ISSN:0975-9646

Introduction to Modern Encryption Standard (MES)-II: An independent and efficient Cryptographic approach for Data Security

Surajkumar J. Manowar , A. M. Sahu

Department. of CSE, G. H. Raisoni College of Engineering and Management, Amravati, 444701, Maharashtra, India.

Abstract- **In this paper we have introduced a new symmetric key cryptographic method called Modern encryption Standard (MES)-II. One of the authors have published Modern Encryption Standard Version-I(MES-I). 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**.

Key words: Vernam Cipher Method; MES; TTJSA; DJSA.

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 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.

2. RELATED WORK

The generalized modified vernam cipher method with feedback with fixed block size was developed by many authors [1,5,6,7,8,9,10,11].The algorithm for "Symmetric key Cryptography using modified DJSSA symmetric key" by Dripto Chatterjee, Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath [2] 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. The advantage is that it is almost impossible to break the encryption algorithm without knowing the exact key matrix and the exchange method. 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.

After that the work was done on "Symmetric key Cryptography using two-way updated – Generalized Vernam Cipher method: TTSJA algorithm" [3], where the use of two different algorithms were made to make the encryption process too hard. It was applied on some known text where the same character repeats number of times and we found that after encryption in the output pattern there is no repetition of pattern in the output string. The key matrix is of size 16x16. This key may be generated in 256! ways. These method uses two distinct methods i.e. modified vernam cipher method and vernam cipher method using XOR operation. This method too is a block cipher method and is hard to implement due to complex computational operations. The overhead of these method is very less and hence this method may be applied specially in encryption of bio-informatics data where the same pattern is repeated or to encrypt short message, password etc.

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" by Satyaki Roy, Navajit Maitra, Joyshree Nath,Shalabh Agarwal and Asoke Nath. [4] Method came to the scene of Cryptosystem. 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 combination of different algorithms came into picture for effective encryption results. "An Integrated Symmetric Key Cryptographic Method – Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm" by Somdip Dey, Joyshree Nath, Asoke Nath. [5] In these work we use three different algorithms namely TTJSA, Caesar Cipher & Bit Rotation Method to make the encryption process unbreakable from standard cryptographic attack. The spectral analysis shows that our method is unbreakable. The output results were same as compared to above algorithm in respect of repetition of pattern. It was tested closely and has found satisfactory result in almost all cases. But, the obvious pattern of Caesar Cipher Encryption Method, is not used, instead variable numerical number should be used.

And finally the independent algorithm came into effect rather than combination of two or three or more algorithms i.e. "Modern Encryption Standard (MES) Version-I: An Advanced Cryptographic Method" by Somdip Dey, Asoke Nath [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. The Modern Encryption Standard (MES): Version-I has satisfactory results but was less secure due to noncomplex & obvious encryption technique.

Also, many authors have put forward the ideas and concept behind Symmetric Key cryptography [1,5,6,7,8,9,10,11]. The use of Random Key generator for cryptography is been used in MES-II algorithm for encryption [1]. At the same time, the technique of combined bit manipulation is used in NJJSSA algorithms [4]. Integration or combinations of various different encryption algorithms such as DJSA, DJMNA, NJSSA, SJA, Advanced Caeser Cipher Method, etc. [6,7,10,11] have special impact on security.

3. ALGORITHM FOR MES-II ENCRYPTION

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.

4. PROPOSED SCHEME

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 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 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 earlier 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. The Decryption process includes the general reverse process of Encryption method.

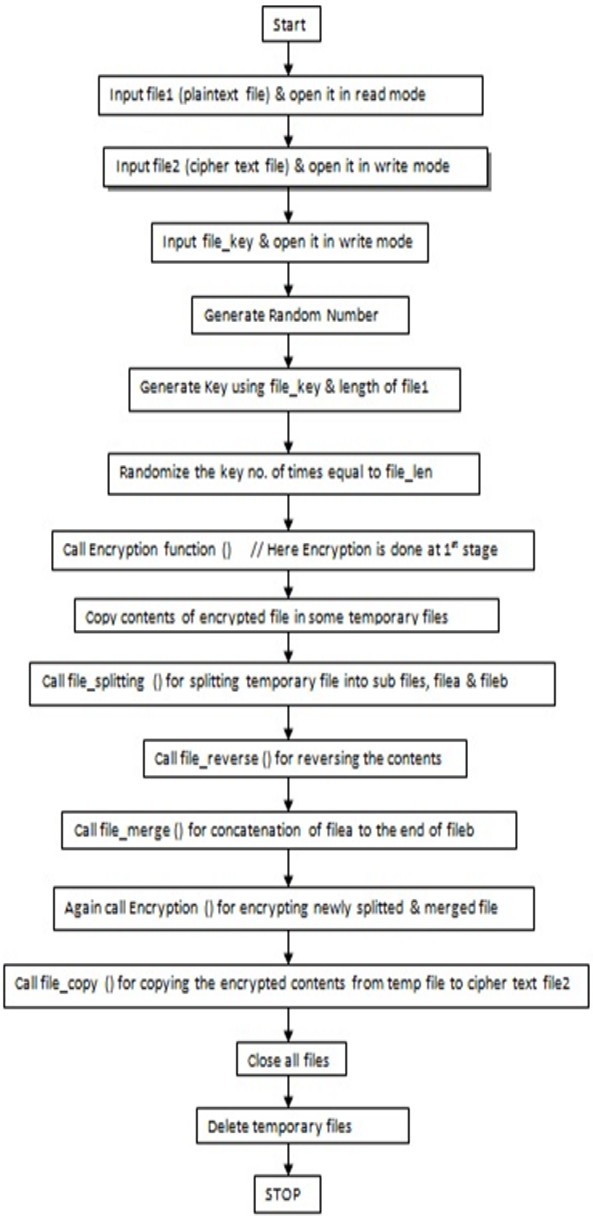

Fig.1: Proposed Algorithm for Encryption using MES-II

5. CONCLUSION

The present method is such that encrypted text cannot be decrypted without knowing the exact initial random key. To generate random key we can use a special random number generator function of Matlab. The program for encryption and decryption can be developed in any Java or Matlab. 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.

REFERENCES

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

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

[3] 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).*

[4] Ultra Encryption Standard(UES) Version-I: Symmetric Key Cryptosystem using generalized modified Vernam Cipher method, Permutation method and Columnar Transposition method: Satyaki Roy, Navajit Maitra, Joyshree Nath,Shalabh Agarwal and Asoke Nath. *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).*

[5] 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, Somdip Dey, Joyshree Nath, Asoke Nath,(IJMECS), ISSN: 2075-0161 (Print), ISSN: 2075-017X (Online), Vol-4, No-5, Page 1-9,2012.*

[6] Symmetric Key Cryptography using Random Key generator: Asoke Nath, Saima Ghosh, Meheboob Alam Mallik: *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).*

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

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

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

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

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