PERFORMANCE EVALUATION OF CRYPTOGRAPHIC ALGORITHMS: MES VERSION I AND MES VERSION II

Prof. R. V. Bambodkar*

Prof. AmitSahu**

Prof. Shailendra Shende***

ABSTRACT

In this paper we are comparing two different algorithms namely Modern Encryption Standards (MES) Version I [1] and Version II [2]. MES Version I algorithm is the amalgamation of two different encryption algorithms namely TTJSA and DJSA in randomized fashion. The method is to split the file, which is to be encrypted, and encrypting the split sections of the file in various ways using TTJSA and DJSA cipher methods, while in MES Version II algorithm there is no amalgamation of different algorithms instead it is an independent encryption algorithm. The method proposed in MES Version II is achieved by applying Modified generalized Vernam cipher method to the plain text file with feedback with different block size from left to right and after that entire content is divided into two files and then combine them by taking 2nd half first and the 1st block. Again the generalized modified Vernam Cipher method again applied from left to right with different block sizes. In this paper work, we will be analyzing and evaluating the performance criteria's of both the encryption algorithms.

Keywords: Vernam Cipher Method; MES; TTJSA; DJSA.

* Assistant Professor, Department of CSE, DMIETR, Wardha, RTMNU, Nagpur, India

** Assistant Professor, Department of IT, GH Raisoni, Badnera, Amravati, SGBAU, Amravati, India

*** Associate Professor, Department of IT , YCCE, Nagpur, RTMNU, Nagpur, India

1.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's 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 method in MES Version I and MES Version II has 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. The methods given in both MES Version I and MES Version II algorithms,may be very useful to encrypt password, short message, encryption key etc. The method in MES II uses generalized modified vernam cipher method with various block size and different keys for each block. In this paper work we will be evaluating the performance criteria i.e. total execution time required to generate cipher text as well as the cryptographic key performance.

2. Related Work

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.

***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.

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 ofwords possible is 65536.In the present work we use the maximum encryption number=64 and maximum randomization number=64. The presentwork is basically the extension of MSAalgorithm [5]. They have used the key matrixof 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.

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.

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 Caeser Cipher Method, etc. [4, 12, 6, and 10] have special impact on security.

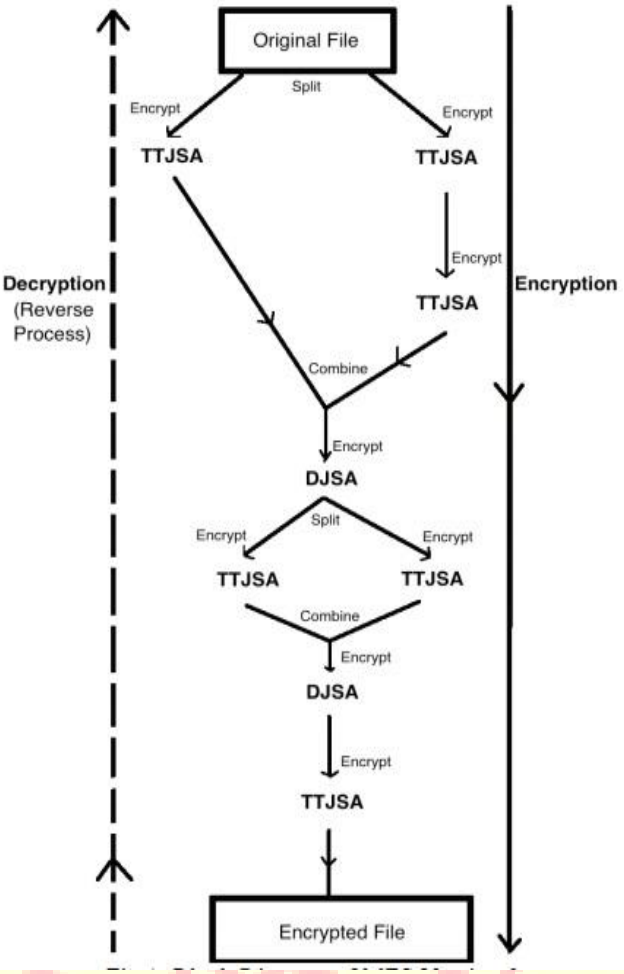


Figure 1: Algorithm for Encryption using MES Version I.

3.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 Version II algorithm [2]. 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) Version IIalgorithm.

In this method, as discussed earlier, in the algorithm, authors use generalized modified Vernam cipher method with various block size and different keys for each block. Also they use the feedback mechanism 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.

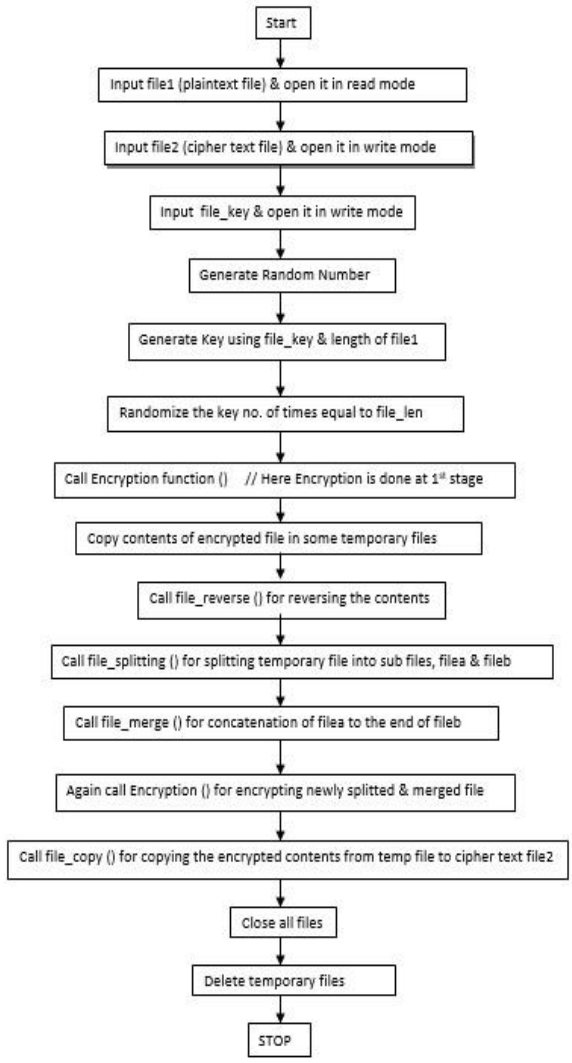


Figure 2: Algorithm for Encryption using MES Version II

In MES II algorithm, the authors 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 interchangedand again applied the modified vernam cipher method with

feedback and key involving some various file operation in between two iteration of the process. The whole operation is repeated number of times to make the encryption process hard. The multiple encryptions make the system more secure.

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.

4. Results and Comparisons

In this paper work the performance analysis of MES Version II and MES Version I is shown through various parameters like key length i.e. cryptographic key generated while execution for encryption results, time required for both encryption and decryption i.e. total execution time required for complete process. The throughput parameters specified, key length and execution time are important to analyze, compare and to decide the efficiency of any cryptographic algorithm. So, here, in this section, comparison will be seen between MES Version II and MES Version II encryption algorithms. The new symmetric cryptographic algorithm i.e. Modern Encryption Standard (MES) - Version II [1] is implemented in Java as Java has much better Coding libraries, which have greater impact on programming skills for better and efficient results. Here, we will be comparing the results of MES I already given by authors [1] and MES II with respect to total execution time i.e. time needed for both encryption and decryption process vs. input file size.

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. 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 [13]. At the same time we have the results already given by authors in the MES Version I algorithm [1] as below.

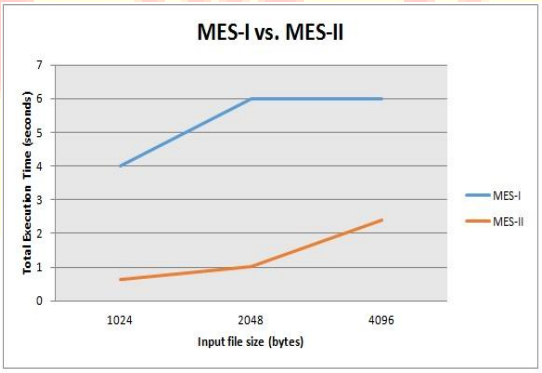
Table 1: MES Version II Result for Input files size vs. Time

Sr. No.	Input File Size (bytes)	MES Version II Total Execution Time (seconds)
1.	1024	0.641
2.	2048	1.034
3.	4096	2.392

Table 2: MES Version I Result for Input file size vs. Time

Sr. no.	Input File Size (bytes)	MES Version I Total Execution Time (seconds)
1.	1024	4
2.	2048	6
3.	4096	6

The execution times required by both algorithms i.e. MES-I and MES-II in above tables 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 more clarification, following is the comparison graph of MES-I and MES-II.



Also, in MES Version I algorithm, the TTJSA cipher method has text key of atmost 16 characters in length and the key matrix is of size 16*16. So the key can be generated in only 256! ways [3]. And the key of DJSA [4] algorithm is of size 256*256*2 and the key can be

generated in 65536! ways. So, on analyzing the key property of MES Version I i.e. of TTJSA and DJSA method, it came to know that the MES Version I works on fixed size key, while that of MES Version II key length in MES-II algorithm is not fixed, it depends on input file size. So large the input file, larger the key size, resulting to higher data security.

5.CONCLUSION

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].The proposed algorithm in both MES-I and MES-II shows that the present method is free from standard cryptography attack such as known plain text attack, brute force attack, and differential attack. Alsothese algorithms will be most effective to encrypt short message such as SMS in mobile phone, password encryption and any type of confidential message. But on analyzing the performance parameters like total execution time and key length and its performance, we can say that MES Version II has better and higher data security performance as compared to MES Version I.

REFERENCES

[1] SomdipDey, AsokeNath, "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, GunjunSekhon and AsokeNath, "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, JoyshreeNath, ShayanDey and AsokeNath, "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] DriptoChatterjee, JoyshreeNath, SuvadeepDasgupta and AsokeNath, "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]AsokeNath, SaimaGhosh, MeheboobAlamMallik,"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] NeerajKhanna, Joel James,JoyshreeNath, SayantanChakraborty, AmlanChakrabarti and AsokeNath, "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] JoyshreeNath, Sankar Das, ShalabhAgarwal and AsokeNath, DriptoChatterjee, "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, NavajitMaitra, JoyshreeNath,ShalabhAgarwal and AsokeNath,"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] SomdipDey, JoyshreeNath, AsokeNath, "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] DriptoChatterjee, JoyshreeNath, SoumitraMondal, SuvadeepDasgupta and AsokeNath, "AdvancedSymmetric 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, JoyshreeNath, Megholova Mukherjee, NehaChaudhury and AsokeNath, "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] ShraddhaSoni, HimaniAgrawal, 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.*