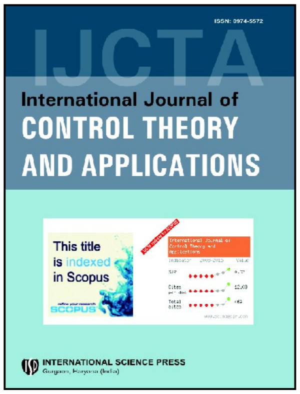

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 29 • 2017

Block Key Based Encryption and Decryption Techniques using MBC for Text Data

R. Sankara Subramanian[1] and S. Sukumaran[2]

[1] Ph.D. (Research Scholar), Dept. of Computer Science, Erode Arts and Science College, (Autonomous), Erode, Tamil Nadu, India -638009, E-mail: rsankarprofessor@gmail.com
[2] Associate Professor, Dept. of Computer Science, Erode Arts and Science College (Autonomous), Erode, Tamil Nadu, India -638009, E-mail: prof_sukumar@yahoo.co.in

Abstract: In this paper, a new technique has been developed for mapping the text using Matrix Base Conversion (MBC). MBC considered the input plain text into ASCII values. A symmetric algorithm is developed for encryption and decryption using same key at the sender and receiver end. In this algorithm the input string is first converted into its ASCII values. It performs a string manipulation algorithm which will change the relative position of atomic data values by reversing them. Here, divide the string into square matrices of maximum possible order and then add magic square matrix of same size is considered. The base conversion is performed on the basis of key which is calculated by the size of square matrix generated. The base conversion is also performed on the remaining elements which could not be containing in the square matrices. The experimental result shows that this MBC provides better for encrypting and decrypting the text file when compared with the existing methods such DES and Blowfish.

Keywords: MBC, DES, Blowfish, ASCII, Encryption, Decryption.

1. INTRODUCTION

Cryptography is commonly employed security concepts and terminology. The concern for security in practice is addressed by choosing a security protocol, which achieves all the required security objectives. Security protocols realize the security objectives through the use of appropriate cryptographic algorithms. Basic security terminologies used in cryptography are, a message present in a clear form, which can be understood by any casual observer, is known as the plaintext. The processes of encryption and decryption are controlled on a quantity known as the key, which is ideally known only to the valid users. Strength of a security scheme depends on the secrecy of the keys used.

Symmetric Encryption

In Symmetric cryptography, same key is used for encryption and decryption. Key plays an important role in cryptography. The key should be distributed before transmission between two parties. The strength of symmetric key encryption depends on the size of the key. Data can be easily decrypted if a weak key is used in the algorithm. There are various symmetric key algorithms such as DES, 3DES , AES , RSA ,Blowfish.

Asymmetric Encryption

The problem of key distribution is solved by asymmetric key encryption. In asymmetric key encryption, two different keys are used for encryption and decryption - public and private key. The public key of the receiver is used to encrypt the plain text and only the authorized person can be able to decrypt the cipher text through his own private key. Private key is kept secret.

2. RELATED WORKS

Ravi *et al.,* [1] proposed bit shifting and stuffing method stuffing a new bit in the place of unused bit which is shifting from another printable character. After the encryption bit shifting and stuffing for every eight bytes of plain text it will generate seven bytes cipher text and in decryption for every seven bytes of cipher text it will reproduce eight bytes of plaintext.

Santhosh *et al.,* [2] proposed Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers algorithm contains two levels of Exclusive OR operation. The algorithm is useful in transmission of messages and data between one user and another.

Ezeofor *et al.,* [3] presented analysis of network data encryption and decryption techniques used in communication systems. In the Basic simulation program that encrypt and decrypt data are analyzed with different data block sizes.

Obaida *et al.,* [4] developed a new approach for complex encrypting and decrypting Data maintains the security on the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption and decryption.

Satyajeet *et al.,* [5] presented a symmetric cryptographic algorithm for data encryption and decryption based on ASCII values of characters. The secret key is converted to another string is used as key to encrypt or decrypt the data.

Arora *et al.* [6] studied about the performance of different security algorithms on a cloud network and with different inputs. In this work find the Speed-Up Ratio for implementing security algorithms (RSA, MD5 and AES) are used by business with large volumes data are encrypted.

Seth *et al.* [7] comparatively analyzed RSA, DES and AES considering certain parameters are the major issue of concern in any Encryption Algorithm. From the results DES algorithm consumes least encryption time and AES algorithm has least memory usage and RSA consume longest encryption time and memory usage is also very high.

Abdul. Elminaam *et al.* [8] studied about the performance of Symmetric Encryption Algorithms conducted no significant difference when the results are displayed either in hexadecimal base encoding. The changing packet size RC6 requires less time than all algorithms except Blowfish. By changing key size is higher change in the battery and time consumption.

Mandal *et al.* [9] compared data encryption standard and advanced encryption standard techniques on the basis of avalanche effect. The property of any encryption algorithm in which a small change in either the key or the plaintext should produce a significant change in the cipher text.

3. EXISTING METHODOLOGY

3.1. RSA

Ron Rivest, Adi Shamir and Leonard Adleman [10] developed in 1978. It is a public key cryptosystems for key exchange blocks of data. RSA has variable size encryption block with variable size key. RSA is asymmetric cryptosystem based on number theory has block cipher system. To generate the public and private keys used for encryption and decryption purpose. Sender encrypts the message using Receiver public key and then message transmitted to receiver, then receiver can decrypt it. RSA have many errors in design it not preferred for commercial purpose.

3.2. Data Encryption Standard

IBM developed in 1970s after it adopted by the National Institute of Standards and Technology (NIST). Data Encryption Standard (DES) [11] is block Cipher which is developed to encrypt and decrypt blocks of data consisting of 64 bits. The input key for DES is 64 bits long and the actual key 56 bits in length are used. The least significant bit in each byte is parity bit and should be always an odd number of 1s in every byte. The algorithm has 16 iterations that interface the blocks of plaintext values obtained.

3.3. Blowfish

Bruce Schneier developed Blowfish algorithm in the year 1993 [12]. Blowfish is a 64 bit block cipher with variable length key from 32 bit (4 bytes) to 448 bits (56 bytes). The advantage of this algorithm is that it is highly secure and has not been cracked yet. It is suitable and efficient for hardware implementation.

4. PROPOSED METHODOLOGY

The technique of converting a given number from one number system to another by means of simple calculations is known as Matrix Base Conversion. A square matrix in which the sum of all elements in each column and in each row is same is called Magic Square matrix. To calculate the sum use the formula $(r* (r^2+1))/2$, where r is the size of square matrix. A square matrix order refers to a matrix with equal number of rows and columns.

5. ALGORITHM

// Algorithm for Encrypting Text **//**
Input: Plain Text
Output: Cipher text

Step 1 : To calculate the length of input string and assign variable X.

Step 2 : Each element in input string is converted into ASCII value.

Step 3 : If length of the string is even then the string is equally divided into two parts using the left substring and right substring.

Step 4 : If the length of the string is odd then middle most elements is kept unchanged with left substring and right substring respectively.

Step 5 : Reverse the right substring and then repeat step3 and step4 until the derived two substrings more than 3 elements in each substring.

Step 6 : Break the input string into square matrices of maximum possible size of odd order, minimum being 3x3 and place the remaining elements into variable REM.

Step 7 : Repeat this step using remainder REM of this step as input string, until there are 9 or more elements in REM.

Step 8 : Then, place the elements in REM into a square matrix of order 3x3.

Step 9 : Initialize the unoccupied positions by NULL.

Step 10 : Calculate the key as number of columns of all the matrices including 3 for REM by using this key calculate the Base using key-base table.

Step 11 : Adding magic square matrix of size same as that of matrix under considered to matrix. Repeat this step for all the matrices including matrix formed by REM.

Step 12 : Finally, last step merge all the elements of all square matrices, including matrix of REM in the order they were derived. To take only remainder values of REM, not all values.

Step 13 : Then perform base conversion on this merged string to get the cipher text.

// Algorithm for Decrypting Text **//**

Input: Cipher Text

Output: Plain Text

Step 1 : To calculate the length of input string and assign variable X.

Step 2 : Break the input string into square matrices of maximum possible size of odd order, minimum being 3x3 and place the remaining elements into variable REM.

Step 3 : Repeat this step using remainder REM of this step as input string, until there are 9 or more elements in REM.

Step 4 : Then, place the elements in REM into a square matrix of order 3x3.

Step 5 : Initialize the unoccupied positions by NULL.

Step 6 : Calculate the key as number of columns of all the matrices including 3 for REM by using this key calculate the Base using key-base table.

Step 7 : Perform base to decimal conversion on all matrices including matrix for REM.

Step 8 : Subtract magic square matrix of size same as that of matrix under considered to matrix. Repeat this step for all the matrices including matrix formed by REM.

Step 9 : Finally, last step merge all the elements of all square matrices, including matrix of REM in the order they were derived. To take only remainder values of REM, not all values.

Step 10 : Then perform reverse the string operation.

6. EXPERIMENTS & RESULTS

The proposed method is experimented with a different types of text file has process using MATLAB. The table 1.1 shows the comparison values of Encryption and Decryption time.

Table 6.1
Key-Base Table

Key	1	2	3	4	5	6	7	8	9
Base	5	6	7	8	9	8	7	6	5

Input Text

BHARTHIAR UNIVERSITY, COIMBATORE, TAMILNADU

ERODE ARTS & SCIENCE COLLEGE, (AUTONOMOUS)

String Length X = 42

Table 6.2
Comparison Encryption and Decryption Time

Method	*RSA [13]*		*DES*		*MBC*	
File	*Enc Time*	*Dec Time*	*Enc Time*	*Dec Time*	*Enc Time*	*Dec Time*
File01.txt	0.45	0.31	0.12	0.67	0.10	0.22
File02.exe	0.50	0.33	0.10	1.10	0.25	0.07
File03.dll	0.32	1.01	1.01	1.15	0.18	0.93
File04.doc	0.54	0.21	2.01	2.14	0.31	0.14
File05.html	0.48	1.02	3.13	4.09	0.19	0.91

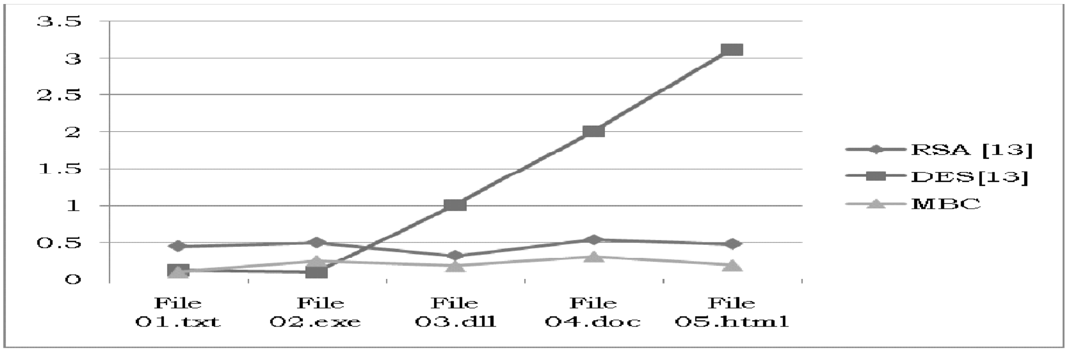

Figure 1.1: Encryption Time

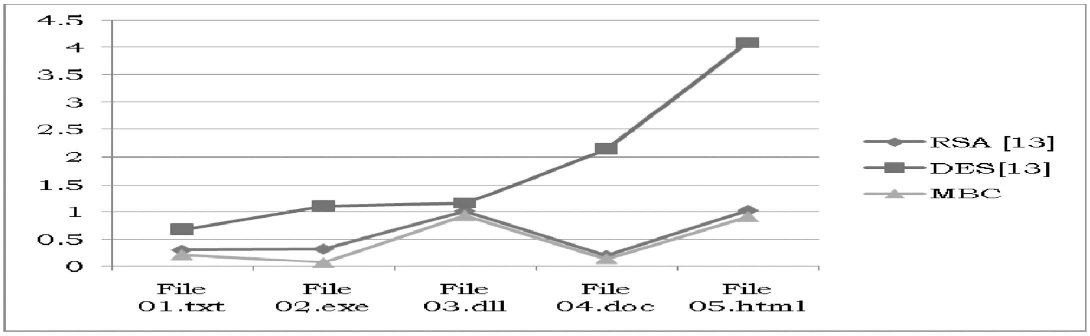

Figure 1.2: Decryption Time

Table 6.3
Bit ratio Comparison

File	*File Size*	*RSA [13]*	*DES[13]*	*MBC*
File01.txt	1.80	45.40	47.57	41.12
File02.exe	3.80	44.90	46.43	42.56
File03.dll	8.50	45.10	47.30	45.30
File04.doc	12.58	44.00	44.00	46.65
File05.html	27.00	45.10	46.80	45.03

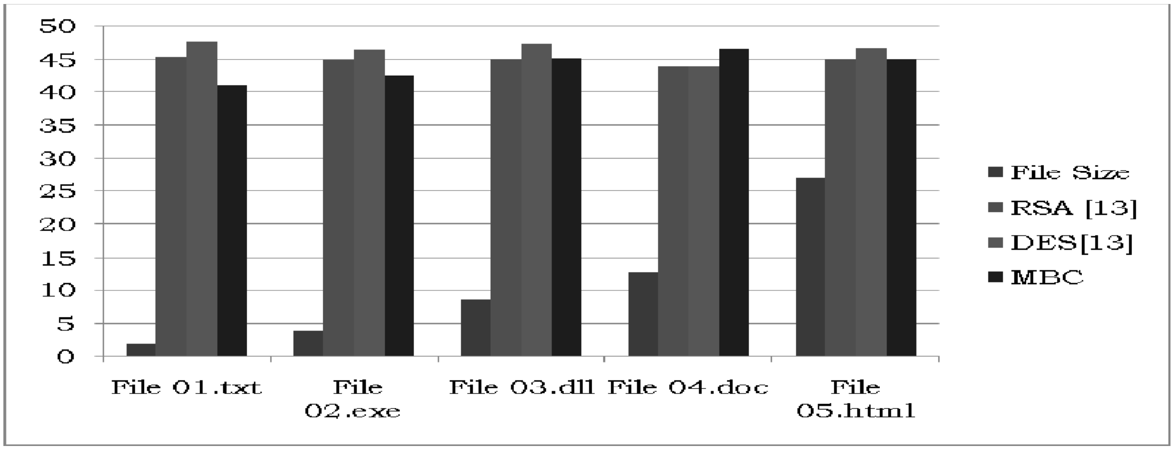

Figure 1.3: Bit Ratio

7. CONCLUSION

In this proposed work, described the concept of divide and conquer to encrypt the input string into cipher text. The string is deformed by using different string reversal operation by using base conversion algorithm dynamically, the base depends on the key is calculated and it depends on the input string. It reduces the probability of hacking string. The magic square matrix is used to increase the randomness among the element of the string. In this work, eliminates the problem of sequencing and number of occurrence of the varied characters. The experimental result proves the MBC provides better encryption and decryption when compared to existing methods. The performances of MBC method when compared to existing methods such as RSA, DES and Blowfish are investigated independently. Moreover, the computational cost of the algorithm is very low compared with existing methods.

REFERENCES

[1] B. Ravi Kumar, P.R.K.Murti Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology, International Journal on Computer Science and Engineering, Vol.3 no.7, 2011.

[2] Santhosh Reddy, owjanya, P. Praveena, Shalini L, Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers International Journal of Scientific and Research Publications, Volume 2, Issue 9, 2012.

[3] Ezeofor C. J., Ulasi A. G "Analysis of Network Data Encryption &Decryption Techniques in Communication Systems" International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 12, 2014.

[4] Obaida Mohammad Awad Al-Hazaimeh, A New Approach For Complex Encrypting and Decrypting Data International Journal of Computer Networks & Communications,Vol.5, No.2, 2013.

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

[6] Priyanka Arora, Arun Singh and Himanshu Tiyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal, Vol. 2, No.5, pp. 179-183, 2012.

[7] Shashi Mehrotra Seth, Rajan ishra, "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, 2011.

[8] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", International Journal of Computer Science and Network Security, Vol.8 No.12, pp. 280-286, 2008.

[9] Akash Kumar Mandal, Chandra Parakash and Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.

[10] Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, pp. 1118 – 1121, 2011.

[11] Sriram Ramanujam and Marimuthu Karuppiah, "Designing an algorithm with high Avalanche Effect", IJCSNS International Journal of Computer Science and Network Security, Vol.11, No.1, pp. 106-111, 2011.

[12] Pratap Chnadra Mandal "Superiority of Blowfish Algorithm," International Journal of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.

[13] Sukalyan Som, Mohit Kundu, Sabyasachi Ghosh, "A Simple Algebraic Model based Polyalphabetic Substitution Cipher", International Journal of Computer Applications, Volume 39, No.8, 2012.

[14] WilliamStallings, Cryptography and Network Security, 5th Edition, Person Education, 2011.