A Hyper Modern Cryptography Algorithm to Improved Data Security: HMCA

Vishwa Gupta
M.Tech(SE) Scholer,
SSSIST ,Shehore
vishwa.gupta80@gmail.com

Gajendra Singh
Head CSE,
SSSIST,Shehore
Gajendrasingh86@rediffmail.com

Ravindra Gupta
Ravindra_P84@rediffmail.com

Abstract: In this paper, we propose an improved block cipher symmetric encryption algorithm that has the same structure of encryption and decryption. So far, conventional cryptography algorithms have difference structure of encryption and decryption. We devise our algorithm by inserting a symmetric layer using random number, encryption number and XOR operations, in which the whole proposed algorithm rounds uses encryption procedure and the same for it decryption procedure. The symmetry layer is put between encryption part and decryption one. The proposed algorithm has the batter speed compared with the comparing encryption algorithm. Nevertheless, the proposed algorithm improves encryption security by inserting the symmetric layer. The proposed algorithm will be useful to the applications which require the same procedure of encryption and decryption.

Keywords: Information security, Encryption, Decryption, Cryptography

To write this paper I have Study about information security using cryptography technique. I have study of detailed description of cryptography technique that what is cryptography, how it's working, advantage and disadvantage and more important thing security of information over public network. I have also study of various cryptography algorithms; important loop hole of security of information in public Network and how I can improve to those loop holes. What will we the approach of our research work and many more?

After the detailed study of Network security using cryptography, I am presenting my proposed work. This paper is dividing in four sections. In section-I, I am presenting just basic introduction about Information Security using cryptography, in section-II, I am presenting detailed description of Information security using cryptography and various algorithms, in section-III, I am presenting my proposed algorithm, and in section IV I am Presenting summary and references where I have completed my research.

Section – I
INTRODUCTION

The main feature of the encryption/decryption program implementation is the generation of the encryption key. Now a day, cryptography has many commercial applications. If we are protecting confidential information then cryptography is provide high level of privacy of individuals and groups. However, the main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation. Cryptography is the methods that allow information to be sent in a secure form in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity. Figure 1 is representing conventional encryption model.

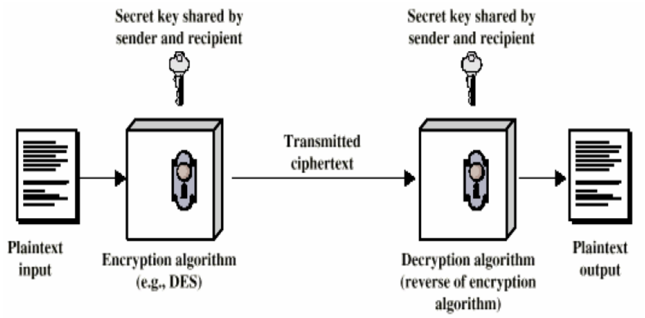

Figure 1: A Simplified Model of Conventional Encryption

Security Services: If we are taking about security of information then following services come in mind.

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)

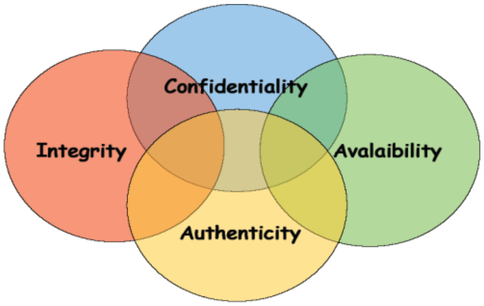

Figure 2: Security Services

Most important security services are shown in figure 2.

Terminology on Cryptography:-

Ciphers vs. Codes: Ciphers are based on the individual characters in a message, and generally translate letter to another letter or symbol. On the other hand, codes translate whole words or phrases where "hello" could be the code for "tomto" or "my self this" could be code for "yes you can do".

Cryptography vs. Steganography: Cryptography and steganography are also regularly confused. Steganography involves concealing the existence of a message such as invisible inks or messages buried within other messages. Cryptography does not conceal the fact that a message exists; cryptography conceals the meaning of the message from those who do not know how to decipher it.

Section – II

Here a newly developed technique named, "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" [1] is discussed. In this they are suggesting a symmetric key method where they have used a random key generator for generating the initial key and that key is used for encrypting the given source file. In this method basically a substitution method where they take 4 characters from any input file and then search the corresponding characters in the random key matrix file after getting the encrypted message they store the encrypted data in another file. For searching characters from the random key matrix they have used a method which was proposed by Nath in MSA algorithm. In that they have the provision for encrypting message multiple times. The key matrix contains all possible words comprising of 2 characters each generated from all characters whose ASCII code is from 0 to 255 in a random order. The pattern of the key matrix will depend on text key entered by the user. They are proposing their own algorithm to obtain randomization number and encryption number from the initial text key. they have given a long trial run on text key and they have found that it is very difficult to match the above two parameters from 2 different Text key which means if some one wants to break his encryption method then he/she has to know the exact pattern of the text key. To decrypt any file one has to know exactly what is the key matrix and to find the random matrix theoretically one has to apply 65536! trial run and which is intractable. They have apply method on possible files such as executable file, Microsoft word file, excel file, access database, FoxPro file, text file, image file, pdf file, video file, audio file, oracle database and they have found in all cases it giving 100% correct solution while encrypting a file and decrypting a file. This method can be used for encrypting digital signature, watermark before embedding in some cover file to make the entire system full secured. In the following section we are going in detail.

Here another newly developed technique named, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" [09] is discussed. In this method they describe about symmetric cipher algorithm which is much more similar to Rijndael. The difference is that, Rijndael algorithm start with 128 bits block size, and then increase the block size by appending columns[10], whereas his algorithm start with 200 bits. In the following section we are going in details.

General Definitions: The intermediate cipher result is called the State. The State can be pictured as a rectangular array of bytes. This array has five rows; the number of columns is denoted by Nb and is equal to the block length divided by 40. They know that the security is the function of block length and the size of key length, so they increase the block length as well as the key length. Basically block length is 200 bits which can be shown as a 5 by 5 matrix of byte. This is illustrated in figure1.in this they are increasing block by appending a column at a time. But they like to emphasize on 200 bit and then compare the security & efficiency between his 200 bits block cipher and Rijndael 128 bits cipher. The input and output used by suggested algorithm at its external interface are considered to be one dimensional arrays of 8-bit bytes numbered upwards from 0 to the 5*Nb-1.The Cipher Key is considered to be a one-dimensional arrays of 8-bit bytes numbered upwards from 0 to the 5*Nk-1.The cipher input bytes (the "plaintext" if the mode of use is ECB encryption) are mapped onto the state bytes in order a0,0, a1,0, a2,0, a3,0, a4,0, a0,1, a1,1, a2,1, a3,1, a4,1 ... , and the bytes of the Cipher Key are mapped onto the array in the order k0,0, k1,0, k2,0, k3,0, k4,0, k0,1, k1,1, k2,1, k3,1, k4,1 ... At the end of the cipher operation, the cipher output is extracted from the state by taking the state bytes in the same order.

Hence if the one-dimensional index of a byte within a block is n and the two dimensional index is (i ,j), we have: $i = n \bmod 5$; $j=\lfloor n/5 \rfloor$; $n=i+5*j$

Section - III

PROPOSED WORK

In this section I am presenting a new block based symmetric cryptography algorithm. In this technique I am using a random number for generating the initial key, where this key will use for encrypting the given source file using proposed encryption algorithm with the help of encryption number. Basically In this technique a block based substitution method will use. In the present technique I will provide for encrypting message multiple times. The proposed key blocks contains all possible words comprising of number (n) of characters each generated from all characters whose ASCII code is from 0 to 255 in a random order. The pattern of the key blocks will depend on text key entered by the user. Our proposed system using 512 bit key size to encrypt a text message. It wills us very difficult to find out two same massages using this parameter. To decrypt any file one has to know exactly what the key blocks is and to find the random blocks theoretically one has to apply 2^{256} trial run and which is intractable. Initially that technique is only possible for some files such as Microsoft word file, excel file, text file.

Encryption Approach Used:-

Here we are using symmetric encryption approach. We have already know that symmetric encryption approach is divide in two type one is block cipher symmetric cryptography technique and another is stream cipher symmetric cryptography but here we are choosing block cipher type because its efficiency and security. In the proposed technique we have a common key between sander and receiver, which is known as private key. Basically private key concept is the symmetric key concepts where plain text is converting into encrypted text known as cipher text using private key where cipher text decrypted by same private key into plane text. 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 private information. Basic concept of symmetric cryptography is shown in figure 3.

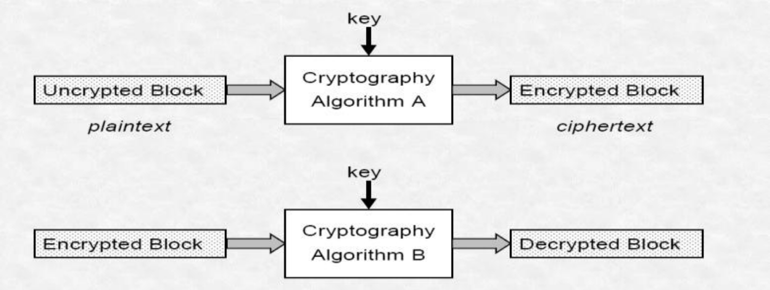

Figure 3: Basic Concept for Symmetric Cryptography

Reasons for Use of Symmetric Approach for Encryption and Decryption:-

- The encryption process is simple.
- Each trading partner can use the same encryption algorithm no need to develop and exchange secret algorithms.
- Security is dependent on the length of the key.
- High rates of data throughput.
- Keys for symmetric-key ciphers are relatively short.
- Symmetric-key ciphers can be used as primitives to construct various cryptographic mechanisms.
- Symmetric-key ciphers can be composed to produce stronger ciphers
- Symmetric-key encryption is perceived to have an extensive history.

Proposed Algorithm for Random number and Encryption Number Calculation:-

1. Define variable length from 1 to 64 and base value from 65 to 2.
2. Calculate random number we follow-up the following steps.
3. Calculate variable Total

   $$\text{Total} = \sum_{m=1}^{n} \text{ASCII code} * b^{m}$$

   = xwyz
4. Calculate Random Value
   Ran_Value = x * b1 +w * b2 + y * b3 + z * b4
5. Now select another variable value V1 which will represent as a Random Number.
   V1 = Mod (Total, Ran_Value)
   V1 = xy
6. If V1 == 0 then
   Set V1 = Ran_Value1
   Else if V1 > 64 then
   Set V1 = V1 – 64
7. Calculate Encryption Number we follow-up the following steps.
8. Calculate Encryption Value
   Enc_Value1 = z * b1 + y * b2 + x * b3 + w * b4
9. Now select another variable V2 which will represent as a Encryption Number.
   V2 = Mod (Total, Enc_Value1)
   V2 = xy
10. If V2 = = 0 then
    Set V2 = Enc_Value1
    Else if V2 > 64 then
    Set V2 = V2 – 64
11. Finally we have Random Number and Encryption number in V1 and V2 respectively.
12. Exit.

Flow Chart of Proposed Key:

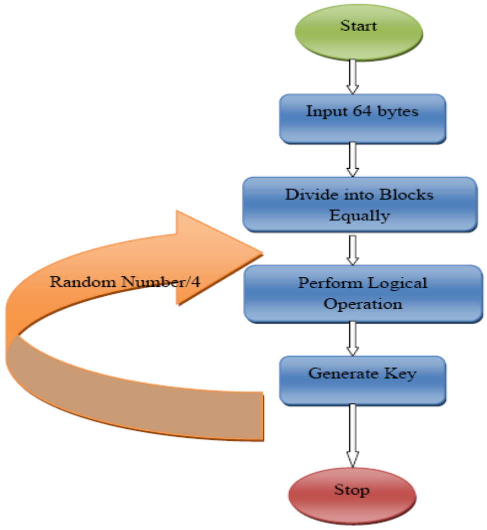

Figure 4: Flow Chart of Proposed Key

Block Diagram of Proposed Key:

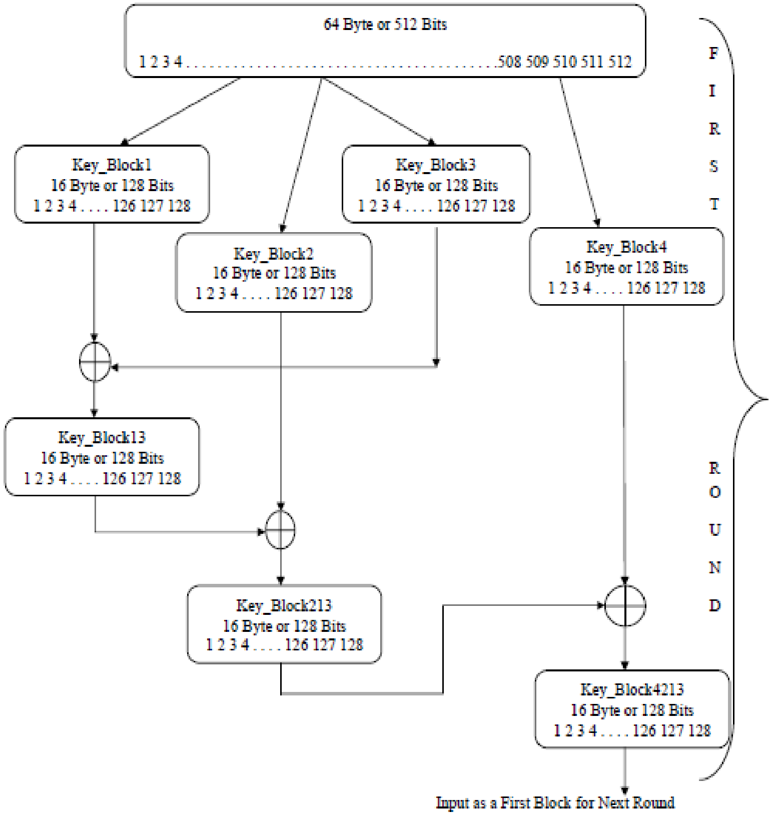

Figure 5: Block Diagram of Proposed Key

Proposed Key Generation Steps:

1. Select or create any private key of Size 256 X 2 bits or 64 characters.
2. Size of selected key will be varying from 128 bits to 512 bits or 16 to 64 characters.

3. We can choose any character from 0 to 255 ASCII code.
4. Use of 64 * 8 key that means 512 bits in length.
5. Divide 64 bytes into 4 blocks of 16 bytes likes Key_Block1, Key_Block2, Key_Block3, and Key_Block4.
6. Apply XOR operation between Block1 and Block3. Results will store in new Key_Block13.
7. Apply XOR operation between Block2 and Block13. Results will store in new Key_Block213.
8. Apply XOR operation between Key_Block213 and Key_Block4. Results will store in new Key_Block4213.
9. Repeat Step 7, 8, 9 till (random number / 4).
10. Exit.

Flow Chart of Proposed Algorithm:

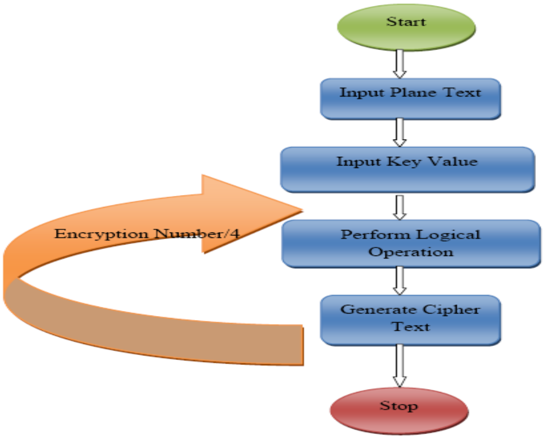

Figure 6: Flow Chart of Proposed Algorithm

Block Diagram of Proposed Algorithm:

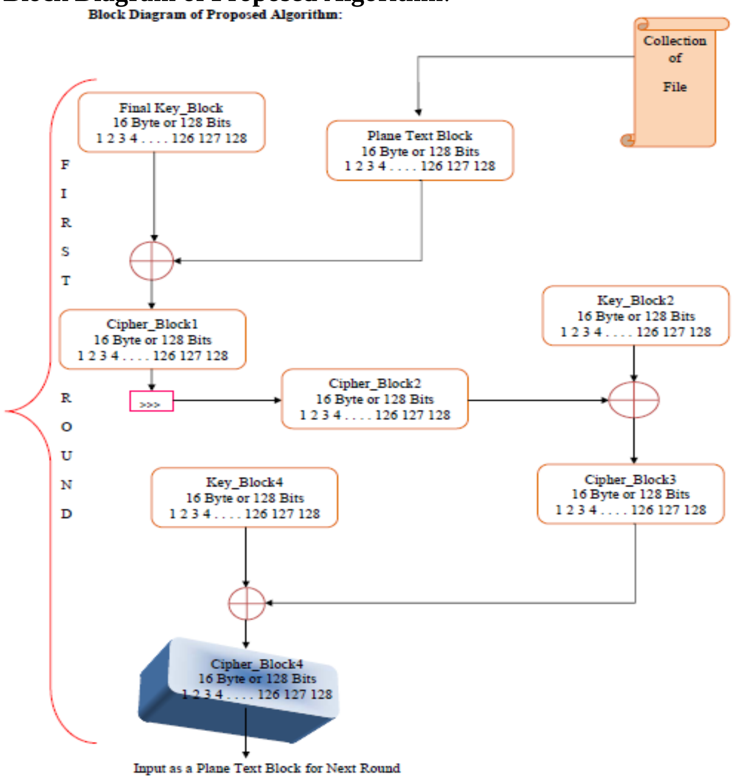

Figure 7: Block Diagram of Proposed Algorithm

1. Initially select plane text of 16 bytes (or we can vary from 16 to 64 depend on requirement).
2. Initially insert key of size 16 bytes (depend on plane text value)
3. Apply XOR operation between key (Key_Block4213) and plane text block (Text_Block). Result will store in Cipher Block1.
4. Apply right circular shift with 3 values. Result will store in new Cipher_Block2.
5. Apply XOR operation between Cipher_Block2 and Key_Block2. Result will store in new Cipher_Block3.
6. Apply XOR operation between Cipher_Block3 and Key_Block4. Result will store in Cipher_Block4.
7. Cipher_Block4 is the input of the next round as a plane text block.
8. Repeat step 1 to 7 till (Encryption Number / 4).
9. Exit.

Section IV
RESULTS COMPARISONS

I am using .Net implementation to present an evaluation system. For calculation of execution time of the known cryptographic algorithm with my proposed cryptography algorithm, it is necessary to describe the detailed evaluation method, as illustrated in Figure- 8. Here I am taking only one evaluating modes to find whether the key and the plaintext have impact on time consuming of cryptographic algorithms: DPSK (different plaintexts in the same key).

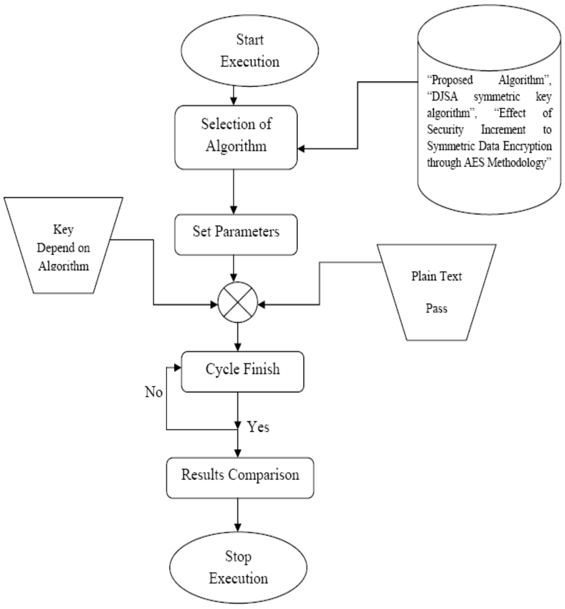

Figure 8: Result Evaluation Model

We are using two parameters for execution time one is encryption value and second is decryption time which is shown in table 1 and table 2 Here I am doing compare execution time of encrypting plaintext on different existing cryptographic algorithms with my proposed cryptography algorithm. During processing, the content of the plaintext and the key are both written by the random number. For evaluation mode, there are two parameters: the number of evaluated plaintexts and the size of evaluated plaintext, where the number of evaluated plaintexts is the number of plaintexts that are generated randomly and the size of evaluated plaintext can be chosen from two kinds that mention above. In this mode, I do n cycles (that is, the number of the evaluated plaintexts). In each cycle, same plaintexts are respectively encrypted by "**A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm**", **"Effect of Security Increment to Symmetric Data Encryption through AES Methodology"** and **"Proposed Algorithm (PA)"** by copying them. Finally, the outputs of the evaluation system execution time, and measured in numeric form. Actually, for an encryption algorithm, the execution time of encryption not only depends on the algorithm's complexity, but also the key and the plaintext have certain impact.

Result Comparison in Tabular Form: - In this I am going to represent our result in the form of table. After comparison the results that were obtained can be well represented in form of tables.

Here, **The Proposed Algorithm** (with 265bit block size in this thesis) and "**A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm"** algorithm (with 128-bit block size) and **"Effect of Security Increment to Symmetric Data Encryption through AES Methodology"** algorithm (with 128-bit block size) have been implemented on a number of different data files like text, pdf and image varying types of content and sizes of a wide range.

But here we are only showing result of text file. Encryption and Decryption time of Various Text files comparisons shown in table 1 and table 2 respectively.

Table 1: - Encryption time comparisons of text files.

Plain Text Size	A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm	Effect of Security Increment to Symmetric Data Encryption through AES Methodology	Proposed Algorithm
	Execution Time Measure in Seconds		
1.66 mb	0:01:34	0:01:32	0:01:25
560 kb.txt	0:00:37	0:00:35	0:00:28
187 kb.txt	0:00:18	0:00:16	0:00:09
46 kb.txt	0:00:11	0:00:09	0:00:02
16 kb.txt	0:00:10	0:00:08	0:00:01

Table 2: - Decryption time comparisons of text files

Plain Text in Size	A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm	Effect of Security Increment to Symmetric Data Encryption through AES Methodology	Proposed Algorithm
	Execution Time Measure in Seconds		
1.66 mb.txt	0:01:34	0:01:32	0:01:25
560 kb.txt	0:00:37	0:00:35	0:00:28
187 kb.txt	0:00:18	0:00:16	0:00:09
46 kb.txt	0:00:11	0:00:09	0:00:02
16 kb.txt	0:00:10	0:00:08	0:00:01

A graphical representation for the table 1 and table 2 is shown in figure 9 and figure 10 with blue line and orange line for encryption time and decryption time of "**A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm"** and **"Effect of Security Increment to Symmetric Data Encryption through AES Methodology"**, respectively and green line is for **"Proposed Algorithm"**. According to the graph, there is a tendency that encryption/decryption time for Proposed Algorithm, and compared algorithms increases with file size. But required time for the encryption/decryption through Proposed Algorithm is much smaller than encryption/decryption time for compared algorithms. The observations were made using personal computer with specifications of Intel Pentium Dual Core E2200 2.20 Ghz, 1 GB of RAM and Window-XP SP2as the platform

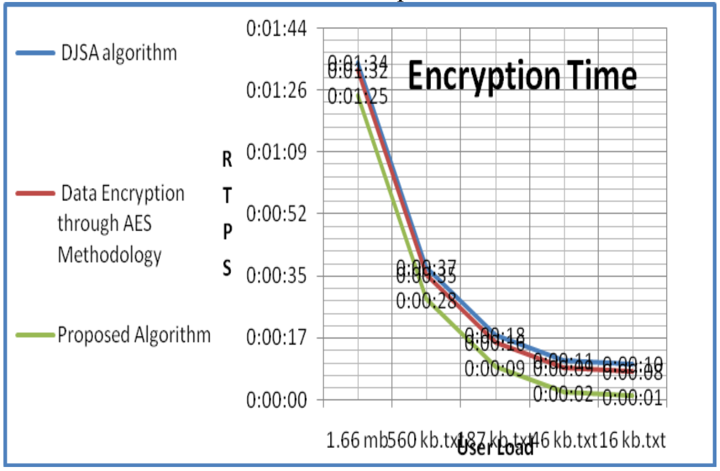

Figure 9: Encryption time comparison of text files between various algorithms with proposed algorithm

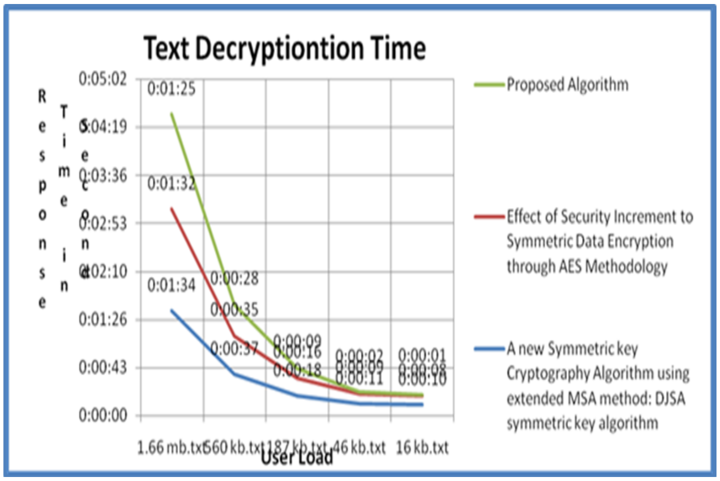

Figure 10: Decryption time comparison of text files between various algorithms with proposed algorithm

Characteristic of Proposed Technique:

Simplicity: Our proposed algorithm is very simple. Each trading partner can use the same encryption algorithm no need to develop and exchange secret algorithms.

Security: Due to the length of the key our proposed technique is very much secured.

Throughput: Due to its simplicity we can encrypt data with high rates. Proposed Keys for symmetric-key ciphers are relatively short.

Efficiency: Due to simplicity our proposed technique is high efficient. To produce stronger ciphers our proposed symmetric key can be a good choice. Symmetric-key encryption is perceived to have an extensive history.

Robustness: With the advances in technology it is of vital importance that our encryption system is robust enough to withstand the advances in technology. The more an encryption technique relies on mathematics, the less the robustness.

Availability: Some of the encryption techniques discussed have been around for years, but not all are fully functional yet. Those that have been around for some time may have the advantage of being "tried-and-tested", while some organizations are not familiar with others.

Integration: The integration level of our encryption system will depend on how easily it can be integrated at the application level. The proposed encryption technique must be able to be implemented on software and hardware.

Distribution: With present day technology evolving around the Internet and networks, it is important that our proposed encryption techniques work on an entire network, not only on a point-to-point basis. When one broadcast a message through a network all the intended recipients should get the same encrypted, secure message.

Time efficiency: Users expect encryption to be immediate, otherwise the process is cumbersome. The time efficiency of our proposed encryption technique measures in second to encrypt and decrypt information and it's very good.

Flexibility: The flexibility issues of our proposed encryption technique are very high which is referring to the use of keys and whether the key lengths are set, or whether different key lengths can be used.

Reliance on users: our proposed encryption techniques support this features. If a user has chosen a "bad" password or key encryption and decryption will not proceed for further action.

Conclusion and Future Enhancement: From the result its is clear that our "proposed technique" is batter result producing as compared "DJSA symmetric key algorithm" and "Effect of Security Increment to Symmetric Data Encryption through AES Methodology". If any user emphasis on security then he can use our proposed algorithm. Our method is essentially block cipher method and it will take less time if the file size is large. The important thing of our proposed method is that it is almost impossible to break the encryption algorithm without knowing the exact key value. We propose that this encryption method can be applied for data encryption and decryption in any type of public application for sending confidential data.

References

[1] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.

[2] Yan Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms "2009 International Conference on Computational Intelligence and Security 978-0-7695-3931-7/09 $26.00 © 2009 IEEE DOI 10.1109/CIS.2009.81.

[3] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.

[4] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[5] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Published by Springer-Verlag.

[6] By Klaus Felten "An Algorithm for Symmetric Cryptography with a wide range of scalability" published by 2nd International Workshop on Embedded Systems, Internet Programming and Industial IT.

[7] Majdi Al-qdah & Lin Yi Hui "Simple Encryption/Decryption Application" published in International Journal of Computer Science and Security, Volume (1) : Issue (1).

[8] T Morkel, JHP Eloff " ENCRYPTION TECHNIQUES: A TIMELINE APPROACH" published in Information and Computer Security Architecture (ICSA) Research Group proceeding.

[9] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.

[10] Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.A. Matin "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 978-0-7695-3263-9/08 DOI 10.1109/SNPD.2008.101 IEEE 2008.

[11] [Rijn99]Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999.