IMPLEMENTATION OF MODERN ENCRYPTION STANDARD (MES): VERSION II

Mr. Surajkumar J. Manowar*

Prof. Amit. M. Sahu*

Abstract

Abstract— In this paper we are implementing a new symmetric key cryptography (SKC) method called Modern encryption Standard (MES)-II [2]. One of the authors have published Modern Encryption Standard Version-I (MES-I) [1]. In the present method there is a use of Modified generalized Vernam cipher method with feedback with different block size from left to right. The entire content of given data is divided in different block sizes. After that entire content is divided into two files and then combine them by taking 2nd half first and the 1st block. The generalized modified Vernam Cipher method again applied from left to right with different block sizes. The authors have proposed the present method and it can be effective to encrypt various types of plain text files and the method is free from standard cryptography attacks namely brute force attack, known plain text attack and differential attack. MES –II can be used as independent encryption algorithm to encrypt any short message such as SMS, Password or encryption key etc.

Keywords— Vernam Cipher Method; MES; TTJSA; DJSA

* Department of CSE, G. H. Raisoni College of Engineering & Management, Amravati, Maharashtra, India.

Introduction

Cryptography and network security is now a very important research area in modern digital communication network. Due to tremendous development in communication network now it is very easy for anyone to get any kind of information from internet. Password breaking and hacking any email message is not a difficult issue. The bank services are now done through internet. Any kind of money transaction is possible through on-line e-banking system. Most of these transactions are done through verification of user-id and password. The user-id is mostly public only the password is private. If the password is strong then it may not be possible to break by any hackers but if the password is weak then the hackers can break it very easily. In fact there are quite a number of websites where much software are available which can be used to break the password of the user-id. To prevent this type unwanted intrusion now the scientists have switch over to new kind of authentication of users using fingerprint authentication. This may be one good solution as no two persons have the same type of thumb impression. When we send some information through internet without any encryption then anybody can read those data in between as a middle man and he/she can divert it to different destination. Data security and authenticity of data is now a major issue in data communication network. It is now an open secret to everybody that any confidential data should not be sent in raw form on the other hand it should be sent in encrypted form so that during transition from one computer to other computer no intruder or hacker can read the data and misuse it. In any commercial organization the disaster may happen if a marketing manager of a private company is sending some crucial data related to the sales of the company to his Managing Director over the e-mail and some intruder intercepts that data from the internet and passes it on to some other rival company. This type of disaster may occur if the data is sent in an unprotected manner. To protect any kind of hacking problems nowadays network security and cryptography is an emerging research area where the programmers are trying to develop some strong encryption algorithm so that no intruder can intercept the encrypted message. The present proposed method is symmetric key cryptography. The encryption and decryption is done through single key which should be known to the sender and also to the receiver. The merit of symmetric key cryptography is that the key management is very simple as one key is used for both encryption as well as for decryption purpose on the other hand in case of public key crypto system two keys are used. One key is used for encryption purpose and the other key for decryption purpose. The encryption key is called public key that is known to everybody

and the decryption key is called private key and that is known to receiver only. The problem of Public key cryptosystem is that one has to do huge amount of computation for encrypting any plain text. Moreover in some public key cryptography the size of encrypted message may increase. Due to complexity of calculation the public key cryptosystem may not be suitable in a case like sensor networks where the excess battery voltage consumption is not permissible. So in sensor networks we have to adopt some effective encryption method which should not consume the battery voltage too much. In the present work we are proposing a symmetric key method called Modern Encryption Standard Version II (MES-II) [1] which can be used to encrypt data in sensor network, mobile network, and ATM network, defense or even in corporate sector also. The present method may be very useful to encrypt password, short message, encryption key etc. In the present method the authors applied generalized modified vernam cipher method with various block size and different keys for each block. The authors have also used the feedback in this method to give further strength to this algorithm. In the present work the authors have modified the method using variable block size and variable key. After completion of encryption in forward direction then the entire file is divided in two parts and the two parts interchanged and again applied the modified vernam cipher method with feedback and new key. The whole operation is repeated number of times to make the encryption process hard. The multiple encryptions make our system very secure.

Literature Review

Many different cryptographic algorithms are been researched every day. All of them have different methodology and working area to generate cipher text. Some of them are as discussed below.

A. *TTJSA Algorithm*: In this method the authors [3] have used two methods MSA [5] and NJJSAA [6] which were developed by Nath et al. and have developed a new algorithm, generalized modified Vernam Cipher Method. The above three methods are applied in random order on any given plain text for a number of times to get the ultimate cipher text file. In this method, authors modified the standard Vernam Cipher Method for all characters (ASCII code 0-255) with randomized keypad, and have also introduced a feedback mechanism. The authors have also applied this method on some known text where the same character repeats for a number of times and we have found that after encryption there is no repetition of pattern in the

output file. This feature is been tested closely and have found satisfactory result in almost all cases. This has been possible as it had used modified vernam cipher method with feedback mechanism and also NJJSAA method, where they use mainly the bit manipulation. The key matrix is of size 16x16. This key may be generated in '256!' ways. In bit manipulation method there is a use block cipher method and in MSA method we use stream cipher method. The method uses first bit manipulation and then MSA encryption method. There is lot of scope to modify the present method.

B. *DJSA Algorithm*: In this method [4] the authors considered the size of the key matrix to be 65536 and in each cell we store 2 characters pattern instead of 1 character unlike MSA method [5]. If someone wants to give a brute force method to find our actual key then one has to give a trial for factorial 65536 runs! Theoretically this is an intractable problem. Moreover the authors have also introduced multiple encryptions here to make the system more secured. In the present work the authors have introduced a square key matrix of size 256 by 256 where in each cell there are all possible 2-lettered words (ASCII code 0-255). The total number of words possible is 65536. In the present work we use the maximum encryption number=64 and maximum randomization number=64. The present work is basically the extension of MSA algorithm [5]. They have used the key matrix of size 256x256x2. This key may be generated in 65536! ways. So in principle it will be difficult for anyone to decrypt the encrypted text without knowing the exact key matrix. Our method is essentially block cipher method and it will take more time if the files size is large and the encryption number is also large.

C. *MES Version I algorithm*: And some more secured algorithm was designed using combination of two or three or more algorithms i.e. "Modern Encryption Standard (MES) Version-I: An Advanced Cryptographic Method" [1]. The proposed method was Modern Encryption Standard version-I (MES version-I) and, the method is achieved by splitting the file, which is to be encrypted, and encrypting the split sections of the file in various ways using TTJSA and DJSA cipher methods. The method has been tested on different files and the results were very satisfactory. Though the results of Modern Encryption Standard (MES): Version-I are satisfactory but was less secure due to noncomplex & obvious encryption

technique along with the idea of combination of different algorithms as using combination of different encryption algorithms doesn't lead to good security ethics.

D. *SKC using DJSSA Algorithm*: The algorithm for Symmetric key Cryptography using modified DJSSA symmetric key [7] was developed which specifies the use maximum encryption number=15 and maximum randomization number=8. Here there is a use of key matrix of size 65536x256x3. This key may be generated in 16777216! ways. So it is not possible for anyone to decrypt the encrypted text without knowing the exact key. In this method we have used two stages of encryption, one by exchanging bits and then by changing pattern according to random key matrix. But this method is essentially a block cipher method and it will take more time if the files size is large and the encryption number is also large.

E. *UES-I Algorithm*: Here, new encryption algorithm concept "Ultra Encryption Standard (UES) Version-I: Symmetric Key Cryptosystem using generalized modified Vernam Cipher method, Permutation method and Columnar Transposition"] method came to the scene of Cryptosystem [9]. It combines three different methods namely, Generalized Modified Vernam Cipher method, Permutation method and Columnar Transposition method. In the Modified UES Version-I the authors have applied the three encryption methods empowered with multiple encryption, randomized key generation and sequence of column extraction on some known text where the same character repeats for a number of times and we have found that after encryption there is no repetition of pattern in the output file. Using combination of different encryption algorithms doesn't lead to good security ethics.

Also, many authors have put forward the ideas and concept behind Symmetric Key cryptography [7, 8, 9, 10, 11, and 12]. The use of Random Key generator for cryptography is been used in MES-II algorithm for encryption [5]. At the same time, the technique of combined bit manipulation is used in NJJSSA algorithms [6]. Integration or combinations of various different encryption algorithms such as DJSA, DJMNA, NJJSSA, SJA, Advanced Caesar Cipher Method, etc. [4, 12, 6, and 10] have special impact on security.

Algorithm for Advanced Encryption: MES Version II

As the literature review has the greater impact on efficiency and more secure cryptography, we have to implement Modern Encryption Standard Cryptography for Data security purpose. As the

objective of good encryption algorithm is to provide a higher data security in encrypted or unreadable format, which is to be achieved by Modern Encryption Standard algorithm. Also we need to cross check that the processing and implementation of the algorithm should not cause corruption of information in the original data or message and also the size of the enciphered text should not be larger than the original plain text. And there should be no repetition of pattern in the output, which is to be taken care of, while implementing the Modern Encryption Standard (MES) algorithm. The proposed system model for encryption using Modern Encryption Standard-II can be elaborated with an algorithm. The following algorithm is shown for Encryption process in a diagrammatic view rather than the step-wise procedures.

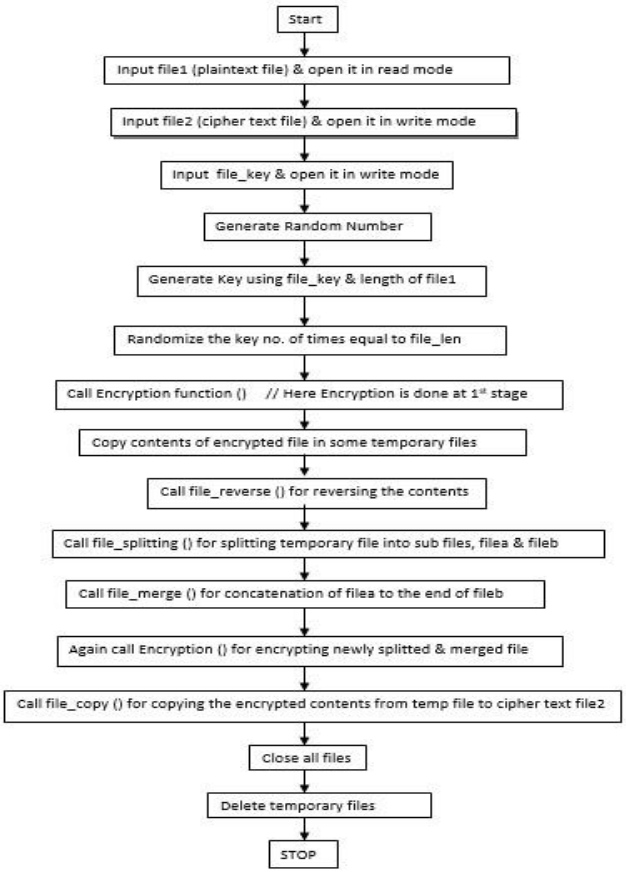

Fig.1: Algorithm for Encryption using MES-II

Methodology

In the present method, as discussed earlier, in the algorithm, we use generalized modified vernam cipher method with various block size and different keys for each block. We also used the feedback in this method to give further strength to this algorithm. The generalized modified

vernam cipher method with feedback with fixed block size was already developed. In the present work we modified the method using variable block size and key. After completion of encryption in forward direction then the entire file is divided in two parts, the encrypted contents of file are reversed and stored on temporary file. After that, the file is splitted in two parts; we can divide in more than two also. On splitting the file, merge the parts in reverse order i.e. concatenate sub part 1 to the end of sub part 2; or it can be done by random number generation using tictoc function. After completing this procedure, encryption function is called again. The whole operation is repeated number of times to make the encryption process hard. The multiple encryptions make the system more secure. These are some important algorithms included in this paper for Encryption & Decryption along with various File operations algorithms, Key generation algorithms and Key manipulation algorithms namely- Encryption Algorithm: Main(), Decryption Algorithm:Main(), Function Vernam_Cipher: Feedback_Encryption(), FunctionVernam Cipher: Feedback_Decryption(), function keygen(), function randomizing key(), function filereverse(), function filesplitting(), function mergefile(), function filecopy(), function tictoc(), etc.

The main module of Encryption takes names of the plain text file and cipher text file as input from the user. It also takes the key used for encryption as input and executes the complete encryption algorithm by calling the various functions involved in this encryption method. The methodology for encrypting the given data is explained in this section, which is meant for only Encryption purpose only. And at the receiver's end, the enciphered file is to be decrypted for getting the original plain text file as the Decryption process includes the general reverse process of Encryption method.

Implementation Results and Comparisons

In this paper work the result of MES Version II will be discussed along with the performance analysis of MES Version II will be compared with various encryption algorithms in view of total execution time i.e. time required for both encryption and decryption, key length and its performance. The throughput parameters specified, key length and execution time are important to analyze, compare and to decide the efficiency of any cryptographic algorithm. The new symmetric cryptographic algorithm i.e. Modern Encryption Standard (MES) - Version II [2] is implemented in Java as Java has much better Coding libraries, which have greater impact on programming skills for better and efficient results. First of all, let's look at the results of

encryption and key performance. Here input plain text file is processed through the MES Version II cryptographic algorithm. The encrypted contents are stored in text file. All the file operations and manipulations are done through text file only.

Sample Test Case:

"St. Xavier's College, Kolkata, which completed 150 years in 2010, is an autonomous college under the University of Calcutta. The college received NAAC accreditation in 2011 with a score of 3.53 (out of 4) at A grade. It has also been declared as a College with potential for excellence, by U.G.C Autonomous status was granted to the College by the University of Calcutta through a letter dated March 06, 2006. Autonomy came into effect from the academic year of 2006-2007".

The above sample test case of plaintext file has passed through the MES encryption process and results are out with desired & greater security and efficiency. Following is the screenshot of the Encrypted Text of sample Test Case.

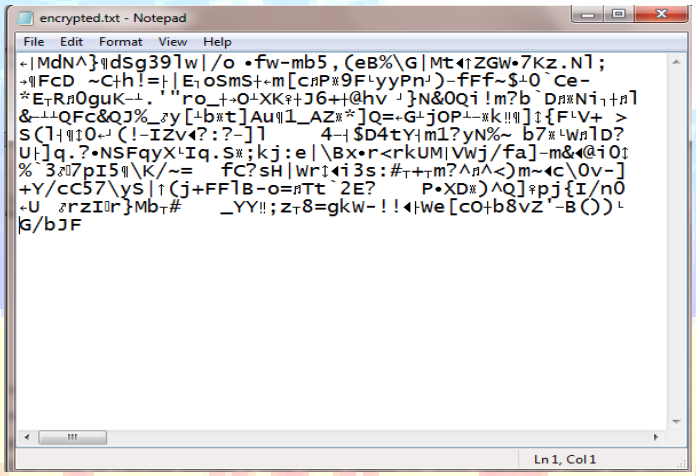

Fig.2: Encrypted text of Sample Test case

The cryptographic key generated in above sample case is shown below. As the cryptographic key is formed with respect to size of plain text file, the size of cryptographic key is approximately same as the size of input file. Following is the screenshot of the Cryptographic Key generated for sample Test Case.

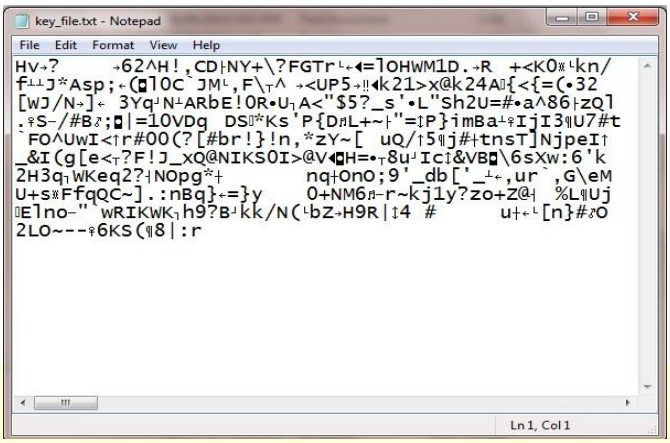

Fig.3: Cryptographic Key generated for sample Test Case.

During the encryption process, the key generated for encryption and decryption process is same in symmetric key cryptography. So, the cryptographic key is an important part for whole cryptographic algorithm to execute in efficient manner. Also, if the encryption and decryption process or algorithm has to be run on different computer systems, then the cryptographic key which is generated in encryption process has to be exchange by sender to the receiver through confidential and secure medium so that to decrypt the cipher text using the same cryptographic key. Now, we will move towards comparison part of the algorithm. Here we will be comparing the results of MES I already given by authors [1] and MES II with respect to total execution time obtained vs. input file size.

Table I: MES-I vs. MES-II Result for Input file size vs. Total Execution Time.

Input File Size (bytes)	MES Version I Total Execution time (seconds)	MES Version II Total Execution time (seconds)
1024	4	0.641
2048	6	1.034
4096	6	2.392

The outputs are taken as size of plain text file in bytes vs. total execution time in seconds. Three samples of input plain text file is taken i.e. 1024 bytes, 2048 bytes and 4096 bytes. And for each of them, total execution time is marked with respect to time required. The graph shows that the execution time required for input plain text file size through MES Version II is less than the MES

Version I. It means that MES Version II has faster execution time, avoiding delay, for encrypting the contents of file than MES Version I, which results to higher efficiency of any cryptographic system. As the MES I cipher methods is a combination of TTJSA and DJSA methods, it requires more time as compared to MES Version II, which is an independent symmetric key cryptographic algorithm. For better clarification, graph is shown below.

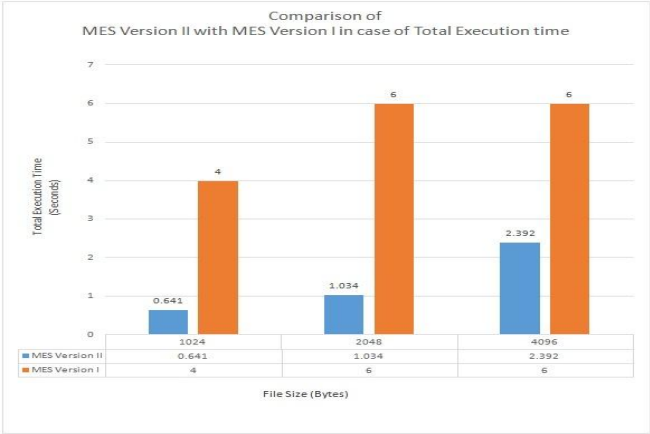

Fig.4: MES-I vs. MES-II graph for Execution time

So in case of MES-II, it shows that execution time is directly proportional to the size of plain text file. As the size of input plain text file gets increased, the execution time also increases,ultimately increases the security as key length is large. At the same time the results of MES-I compared, are already given by authors in the MES Version I algorithm [1].

Now after comparing in case of total execution time, we will see the comparison in case of key length as key length is one of the important factors for data security, as greater the key length, greater the security is [13]. Here we will be comparing the key length of MES Version II with AES, DES, etc.

Table II: MES-II vs. AES Result for Input file size vs. Key Length.

Input File Size (bytes)	AES Key Length (bytes)	MES Version II Key Length (bytes)
1024	20 (160 bits)	51
2048	20 (160 bits)	1600
4096	20 (160 bits)	3853

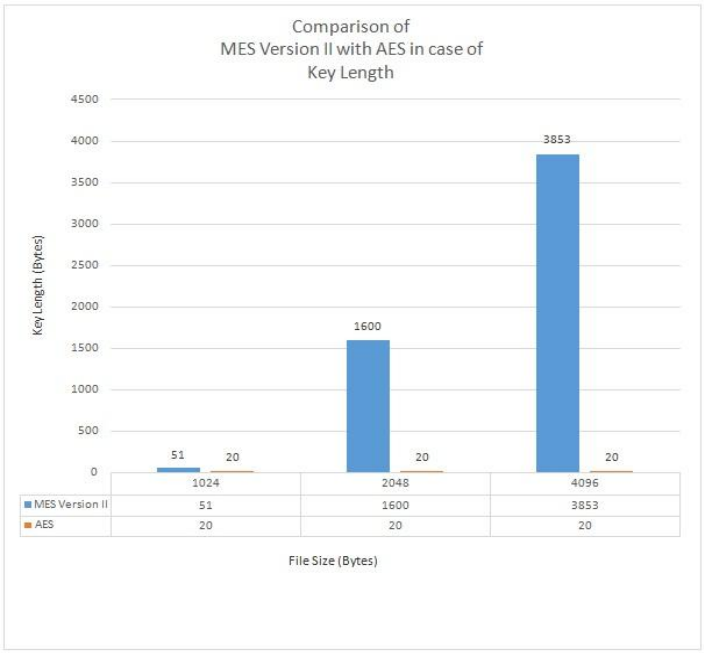

Fig.5: MES-I vs. AES graph for Key length

In above comparison of MES Version II with AES in case of Key Length shows that as the key length of Modern Encryption Standard Version II does not work on fixed size key, rather it works on size of input plain text file. Also AES algorithm has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits as the Rijndael specification is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. It means that the key size for AES ranges from 128 to 256 bits. In this case, AES has text key of 16 characters and the key size specified is 20 bytes which is fixed and is equal to 160 bits. So in comparison of MES II with AES in case of Key Length, AES shows fixed key size of 20 bytes resulting to low data security while the MES II shows increased key length depending on input file size, resulting to higher data security [13].

Here the same concept of increased key length is applied to DES, and it gives the same result as obtained in case of AES. Let's look at the comparison scenario of MES Version II with DES in case of key Length. The tabular form of DES and MES Version II results and subsequent graph are shown below.

Table III: MES-II vs. DES Result for Input file size vs. Key Length.

Input File Size (Kilo bytes)	DES Key Length (bytes)	MES Version II Key Length (bytes)
15	7 (56 bits)	14328
30	7 (56 bits)	29953

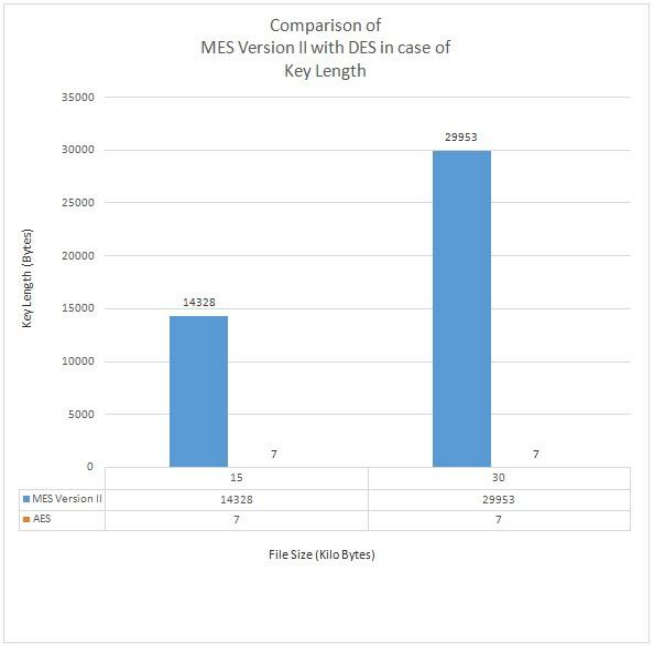

Fig.6: MES-I vs. AES graph for Key length

In case of comparison, DES has key of 56 bits [14] which is fixed and is equal to 7 bytes. So in comparison of MES II with DES in case of Key Length, DES shows fixed key size of 7 bytes resulting to low data security while the MES II shows increased key length depending on input file size, resulting to higher data security [13]. This does not has any issue for encryption with DES algorithm, but it matters in MES Version II algorithm as the key length increases with respect to size of plain text file.

Conclusions

The present method is such that encrypted text cannot be decrypted without knowing the exact initial random key. MES-II algorithm is developed in Java. In the present method we have used only generalized modified vernam cipher method with variable block size and variable key and also the encryption done in two ways. It is byte wise encryption method. The present method may be clubbed with bit wise encryption standard. We can further modify to add some more complex bit wise operations with MES-II to obtain further complex encryption method. The proposed algorithm shows that the present method is free from standard cryptography attack such as known plain text attack, brute force attack, and differential attack. The present method will be most effective to encrypt short message such as SMS in mobile phone, password encryption and any type of confidential message. We can have any type of file for encryption purpose such as text, audio, video, etc. In the future work we would be adding some more complex bit-wise operations and will integrate vernam cipher method in bit level. The method proposed in MES Version II algorithm has the implementation of higher security. One thing to be noted that the key length in the MES-II algorithm is not fixed; it depends on the size of input plain text file. It means it depends on plain text file. Large the size of plain text file, larger will be the key length, resulting to higher security as the data security depends mostly on the size of input file [13]. But on studying, analysing and comparing the performance parameters like total execution time and key length and its performance with other encryption algorithms, we can say that MES Version II has better and higher data security performance as compared to other encryption algorithms.

Acknowledgement

We are very much grateful to the Head of Computer Science & Engineering Department to give us this opportunity to work on symmetric key Cryptography. Also, we sincerely express our gratitude to our Principal for giving constant encouragement and facilities in doing research in cryptography. Last but not the least; we would like to express our thankfulness to all my friends, family members and well-wishers.

References

[1] Somdip Dey, Asoke Nath, "Modern Encryption Standard (MES) Version-I: An Advanced Cryptographic Method", Proceedings of IEEE 2nd World Congress on Information and Communication Technologies (WICT- 2012), pp. 242-247.

[2] Rahul Deep Sircar, Gunjun Sekhon and Asoke Nath, "Modern Encryption Standard (MES): Version-II," 2013 International Conference on Communication Systems and Network Technologies, IEEE Computer Society, 978-0-7695-4958-3/13 $26.00 © 2013 IEEE DOI 10.1109/CSNT.2013.

[3] Trisha Chatterjee, Tamodeep Das, Joyshree Nath, Shayan Dey and Asoke Nath, "Symmetric key cryptosystem using combined cryptographic algorithms- generalized modified vernam cipher method, MSA method and NJJSAA method: TTJSA algorithm", Proceedings of IEEE International conference: World Congress WICT-2011 t held at Mumbai University 11-14 Dec, 2011, Page No. 1179-1184(2011).

[4] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta and Asoke Nath, "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm", Proceedings of IEEE International Conference on Communication Systems and Network Technologies, held at SMVDU(Jammu) 03-06 June,2011, Page-89-94(2011).

[5] Asoke Nath, Saima Ghosh, Meheboob Alam Mallik, "Symmetric Key Cryptography using Random Key generator: MSA Algorithm", Proceedings of International conference on security and management (SAM'10" held at Las Vegas, USA Jull 12-15, 2010), Vol-2, Page: 239-244(2010).

[6] Neeraj Khanna, Joel James,Joyshree Nath, Sayantan Chakraborty, Amlan Chakrabarti and Asoke Nath, "New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm", Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 125-130(2011).

[7] Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath, Dripto Chatterjee, "Symmetric key Cryptography using modified DJSSA symmetric key algorithm", Proceedings of International conference Worldcomp 2011 held at LasVegas 18-21 July 2011, Page-306-311, Vol-1(2011).

[8] Article "Symmetric key Cryptography using two-way updated – Generalized Vernam Cipher method: TTSJA algorithm", International Journal of Computer Applications (IJCA, USA), Vol 42, No.1, March, Pg: 34 -39(2012).

[9] Satyaki Roy, Navajit Maitra, Joyshree Nath,Shalabh Agarwal and Asoke Nath, "Ultra Encryption Standard(UES) Version-I: Symmetric Key Cryptosystem using generalized modified Vernam Cipher method, Permutation method and Columnar Transposition method", Proceedings of IEEE sponsored National Conference on Recent Advances in Communication, Control and Computing Technology-RACCCT 2012, 29-30 March held at Surat, Page 81-88(2012).

[10] Somdip Dey, Joyshree Nath, Asoke Nath, "An Integrated Symmetric Key Cryptographic Method – Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and reversal Method: SJA Algorithm", International Journal of Modern Education and Computer Science, (IJMECS), ISSN: 2075-0161 (Print), ISSN: 2075-017X (Online), Vol-4, No-5, Page 1-9,2012.

[11] Dripto Chatterjee, Joyshree Nath, Soumitra Mondal, Suvadeep Dasgupta and Asoke Nath, "Advanced Symmetric key Cryptography using extended MSA method: DJSSA symmetric key algorithm", Jounal of Computing, Vol 3, issue-2, Page 66-71, Feb (2011).

[12] Debanjan Das, Joyshree Nath, Megholova Mukherjee, Neha Chaudhury and Asoke Nath, "An Integrated symmetric key cryptography algorithm using generalized vernam cipher method and DJSA method: DJMNA symmetric key algorithm", Proceedings of IEEE International conference: World Congress WICT-2011 to be held at Mumbai University 11-14 Dec, 2011, Page No. 1203-1208 (2011).

[13] Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma, "Analysis and Comparison between AES and DES Cryptographic Algorithm," International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012.

[14] Sombir Singh, Sunil K Maakar and Dr. Sudesh Kumar, "A Performance Analysis of DES and RSA Cryptography," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 3, May – June 2013.

Authors Bibliography

Mr. Surajkumar J. Manowar is currently pursuing M.E. Degree in Computer Science and Engineering at G. H. Raisoni College of Engineering and Management, Amravati, Maharashtra. He received B.E. Degree in Computer Engineering from STES's Smt. Kashibai Navale College of Engineering, Pune, in 2010.

Prof. A. M. Sahu is presently working as Assistant Professor in CSE department at G. H. Raisoni College of Engineering & Management, Amravati, Maharashtra. He completed his M.E (IT) from Sipna's College of Engineering & Technology, Amravati, Maharashtra in 2012. He received B.E (IT) Degree from HVPM's College of Engineering, Amravati, Maharashtra, in 2009. He is currently guiding 3 M.E Scholars and has published more than 20 papers in national and international journals.