hardware components or program code in an application. Most encryption methods use a secret value called a key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the text, as depicted in below figure [3]

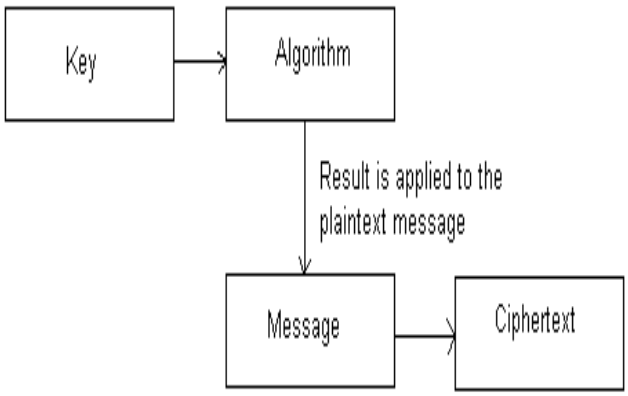


Figure 3: Key is used to generate the ciphertext

The key is inserted into the mathematical algorithm and the result is applied to the message, which ends up in ciphertext. The key can be any value that is made up of a large sequence of random bits. An algorithm contains a keyspace, which is a range of values that can be used to construct a key. The larger the keyspace, the more available values can be used to represent different keys, and the more random the keys are, the harder it is for intruders to figure them out. The main objective of every cryptographic algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key.

II. LITERATURE SURVEY

V. Vasudha Rani, K. Kanaka Vardhini, "Secure and Efficient key Ciphering through ASCII Codes"

To provide more security for the data the authors proposed an algorithm with feature of self generated key or the key is generated from the input data that is to be encrypted. In this system they used a fixed length key which is of 8-bits. The main focus of the author is on the security that is required at a level as well as on speed of execution that is the time required to encrypt and decrypt the data. With this algorithm both security and speed of execution are possible. And the key which is generated is unpredictable till it is not generated. In this proposed system security aspect is high and execution time is less compared to common existing encryption techniques [3].

V. Gupta, G. Singh, R. Gupta, "Advance cryptography algorithm for improving data security"

The author developed a new cryptography algorithm which is based on block cipher technique and used cryptography logical operation like XOR and shift operation. The proposed algorithm used random number method for generating the initial key and fixed key length of 512 bit key size to encrypt a text message. Experimental results used two parameters for execution time. And then implemented encryption and decryption time comparisons of text files with other two existing commonly cryptography algorithms [8].

D. Sravan Kumar, CH. Suneetha, A. Chandrasekhar, "A Block Cipher using Rotation and Logical XOR operations"

Data encryption is an important part of secure communication of the messages. In this paper, the author proposed a method of encrypting the data in blocks using the operation rotation and logical exclusive-OR. The size of the data block is selected to be of 64 characters and using ASCII code each character of the block is coded to 8 bit binary format. Data in blocks are encrypted in 8 rounds using rotation and XOR operation with one time key derived for each round from the session key of that particular bock. The proposed key scheduled algorithm is less prone to timing attacks as well as brute force attacks [10].

III. EXISTING WORK

A. Encryption system with self generated key of fixed length

To encrypt the data the author proposed a technique which is based on ASCII values of input data. This algorithm is based on symmetric key encryption approach. In this system they used a random method to generate the fixed key of 4 characters [2]. Further various transformations are applied to encrypt the data with the help of generated random key. To decrypt the data reverse transformations are applied on encrypted data. The existing system has the moderate level of security because it encrypts the data only one time by using fixed length key.

TABLE 1: NUMBER OF DECRYPTION STEPS

Input data (Plain text) in bytes	Number of decryption steps
4	12
8	25
12	37
16	52

IV. PROPOSED WORK

To increase the level of security further exclusive-OR operation is performed to generate the final ciphertext and corresponding security factor is computed by applying the exclusive-OR operation based advanced encryption system (XAES) algorithm. The output of self generated key of variable length i.e. SGKVL encryption algorithm [1], before applying XOR operation is considered as input to XAES algorithm. To start the exclusive-OR operation, equivalent zeros are inserted to output data of SGKVL algorithm and corresponding bits are calculated. To accomplish the encryption process entire string of input data is divided into two halves i.e. LHH and RHH array of bits. And then XOR operation is performed on values of these two halves. After this various operation like complement and concatenation are performed on resultant values. And then at last, division operation is performed to get final ciphertext. To get the encrypted text reverse XOR operation is applied on final ciphertext. This final ciphertext is considered as input to SGKVL decryption algorithm. To perform the decryption process, the receiver uses an algorithm that is known as decryption algorithm and a key to transform the cipher text back to original message. Then after getting encrypted text, system get the ASCII values of generated encrypted text of SGKVL algorithm and find the minimum ASCII value by traversing each ASCII value of encrypted text. To calculate the difference subtract the each ASCII value of final encrypt key from the each ASCII value of encrypted text. After this, add the minimum ASCII value of generated encrypted text to each value of the difference to get the plaintext or original text.

Steps to perform encryption process:

Step 1: Insert equivalent no. of zeroes to input data length.

Step 2: Get the ASCII code value of input file and convert the entire input file to its bits equivalent.

Step3: Divide the whole data length into two halves into LHH and RHH array of bits.

Step 4: Now perform exclusive-OR operation on the bits of these resultant values and stored the result into xorh variable.

Step 5: Applied complement operation on RHH and xorh bit values and after this perform the concatenate operation between RHH and xorh variable and stored the result in an encr. variable.

Step 6: Divide the original length by 8 and get the encoded form of input data.

Step 7: Exit.

Steps to perform decryption process:

Step 1: Take the encrypted value in as input string.

Step 2: Take the complement of RHH and xorh bit array values.

Step 4: Now perform exclusive-OR operation on the resultant values of RHH and xorh and stored it in LHH variable.

Step 5: After this perform the concatenate operation between the LHH and RHH and stored the result in decr. variable.

Step 6: Divide the entire bit length by 8 and get the decoded form of input data.

Step 7: Exit.

V. RESULTS & DISCUSSIONS

It is shown that the security can be enhanced by applying XAES algorithm. For different data sets, results of existing algorithm [2] are compared with XAES algorithm. The output of SGKVL algorithm [1] is considered as input to XAES algorithm.

The simulation results of XAES algorithm are:

A. Testing Data Set for different input data size:

It is shown that the security can be improved by applying XAES algorithm. For different data sets, results of existing algorithm are compared with XAES algorithm. To improve security, exclusive-OR operation is performed on encrypted data. Security of an algorithm is measured by computing number of decryption steps. Higher the number of decryption steps to decrypt the ciphertext to get original message shows higher level of security. As shown below, for input text data of different lengths, number of decryption steps varies. According to XAES algorithm, number of decryption steps taken by decryption algorithm to decrypt the ciphertext is high than number of decryption steps of existing algorithm [2].

TABLE 2: NUMBER OF DECRYPTION STEPS OF DIFFERENT DATA VALUES

Input data (Plain Text) size in bytes	Existing Algorithm with fixed length key	XAES Algorithm
4	12	28
8	25	40
12	37	53
16	52	71

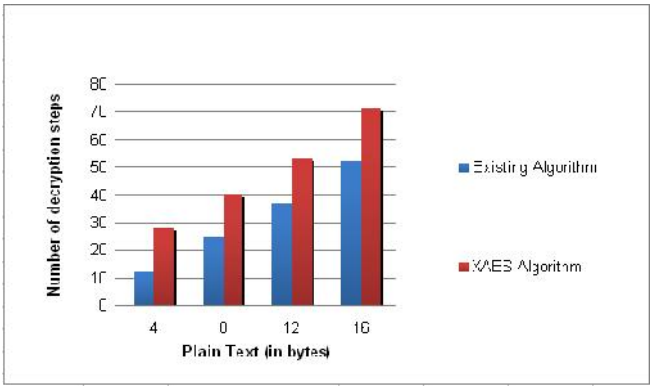


Figure 4: Security comparisons with existing algorithm

B. Testing Data Set for different input data size:

Now, different data values are taken to compute number of decryption steps. For different data sets, results of existing algorithm are compared with XAES algorithm. To improve security, exclusive-OR operation is performed on encrypted data. Security of an algorithm is measured by computing number of decryption steps. Higher the number of decryption steps to decrypt the ciphertext to get original message shows higher level of security. As shown below, number of decryption steps varies according to different data values.

TABLE 3: NUMBER OF DECRYPTION STEPS OF DIFFERENT DATA VALUES

Input data (Plain Text) size in bytes	Existing Algorithm	XAES Algorithm
20	70	87
40	124	141
60	180	198
80	251	267

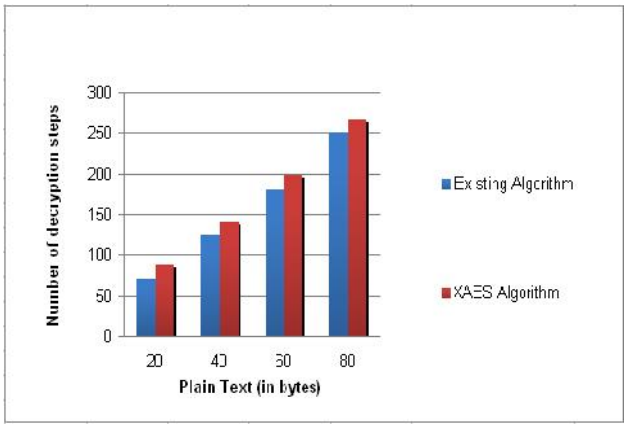


Figure 5: Security comparisons with existing algorithm

Graphical representation of the above described table is shown in figure 4 and 5 for computing security in terms of number of decryption steps of "Encryption system with self generated key of fixed length [2]" and "XAES Algorithm". According to the graph, there is tendency that number of decryption steps of proposed algorithm, and compared algorithm increases with text data size. As shown, number of decryption steps varies according to different data values. According to XAES algorithm, number of decryption steps taken by decryption algorithm to decrypt the ciphertext is high than number of decryption steps of existing algorithm [2].

V. CONCLUSIONS

In the proposed encryption system, logical operation like exclusive-OR is performed on input data to increase the level of security. It is shown that the security can be improved by applying XAES algorithm. Security of an algorithm is measured by computing number of decryption steps. Higher the number of decryption steps to decrypt the ciphertext to get original message shows higher level of security. From the results, it is computed that number of decryption steps taken by decryption algorithm to decrypt the ciphertext according to XAES algorithm is higher than number of decryption steps of existing algorithm. Thus a stronger encryption system is developed that results in maximum security to encrypt the plain text messages. The system can be further extended to encrypt the multimedia data such as audio files, video files and images etc.

REFERENCES

[1] Charru, Paramjeet Singh, Shaveta Rani, "Efficient Text Data Encryption system to Optimize Execution Time and Data Security", International Journal of Advanced Research in Computer Science and Software Engineering, volume 4, Issue 7, July 2014, ISSN: 2277 128X.

[2] Udepal Singh, Upasna Garg, "An ASCII value based text data encryption system", International Journal of Scientific and Research Publications (IJSRP), Volume 3, Issue 11, November 2013, ISSN 2250-3153.

[3] V. Vasudha Rani, K. Kanaka Vardhini, "Secure and efficient key ciphering through ASCII codes", International Journal of Systems, Algorithms & Applications(IJSAA), Volume 3, Issue ICRAET 13, March 2013, ISSN Online: 2277-2677.

[4] A. Mathur, "An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", International Journal on Computer Science and Engineering (IJCSE), Vol. 4, No. 09, September 2012.

[5] E.Thambiraja, G.Ramesh, Dr. R.Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012, ISSN: 2277 128X.

[6] G. Gupta, R. Chawla, "Review on Encryption Ciphers of Cryptography in Network Security", International Journal of Advanced Research in Computer Science and Software Engineering (IJARSSSE), Volume 2, Issue 7, July 2012, ISSN: 2277 128X.

[7] AL. Jeeva, Dr. V. Palanisamy, K. Kanagaram, "Comparative analysis of performance efficiency and security measures of some encryption algorithms", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 3, May-June 2012, pp.3033-3037.

[8] V. Gupta, G. Singh, R. Gupta, "Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software

Engineering, volume 2, Issue 1, January 2012, ISSN: 2277 128X.

[9] CISSP All-in-One Certification Exam Guide, ch-08: Cryptography.

[10] D. Sravan Kumar, CH. Suneetha, A.Chandrasekhar, "A Block Cipher using Rotation and Logical XOR operations", International Journal of Computer Science, Volume 8: Issue 6,No 1, November 2011.

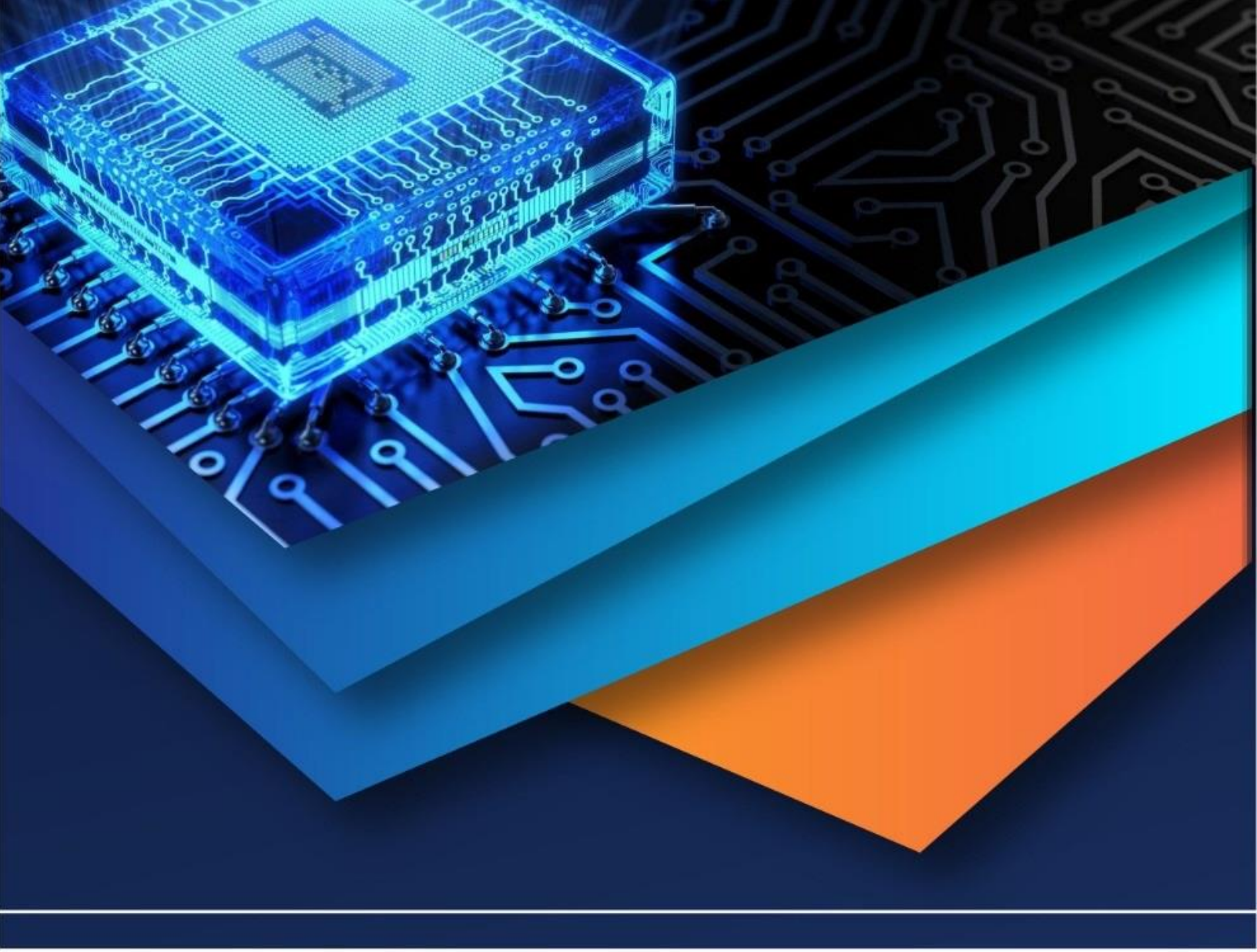
[11] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha, "Throughput Analysis of Various Encryption Algorithms", International Journal of Computer Science and Technology (IJECT), Vol. 2, Issue 3, September 2011, ISSN : 2230-7109 (Online) | ISSN : 2230-9543 (Print).

[12] Gary C. Kessler, "An Overview of Cryptography", May 1998, an article available at www.garykessler.net/library/crypto.html.

[13] Behrouz A. Forouzan, "Data communication and networking", second edition update, copyright © 2001, 1998 by the Tata Mc Graw-Hill companies.

[14] Er. Vidiksha, Er. Shekher Saini, "Data Encryption and Decryption using Deterministic Random Key for Transmission: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013, ISSN: 2277 128X.

[15] Prof. K. Govinda, Dr. E. Sathiyamoorth "Multilevel cryptography technique using graceful codes", Journal of Global Research in Computer Science, Volume 2, No. 7, July 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY