A New Method in Symmetric Encryption for block cipher module: A Bit Shifting Approach

Hari Krishan Soni
School of Information Technology
RGPV,Bhopal (M.P.) India,

Dr. Sanjeev Sharma
School of Information Technology
RGPV,Bhopal (M.P.) India,

Prof. SantoshSahu
School of Information Technology
RGPV,Bhopal (M.P.) India,

ABSTRACT
Most of the sensitive information in the data communication has latent security problems. The algorithm method of AES, DES, 3DES and RC2 which were widely used are not suitable for the coding of advanced language tools. Therefore, we proposed the mixed encryption algorithm based on bit shifting and matrix calculation to solve the problem. Our method is easy to adopt the coding of advanced language and is safe enough. The security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those know the secret key. The proposed algorithms consume very less amount of computing resources such as CPU time, memory and battery power [18]. Our implementations also showed the highest throughputs for all type of files and file size and comparison has been conducted with AES, DES, 3DES,RC2 [1] and result shows the effectiveness and speed of our algorithm.

Keywords: AES, DES, 3DES, RC2 Computer Security, Encryption Techniques, Cryptography

1. INTRODUCTION
The information security might be defined as "Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure" [19]. But why is it important to secure information? In today's high technology environment, organizations are becoming more and more dependent on their information systems. The public is increasingly concerned about the proper use of information, particularly personal data. The threats to information systems from criminals and terrorists are increasing. Many organizations will identify information as an area of their operation that needs to be protected as part of their system of internal control.

For secure communication over public network data can be protected by the method of encryption. Encryption converts that data by any encryption algorithm using the 'key' in scrambled form. Only user having access to the key can decrypt the encrypted data. Encryption is a fundamental tool for the protection of sensitive information. The purpose to use encryption is privacy (preventing disclosure or confidentiality) in communications. Encryption is a way of talking to someone while other people are listening, but such the other people cannot understand what you are saying [18]

Following are some necessary security principles are required when two applications are exchanging the information.

Confidentiality- The principle of confidentiality specifies that only the sender and the intended recipient(s) should be able to access the contents of a message.

Integrity- When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.

Authentication- The authentication process ensures that the origin of an electronic message or document is correctly identified.

Non-repudiation- There are situations where a user sends a message and later on refuses that she/he had sent that message. Non-repudiation does not allow the sender of a message to refuse the claim of not sending that message.

Availability- The principle of availability states that resources should be available to authorized parties at all times. Interruption puts the availability of resources in danger.

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA).Public key encryption is biased on mathematical function, computationally intensive and is not very efficient for small mobile devices [19].When the amount of data is very small, then evensome efficient algorithms prove to be obsolete. They takemore amount of time than usual to compute this smallamount of data. Hence a special algorithm, which is amodification to the trivial symmetric key algorithm, is to beused.

This paper examines a method for evaluating performance of selected symmetric encryption of various algorithms. Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. Battery power is subjected to the problem of energy consumption due to encryption algorithms.

This study evaluates five different encryptionalgorithms namely; AES, DES, 3DES, RC2, and proposed algorithm. The performance measure of encryptionschemes will be conducted in terms of encryption time taken by each algorithm,changing packet size andchanging key size for the selected cryptographicalgorithms.

This paper is organized as follows.Section 2 will briefly discuss the encryption algorithms used in our paper i.e. AES,DES,3DES and RC2. Related work is discussed in Section 3. The section 4 describes the proposed algorithm. In section 5 result analysis is performed. We conclude briefly in section 6.

2. OVERVIEW OF ENCRYPTION ALGORITHM

The cryptographic techniques can be categorized as shown in the following figure.

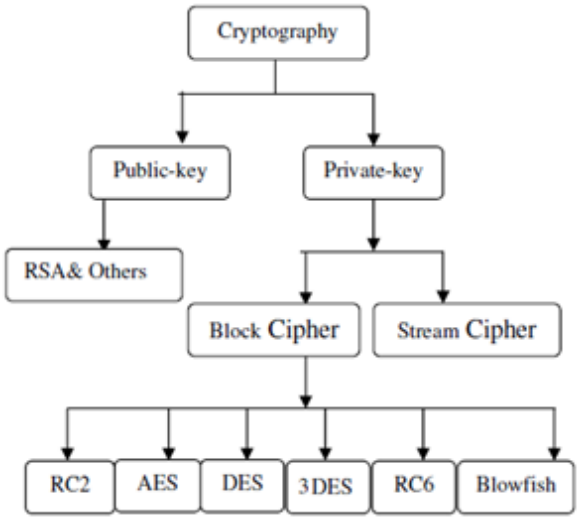

Fig.1. Different Cryptographic Techniques

Brief definitions of the most common encryptiontechniques are given as follows:

AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. it encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications [14].

DES: (Data Encryption Standard), was the firstencryption standard to be recommended by NIST(National Institute of Standards and Technology).DESis (64 bits key size with 64 bits block size). Since thattime, many attacks and methods recorded theweaknesses of DES, which made it an insecure blockcipher [14].

3DES is an enhancement of DES; it is 64 bit blocksize with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods [14].

RC2 is a block cipher with a 64-bits block cipher with a variable key size that range from 8 to128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts [14].

3. RELATED WORK

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources.

It was shown in [1] that energy consumption of different common symmetric key encryptions on handheld devices. It is found that after only 600 encryptions of a 5 MB file using Triple-DES the remaining battery power is 45% and subsequent encryptions are not possible as the battery dies rapidly.

A study in [19] is conducted for different popular secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on two different hardware platforms, to compare their performance. They had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data [20].

4. PROPOSED TECHNIQUES

Internet and networks applications are growing very fast, so the requirements to protect such applications are increased. Encryption algorithms play an important role in information security systems. Our method is easy to adopt the coding of advanced language and is safe enough on the other side; AES, DES, 3DES, RC2 algorithms consume a large amount of computing resources such as CPU time, memory, and battery power. We provide comparison of four of the most common encryption algorithms namely: AES, DES, 3DES, RC2, with our proposed algorithm. Comparison has been conducted for different file types and file sizes and exper-imental results are given to demonstrate the effectiveness of each algorithm.

A. *Key Generation Method*:

In order to provide quick and simpleencryption/decryption, the bits size of the secret key has tobe chosen effectively. For encrypting small amountof data, there should not be any overhead to the encryptingsystem as well as there should not be any compromise on thesecurity level. Thus an optimized size of 64 bits is chosen.

Steps for key generation:

Step 1: Select a Key called "K"
Step 2: Choose first eighteen characters from Key "K".
Step3: If it is less than 18 character then fills remaining character as "a".
Step 4: Construct two square matrixes of 3X3 and fill thatmatrixes with keyvalue c_1, c_2up to$c_9$in the following manner (where c_1 means first characterof key, and so on)

KeyMatrix"KM_1"=

c_1	c_2	c_3
c_4	c_5	c_6
c_7	c_8	c_9

Andc_{10}, c_{11} up to c_{18} in following manner

Key Matrix"KM_2" =

c_{10}	c_{11}	c_{12}
c_{13}	c_{14}	c_{15}
c_{16}	c_{17}	c_{18}

Step 5: Convert the key value into respective ASCII value of bothKM_1andKM_2 matrixes.
Step 6: Multiply $KM_1$and KM_2 and generate a new matrix KM_3 (i.e. $[KM_3] = [KM_1]*[KM_2]$) Say the corresponding multiplication value is$i_1, i_2 \ldots i_9$

KM_3 =

i_1	i_2	i_3
i_4	i_5	i_6
i_7	i_8	i_9

Step 7: Calculate the addition of rows and find three values as follows:

$K1= i_1 + i_2 + i_3$
$K2=i_4 +i_5 +i_6$
$K3= i_7 +i_8 + i_9$

Step 8: This is the final key step

K =K1 * (10)6 + K2 * (10)3 + K3

K= K1 K2 K3
K= K MOD (10)9
K = {X1,X2,X3,X4,X5,X6,X7,X8,X9}

B. *Proposed Encryption Algorithm*:

Symmetric cryptography involves two parties who share a joint secret or key. This exclusiveknowledge of the key enables private and securecommunication between the two parties, without the threat of a third party eavesdropping or otherwisetampering with messages in transit.

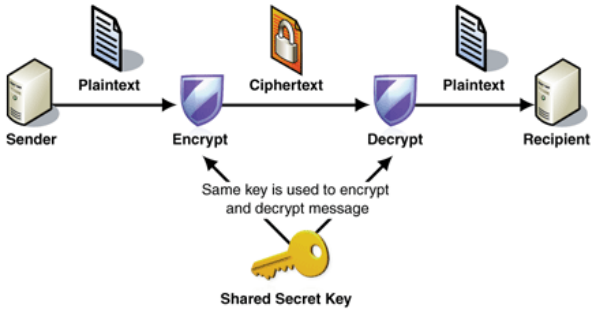

Figure-4.1: Symmetric Key Cryptography

In this instance, the same key is used for encryption and decryption. Contrast this with public key cryptography, which utilizes two keys a public key to encrypt messages and a private key to decrypt them. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. Symmetric key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way.Public key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted. Symmetric key cryptography is sometimes called secret-key cryptography.

C. *Steps for Encryption Algorithm:*

Step 1: Select first 8 character of message.
Step 2: Convert into ASCII values.
Step 3: Convert into binary number.
Step 4: Insert filler bit (B) depend upon the character position in the selected message i.e. $b_1, b_3, b_5, b_7 = 0$And$b_2, b_4, b_6, b_8 = 1$where
$b_1, b_2, b_3, b_4, b_5, b_6, b_7,$ and $b_8$is the respective bit position in the selected message.
Step 5: Now these numbers will be converted into 3X3 matrixes.
Step 6: Insert another filler 3X3 matrix at end filled with $b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8$and 0
.

b_1	b_2	b_3
b_4	b_5	b_6
b_7	b_8	0

Step 7: Convert this 3 X 27 matrix into 9 X 9 matrixes.
Step 8: Now Shift first row and first column according to first value of key K i.e.X1 and repeat this process for all other rows, columns according to respective key valueX2, X3,up to X9.
Step 9: Final step we convert this 81 binary number into 8X10 and 1X1 total 11 binary numbers and convert into character.

5. Results

The following table shows the encryption time taken by different size of data block.

File Size (KB)	AES	3DES	DES	RC2	PA
49	56	54	29	57	3
100	90	81	49	91	3
247	112	111	47	121	4
321	164	167	82	168	5
694	210	226	144	262	7
899	258	299	240	268	8
963	208	283	250	295	8.9

5345	1237	1466	1296	1570	283
7310	1366	1786	1695	1915	340
Time	3701	4473	3832	4747	663
Throughput	4.30	3.56	4.16	3.36	24.02

Table-5.1 Average Encryption Time (in milliseconds)and Throughput of Cryptography algorithms

The following graph shows the time taken by different encryption techniques on different packet size.

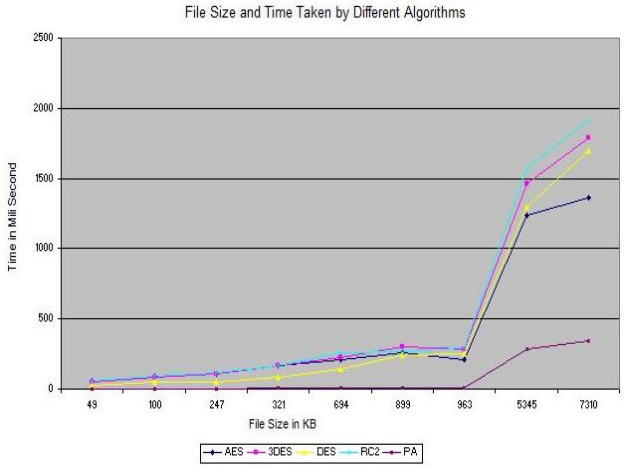

Fig 5.1 Time consumption of encryption algorithm

Encryption time is used to calculate the throughput ofan encryption scheme. The throughput of the encryption scheme is calculated by dividing the total plaintextin kilobytes encrypted on the total encryption timefor each algorithm in. As the throughput value is increased,the power consumption of this encryption technique is decreased. The following figure shows the throughput of each algorithm.

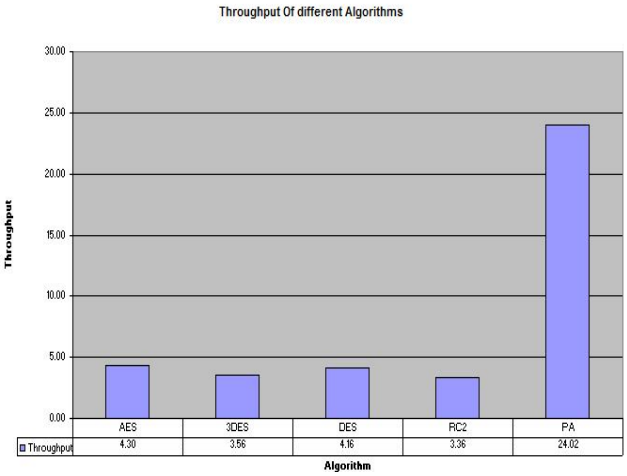

Fig 5.2 Throughput of each encryption algorithm

6. CONCLUSION

Encryption algorithm play an important role in communication security where encryption time, Memory usages output byte and battery power are the major issue of concern. This paper presents a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, 3DES, DES and RC2 With the proposed algorithm. Several points can be concluded from the Experimental results. Based on the text files used and the experimental result it was concluded that our proposed algorithm consumes least encryption time and RC2 has taken maximum time in encryption for same amount of the data.

7. REFERENCES

[1] DiaaSalamaAbdElminaamHatem Mohamed AbdualKade, and Mohiy Mohamed Hadhoud "Evaluating The Performance of Symmetric Encryption Algorithms" International Journal of Network Security, Vol.10, No.3, PP.213 - 219, May 2010

[2] D.Coppersmith, "The data encryption standard (DES) and its strength against attacks", IBM Journal of Research and Development, pp. 243 -250, May 1994.

[3] J. Daemen, and V. Rijmen, "Rijndael: The advanced encryption standard," Dr. Dobb's Journal, pp. 137139, Mar. 2001.

[4] Introduction to cryptography, Part 2: Symmetric cryptography, available at http://www.ibm.com/developerworks/library/s-crypt02 /index.html

[5] Xiaolin Wang, Guoqin Chen, Jianqin Zhou "A note on linear transformations in cryptography" 2009 International Symposium on Information Engineering and Electronic Commerce, 978-0-7695-3686-6/09.

[6] N. E. Fishawy, "Quality of encryption measurement of bitmap images with RC6, MRC6, and rijndael block cipher algorithms," International Journal of Network Security, pp. 241-251, Nov. 2007.

[7] An introduction to PKI, available at: http://www.carillon.ca/library/pkitutorial.php

[8] Hardjono, Security In Wireless LANS And MANS, Artech House Publishers, 2005. International Journal of Network Security,vol.10, No.3, PP.213–219, May 2010

[9] M. S. Hwang and C. Y. Liu, "Authenticated encryption schemes: current status and key issues," International Journal of Network Security, vol. 1, no. 2, pp. 61-73, 2005.

[10] M.H. Ibrahim, "A method for obtaining deniable public-key encryption", International Journal of Network Security, vol. 8, no. 1, pp. 1-9, 2009.

[11] M. H. Ibrahim,"Receiver-deniable public-key encryption", International Journal of Network Security, vol. 8, no. 2, pp. 159-165, 2009.

[12] S. Z. S. Idrus, and S. A. Aljunid, "Performance analysis of encryption algorithms text length size on web browsers", IJCSNS International Journal of Computer Science and Network Security, vol. 8, no.1, pp. 20-25, Jan. 2008.

[13] P. Ruangchaijatupon, and P. Krishnamurthy, "Encryption and power consumption in wireless LANs-N," The Third IEEE Workshop on Wireless LANs, pp. 148-152, Newton, Massachusetts, Sep. 27-28, 2001.

[14] W. Stallings, Cryptography and Network Security, Prentice Hall, pp. 58-309, 4th Ed, 2005.

[15] A. A. Tamimi, Performance Analysis of Data Encryption Algorithms, Retrieved Oct. 1, 2008. (http://www.cs.wustl.edu/jain/cse56706/ftp/encryptionperf/index.html)

[16] PrakashKuppuswamy et al./ Indian Journal of Computer Science and Engineering (IJCSE) " Enrichment of security through cryptographic public key algorithm based on block cipher"

[17] An introduction to information security, available: http://openlearn.open.ac.uk/mod/oucontent/view.php?id=397613&section=1

[18] IJCST Vol. 2, Issue 2, June 2011 I S SN : 2 2 2 9 - 4 3 3 3 (P r i n t) | I S S N : 0 9 7 6 - 8 4 9 1 (On l i n e) "Comparative Analysis Of Encryption Algorithms For Data Communication"ShashiMehrotra Seth, Rajan Mishra"

[19] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005, First International Conference, 2006-02-27,P.P. 84- 89.

[20] Results of comparing tens of encryption algorithms using different settings- Crypto++ benchmark-. Retrieved October 1, 2008, from: http://www.eskimo.com/~weidai/benchmarks.html