Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 2; January-March, 2015 pp. 140-143
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Cryptography Algorithm for Improving Data Security

T. Aravindhan

UG student (CSE) DSCET Anna university Chennai, India
E-mail: aravindhan42@gmail.com

Abstract—*Cryptography is the process of protecting information from unauthorized persons. It protects its availability, Confidentiality, privacy and integrity. The information stored on computer database is increased greatly. Many of the information stored is highly confidential and not for public viewing. This paper deals with the new cryptography algorithm which is based on block cipher concept. The logical operations like XOR and substitution methods are been used. These results show that proposed algorithm is secured and efficient. I studied about information security and Cryptography techniques and algorithm for presenting this paper. Basic introduction about Information Security using cryptography and detailed description of Information security using cryptography and various algorithms. I am presenting references where I have completed my paper. The proposed algorithm has the better speed compared with the other encryption algorithm. These algorithm improves encryption security by inserting the symmetric layer and it also reduces the time of encryption and decryption than other algorithms. This algorithm can be applied for the practical application which has the same process of encryption and decryption process.*

Keywords: *Cryptography, Encryption, Decryption, Information Security*

1. INTRODUCTION

The program implementation in encryption/decryption is the generation of the encryption key. Now a day, cryptography has many emerging applications. The high level privacy is been provided to the individual groups for protecting confidential information using cryptography. However, the main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: integrity, authentication, availability, confidentiality. Cryptography is the methods that allow information to be sent in a secure from 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. Fig. 1 is representing conventional encryption.

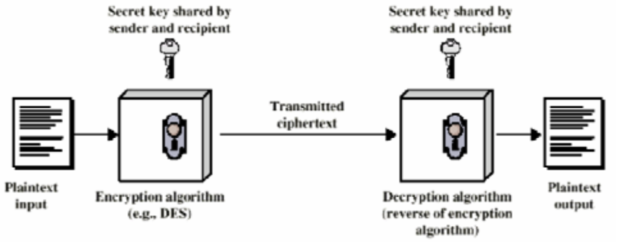

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig. 1: Simplified model of Cryptographic algorithm

Security services: If we are taking about security of information the 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)

SECTION I

Here a newly developed technique named, a new Symmetric key Cryptography Algorithm using extended MSA method: DJSA key algorithm [1] discussed. In this they are suggesting a symmetric key method where they have used an initial key is generated by random key generator and that key is used for encrypting the given source file. In this method basically a substitution method where they take 4 characters area taken from input file and corresponding characters are searched from random key matrix after getting the encrypted message they store the encrypted data in another file. To search characters from the random key matrix they have used a method which was proposed by Nath in MSA algorithm. The key matrix contains possible words comprising of 2 characters each generated from ASCII code is from 0 to 255 in a random order. The Key matrix pattern will depend on text key entered by the user. The own algorithm is been proposed to obtain randomization number and encryption number from the initial text key entered by the user. The own algorithm is been 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 someone wants to break his encryption method then they has to know the exact pattern of the text key. To decrypt any file exact key matrix is to be known to find the random matrix theoretically one has to apply 65536! They have apply method on possible files such as executable file, Word document, Spread sheet document, FoxPro file, text file, image file, pdf file, video file, audio file, oracle database and they have found giving correct solution while encrypting a file and decrypting a file.

The following section the detailed method is discussed

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.

Section II

PROPOSED WORK

In this part presenting a new block symmetric cryptography algorithm. The random number is been used for generating the initial key, where this key will used for encrypting the source file using proposed encryption algorithm with the help of encryption number. Basically this deals with a technique of block based substitution method is used. The encrypting message is provided multiple times in this technique. The 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 key blocks pattern will depend on text key entered by the user. The proposed system using 512 bit key size to encrypt a text message. Finding the two same message through this technique is difficult. 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 2256 trial run and which is not traceable. This technique is possible only for Text document, spread sheet document, word documents.

Encryption Approach

The symmetric encryption approach is been used. The 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 of its efficiency and security. This technique have a common key between sender 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 related to the decryption key, 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.

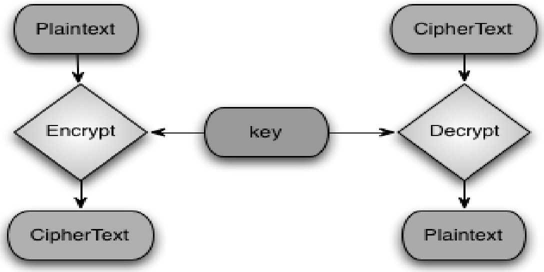


Fig. 2: Basic Concept for Symmetric Cryptography

2. REASONS FOR USING SYMMETRIC APPROACH FOR ENCRYPTION AND DECRYPTION:-

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

3. 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 are store in new Key_Block13.
7. Apply XOR operation between Block2 and Block13. Results are 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

4. STEPS OF PROPOSED ALGORITHM:

1. Initially select plane text of 16 bytes (or we can vary from 16 to 64 depend on requirement).

Initially insert key of size 16 bytes (depend on plane text value)

1. Apply XOR operation between key (Key_Block4213) and plain text block (Text Block). Result will store in Cipher Block1.
2. Apply right circular shift with 3 values. Result will store in new Cipher_Block2.
3. Apply XOR operation between Cipher_Block2 and Key_Block2. Result will store in new Cipher_Block3.
4. Apply XOR operation between Cipher_Block3 and Key_Block4. Result will store in Cipher_Block4.
5. Cipher_Block4 is the input of the next round as a plane text block.
6. Repeat step 1 to 7 till (Encryption Number / 4).
7. Exit.

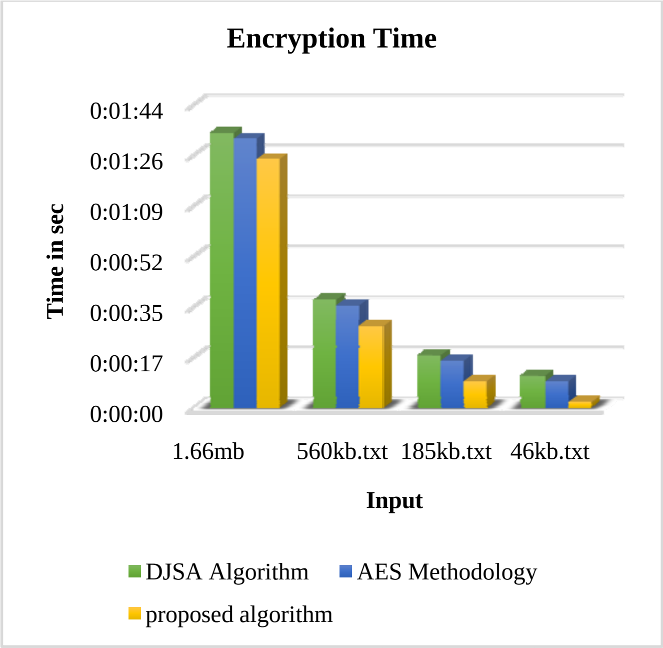
5. RESULT COMPARISONS

I have used 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 proposed cryptography algorithm. 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. The outputs of the 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 Tabulation: 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. The results of text file is shown here. Encryption and Decryption time of Many Text files comparisons shown in table 1 and table 2 accordingly.

Table 1: Encryption time comparisons of text files.

Text Size	DJSA ALGORITHM	ENCRYPTION USING AES METHODOLOGY	PROPOSED ALGORITHM
1.66mb	0.01.34	0.01.32	0.01.25
560kb.txt	0:00:37	0:00:35	0:00:28
185kb.txt	0:00:18	0:00:16	0:00:09
46kb.txt	0:00:11	0:00:09	0:00:02
16kb.txt	0:00:10	0:00:08	0:00:01

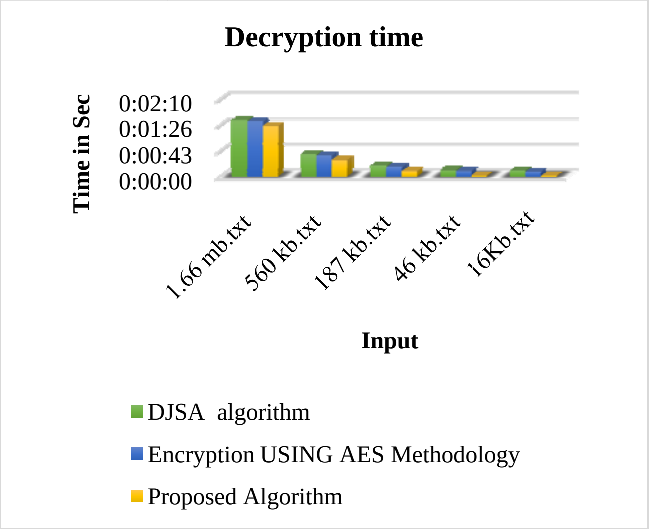


graphical representation for the table 1 and table 2 is shown in Fig. with blue line and green line for encryption time and decryption time of "A Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" and "Effect of Security Increment to Symmetric Data Encryption 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

Table 2: Decryption time comparisons of text files.

Text Size	DJSA algorithm	Encryption USING AES Methodology	Proposed Algorithm
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



6. CONCLUSION

From the result it is clear that our “proposed technique” is batter result producing as compared “DJSA 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. The 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. The propose that this encryption method can be applied for data encryption and decryption in any type of public application for sending confidential data.

7. ACKNOWLEDGEMENTS

I would like to thank Dr. Debdeep Mukhopadhya from IIT Kharagpur for helping through lectures in NPTEL online courses.

I would also like to thank my college management for supporting me in this work.

REFERENCES

[1] 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.

[2] 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.

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

[4] Neal Koblitz “A Course in Number Theory and Cryptography” Second Edition Published by Springer-Verlag.

[5] 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.

[6] 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.

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

[8] 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.

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