A Secure and Fast Approach for Encryption and Decryption of Message Communication

Ekta Agrawal
Shri Vaishnav Institute of Management, Indore
8 PUBLICATIONS **7** CITATIONS
SEE PROFILE

Parashu Ram Pal
ABES Engineering College
50 PUBLICATIONS **148** CITATIONS
SEE PROFILE

ISSN 2321 3361 © 2017 IJESC

Research Article Volume 7 Issue No.5

A Secure and Fast Approach for Encryption and Decryption of Message Communication

Ekta Agrawal[1], Dr. Parashu Ram Pal[2]
Research Scholar[1], Professor[2]
Department of Faculty of Computer Science[1], Department of MCA[2]
Pacific Academy of Higher Education & Research University, Udaipur, Rajasthan, India[1]
Lakshmi Narain College of Technology, Bhopal, M.P, India[2]

Abstract:
Encryption is one the most effective approach to achieve data security and privacy. The Encryption techniques hide the original content of a data in such a way that the original information is recovered only through using a key known as decryption process. The objective of the encryption is to secure or protect data from unauthorized access in term of viewing or modifying the data. Encryption can be implemented occurs by using some substitute technique, shifting technique, or mathematical operations. Several symmetric key base algorithms have been developed in the past year. In paper an efficient reliable symmetric key based algorithm to encrypt and decrypt the text data has proposed. The method uses 8 bit code value of alphabet and perform some simple calculation like logical NOT and simple binary division to produce. The proposed method is easy to understand and easy to implement.

Keywords: Encryption, Decryption, Symmetric Method, Key Size and File or Message Size.

I.INTRODUCTION

Data security has become most important aspect while transmission of data and storage. The transmission and exchange of image also needs a high security. Cryptography is the art of secret writing. Cryptography is used to maintain security. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. Figure 1 shows the information transmitting between sender and receiver. Figure 2 shows the creation of interrupts between sender and receiver. Figure 3 shows the changes, theft or delete information between sender and receiver.

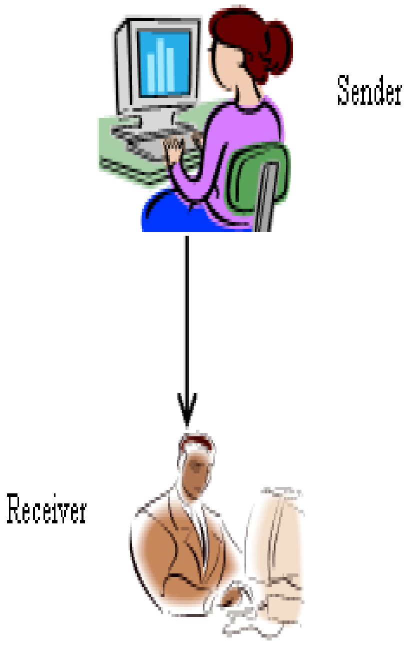


Figure.1. Information Sender and Receiver

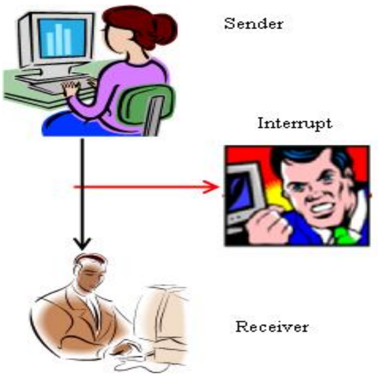


Figure .2. Creating Interrupts between Sender and Receiver

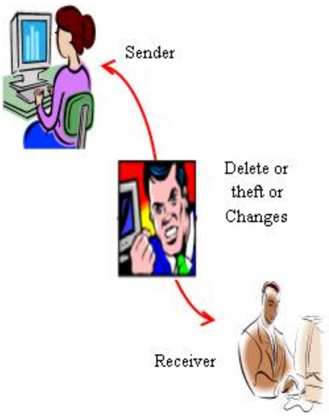
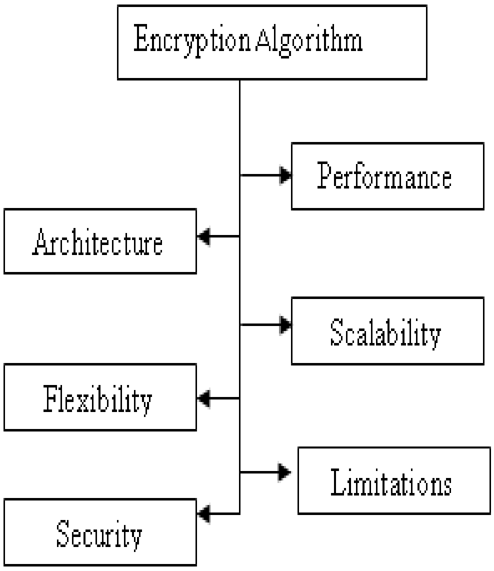


Figure.3. Changes, Theft or Delete Information between Sender and Receiver

II. SECURITY STANDARDS

Several symmetric algorithms exist but there are some parameters to evaluate them. To select appropriate algorithm for a particular application we need to know its strength and

limitation. There are some parameters need to consider these parameter include Architecture, Performance, Flexibility Security, Scalability and Limitations. Figure 4 shows the parameters for encryption
Algorithm



.
Figure. 4. Security Parameters

The security parameters are as follows:

2.1 Architecture:-Architecture includes structure and mathematical operations that an algorithm performs for encryption and decryption. Characteristics and how they are implemented. It also includes key used in the algorithm (secret key or public key) for encryption and decryption.

2.2 Performance:-Performance includes time required for Encryption and decryption, Memory required Software hardware performance and computational cost.

2.3 Security:-Security measures strength of the algorithm form attacks. It includes required element, possesses and property of algorithm. Security of an encryption algorithm depends on the key size used to execute the encryption. Length of key is measured in bits
.

2.4 Flexibility:-Flexibility defines whether the algorithm allows some modification or not. Some time we need to modify the algorithm because of the requirements.

2.5 Scalability:-We test the algorithm for different size of the file or data. So scalability is one of the important elements for algorithms. Scalability depends on certain parameters such as Memory Usage, Encryption rate, Software hardware performance; Computational efficiency.

2.6 Limitations:-Each and every algorithm has some drawback for an encryption algorithm we already known attacks or weakness of the algorithm. Limitation defines how fine the algorithm works for the resources available to it, how often is vulnerable to different types of attacks.

III. LITERATURE REVIEW

Several papers have been reviewed and observed certain aspects to implement the effective approach for encryption and decryption algorithm for security.

In 2010 Ayushi proposed “A Symmetric Key Cryptographic Algorithm “. There are two basic types of cryptography Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. She represents various symmetric key algorithms in detail and then proposes a new symmetric key algorithm.. [4]

In 2012 Suyash Verma et al proposed “An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security”. They proposed new encryption algorithm and used block cipher generating mechanism. They proposed evaluation, results by calculation with different plaintexts in the same key (DPSK) mode. By the results they show that, under the same key size and for the same size of the data, proposed algorithm work faster than existing algorithm [5]**.**

In 2013 Prerna Mahajanet al proposed “A Study of Encryption Algorithms AES, DES and RSA for Security”. They implemented three encryption techniques like AES, DES and RSA algorithms and compared their performance of other encryption techniques based on time for encryption and decryption. They also show results of analyses of effectiveness of each algorithm. Based on the text files used and the experimental result [6].

In 2014 Anjula Gupta et al. proposed “Cryptography Algorithms: A Review”. They proposed a study of existing encryption techniques are analyzed to promote the performance of the encryption methods. To sum up, all techniques they used unique ID. They surveyed many papers; found that throughput value of BLOWFISH is greater than all symmetric algorithms. Power Consumption value of BLOWFISH is least [7].

In 2014 Reema Gupta et al proposed “Efficient Encryption Techniques in Cryptography Better Security Enhancement”. They proposed a study of Encryption techniques and discussed with their limitations and procedure .Huffman coding and B2G, G2B is used for encryption. They also discussed various transpositional techniques like Simple columnar, simple row, Route cipher, transposition [8].

In 2015 Abhishek Joshi et al proposed “An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attacks” They proposed an efficient cryptographic scheme for text message Protection against Brute force and Cryptanalytic attacks. They show that this technique can also be used for most crucial applications where it requires a significant security of transmitted message and also there is no overhead on the transfer of message and the key when it is used with our proposed technique [9].

In 2015 Ashraf Odeh et al “A Performance Evaluation of Common Encryption Techniques with Secure Watermark System (SWS)”. They demonstrate a fair comparison between the most common algorithms and with a novel method called Secured Watermark System (SWS) in data encryption field according to CPU time, packet size and power consumption. They provides a comparison the most known algorithms used in encryption: AES (Rijndael), DES, Blowfish, and Secured Watermark System (SWS). They apply the same methodology on images and audio data [10].

In 2016 Sushil Kumar Tripathi "An Efficient Block Cipher Encryption Technique Based on Cubical Method and Improved Key". They presented an efficient block cipher encryption techniques based on improved key. Proposed EES method is based on block level symmetric encryption. The proposed EES method is based on improve cubes. They used a pair of binary inputs are contains by each cell. The Cube can able to provide a various number of combinations. The proposed EES algorithm, performed a series of bit transformations, by using of S-BOX, operation XOR, and operation AND [11].

IV.SYMMETRIC APPROACH

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. A single key is used for both encryption and decryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. She represents various symmetric key algorithms in detail and then proposes a new symmetric key algorithm. Algorithms for both encryption and decryption are provided here. The advantages of this new algorithm over the others are also explained. [4] The proposed algorithm will be designed to compare with the symmetric approach given by Ayushi. [4]

Symmetric Key Cryptographic Algorithm

4.1 Encryption Algorithm

Step 1: Generate the ASCII value of the letter
Step 2: Generate the corresponding binary value of it. [Binary value should be 8 digits e.g. for decimal 32 binary number should be 00100000]
Step 3: Reverse the 8 digit's binary number
Step 4: Take a 4 digits divisor (>=1000) as the Key
Step 5: Divide the reversed number with the divisor
Step 6: Store the remainder in first 3 digits & quotient in next 5 digits (remainder and quotient wouldn't be more than 3 digits and 5 digits long respectively. If any of these are less than 3 and 5 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the cipher text i.e. encrypted text

4.2 Decryption Algorithm

Step 1: Multiply last 5 digits of the cipher text by the Key
Step 2: Add first 3 digits of the cipher text with the result produced in the previous step
Step 3: If the result produced in the previous step i.e. step 2 is not an 8-bit number we need to make it an 8- bit number
Step 4: Reverse the number to get the original text i.e. the plain text

V.PROPOSED APPROACH

5.1 Encryption Process

Step 1: Use ASCII 8 bit value letters.
Step 2: Inverse the odd position bits of the 8 bit element.
Step 3: Interchange bit for consecutive position
Step 4: Divide 8 bits into two part first four digits as element-1 and last four digits as element-2.
Step 5: Use 100 as key and divide and element-1 and element-2.
Step 6: Get the quotient-1, remainder-1 and quotient-2, remainder-2.
Step 7: quotient-1, remainder-2, quotient-2, and remainder-1
Step 8: Merge to get the 8 bit cipher text.

5.2 Decryption process

Step 1: Take the cipher text mark (right to left) first two bit as quotient-, next two bit as remainder-2, now next two quotient-2 and last two bit remainder-1.
Step 2: Multiply the quotient-1 with the key and then add the result with remainder-1 to get element-1. Similarly multiply the quotient-2 with the key and then add the result with remainder-2 to get element-2.
Step 3: Merge element-1 and element-2
Step 4: Interchange bit for consecutive position
Step 5: Inverse the odd position bits of the 8 bit element. And this will be our plain text which was encrypted.

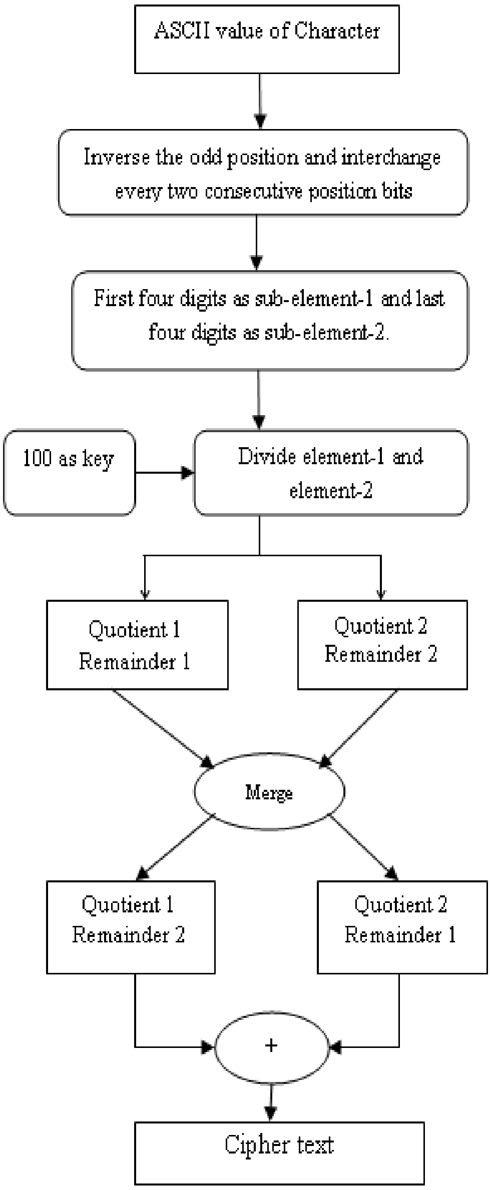
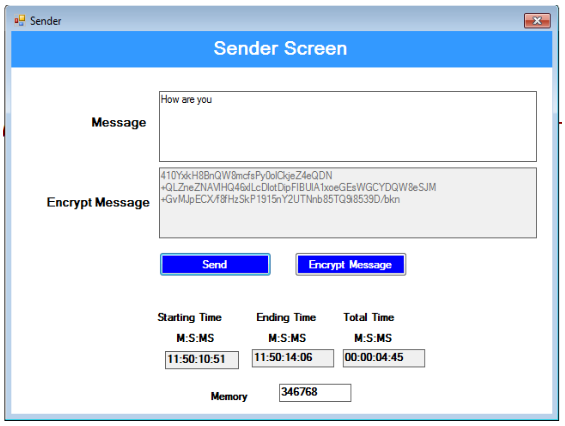

ASCII value of Character
Inverse the odd position and interchange every two consecutive position bits
First four digits as sub-element-1 and last four digits as sub-element-2.
100 as key
Divide element-1 and element-2
Quotient 1 Remainder 1
Quotient 2 Remainder 2
Merge
Quotient 1 Remainder 2
Quotient 2 Remainder 1
+
Cipher text

Figure.5. shows the architecture and flow of proposed algorithm.

VI. EXPERIMENTAL ANALYSIS

For experimental analysis, proposed algorithm with symmetric key algorithm has been implemented and compare with some parameter like key size, message size encryption, decryption time. The i3 pre-processor (2.5GHz Intel Processor with 4M cache memory) and 2GB main memory with Windows7 OS have been used. The algorithms are implemented in using C# Dot net frame work version 10. The simple text message including text only is used. Figure shows the encryption algorithm of the proposed method as sender screen. Decryption algorithm of the proposed technique as receiver screen is shown in figure 7.



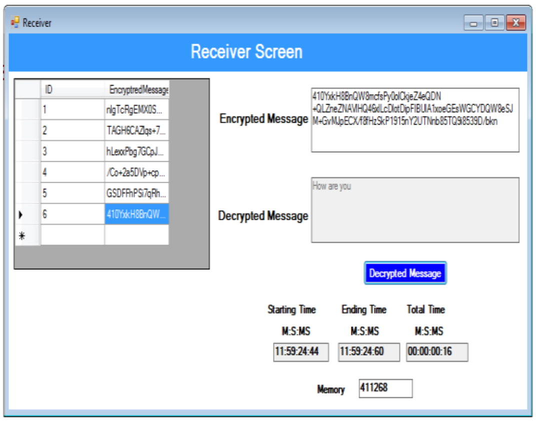
Message: How are you

Encrypt Message: 410YxkH8BnQW8mcfsPy0olCkjeZ4eQDN
+QLZneZNAVlHQ46xlLcDlotDipFIBUIA1xoeGEsWGCYDQW8eSJM
+GvMJpECX/f8fHzSkP1915nY2UTNnb85TQ9i8539D/bkn

Starting Time M:S:MS	Ending Time M:S:MS	Total Time M:S:MS
11:50:10:51	11:50:14:06	00:00:04:45

Memory: 346768

Figure 6 Sender Screen



	ID	EncryptredMessage
	1	nlgTcRgEMX0S...
	2	TAGH6CAZlqs+7...
	3	hLexxPbg7GCpJ...
	4	/Co+2a5DVp+cp...
	5	GSDFRhPSi7qRh...
▸	6	410YxkH8BnQW...
*		

Encrypted Message: 410YxkH8BnQW8mcfsPy0olCkjeZ4eQDN
+QLZneZNAVlHQ46xlLcDlotDipFIBUIA1xoeGEsWGCYDQW8eSJ
M+GvMJpECX/f8fHzSkP1915nY2UTNnb85TQ9i8539D/bkn

Decrypted Message: How are you

Starting Time M:S:MS	Ending Time M:S:MS	Total Time M:S:MS
11:59:24:44	11:59:24:60	00:00:00:16

Memory: 411268

Figure 7 Receiver Screen

VII.GRAPH COMPARATIVE ANAYSIS

On the basis of key size, message size (number of characters) and execution time for encryption has been compared. Table 1 shows comparison between symmetric approach and proposed method on the basis of file size and execution time for encryption. Figure 8 shows the comparisons graph for encryption. Table 2 shows comparison between symmetric approach and proposed method on the basis of key size in bytes for encryption. Figure 9 shows the comparisons graph for encryption.

Table.1. Time required for execution on message size

Message Size (number of characters)	Symmetric Approach (in milliseconds)	Proposed Approach (in milliseconds)
10	646	425
20	1024	848
50	2544	2062

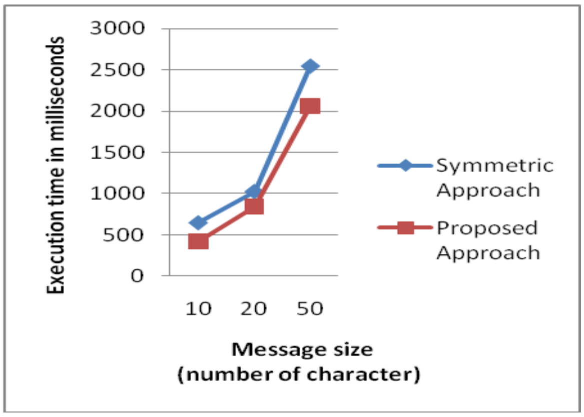


Figure.8. Comparisons graph for encryption using symmetric and proposed approach

Table. 1. Time required for execution on file

Approach	Key size (in bytes)
Symmetric Approach	64
Proposed Approach	48

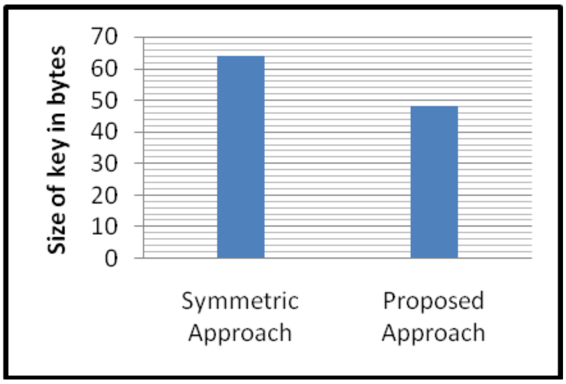


Figure.9. Comparisons graph with key size for symmetric and proposed approach

VIII. CONCLUSION

The proposed method is used for message communication. Short message can be send securely using encryption techniques. The proposed approach is based on number of characters in message and simple calculation and operations are performed to minimize the execution time. In future this work for special characters will be implemented.

IX. 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]. Ayushi "A Symmetric Key Cryptographic Algorithm" International Journal of Computer Applications (IJCA) ISSN : 0975 – 8887) Vol. 1 – No. 15 , February 2010. Available: http://www.ijcaonline.org/journal/number15/pxc387502.pdf

[5]. Suyash Verma, Rajnish Choubey, Roopali soni3“ An Efficient Developed New ymmetric Key Cryptography Algorithm for Information Security” International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012) Available: http://www.ijetae.com/files/Volume2 Issue7 /IJETAE_0712_03.pdf

[6]. Prerna Mahajan & Abhishek Sachdeva “A Study of Encryption Algorithms AES, DES and RSA for Security” Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350 Available: https:// globaljournals.org/GJCST_Volume13/4-A-Study-of-Encry ption-Algorithms.pdf

[7]. Anjula Gupta Navpreet Kaur Walia”Cryptography Algorithms: A Review” International Journal of Engineering Development and Research 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939 Available:https://www.ijedr. org/papers/ IJE DR 1402064.pdf

[8]. Reema Gupta “ Efficient Encryption Techniques In Cryptography Better Security Enhancement” Volume 4, Issue 5, May 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com Available:https://www.ijarcsse.com/docs/p a pers/Volume_4/5_May2014/V4I5-0450.pdf

[9]. Abhishek Joshi a*, Mohammad Wazid b, R. H. Goudarc “An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attacks” Available online at www.sciencedirect.comInternational Conference on Intelligent Computing, Communication& Convergence (ICCC-2014)Conference Organized by Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India Available: http://www.s cience direct.com/science/article/pii/S1877050915007036

[10] Ashraf Odeh, ShadiR.Masadeh, Ahmad Azzazi “A Performance Evaluation Of Common Encryption Techniques With Secure Watermark System (SWS)”International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015. Available: http://a irccse.org /journal/ nsa/7315nsa03.pdf

[11] Sushil Kumar Tripathi “An Efficient Block Cipher Encryption Technique Based OnCubical Method and Improved Key” Imperial Journal of Interdisciplinary Research (IJIR)Vol-2, Issue-6, 2016ISSN: 2454-1362, Available: http://www. Imp eria ljournals.com/index.php/IJIR/article/view/836

[12]Sanidhya U, Shrikanth N.G “An Efficient Encryption And Searching Technique For Cloud Using Rijndael Algorithm” International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 4, Issue 3 (May-June, 2016), PP. 262-267 Available: http://www.ijtra.com/ abst ract.php?id=an-efficient-encryption-and-searching-technique-for-cloud-using-rijndael-algorithm