IJCSN - International Journal of Computer Science and Network, Volume 3, Issue 6, December 2014
ISSN (Online): 2277-5420 **www.IJCSN.org**
Impact Factor: 0.274

A Step Ahead For Improving Data Security

Tejashree D Pawar

Faculty Of Information Technology,
Government Polytechnic Pune

Abstract - Cryptography allows information to be sent in secure form.Information security protects data availability, privacy and integrity. If we are protecting confidential information then cryptography provides high level of privacy of individuals and groups. Access to stored information on computer databases has increased greatly. More companies store business and individual information on computer than ever before. Much of the information stored is highly confidential and not for public viewing. In this paper a new cryptography algorithm which is based on block cipher concept is presented. In this algorithm logical operation like XOR and shifting operation is used. Experimental results show that proposed algorithm is very efficient and secured**.**

Keywords - *Information security, Encryption, Decryption, Cryptography.*

1. 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.. 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 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. Figure 1 is representing conventional encryption

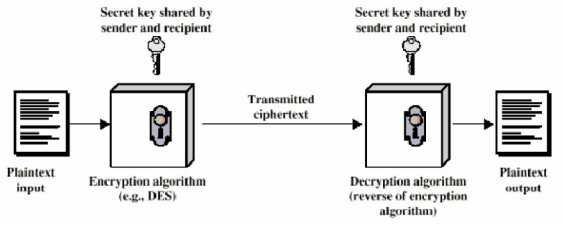

Figure 1: A Simplified Model of Conventional Encryption

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)

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 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.

2. 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 2256 trial run and which is intractable. Initially that technique is only possible for some files such as Microsoft word file, excel file, text file.

3. 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 2.

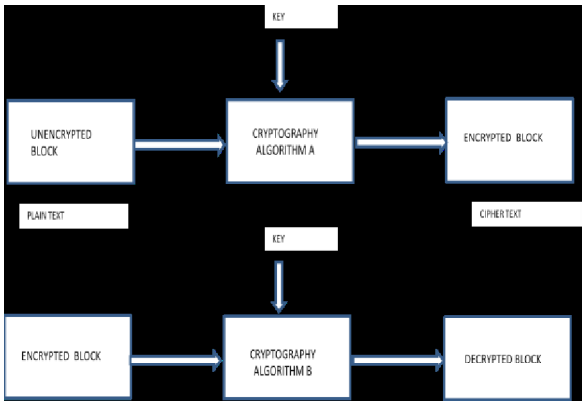

Figure 2: Basic Concept for Symmetric Cryptography

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.

3.1 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

3.2 Steps 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.

4. Results Comparisons

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. In each cycle, same plaintexts are respectively encrypted by "**A newSymmetric key Cryptography Algorithm using extendedMSA method: DJSA symmetric key algorithm"**, **"Effect ofSecurity Increment to Symmetric Data Encryption throughAES Methodology"** and **"Proposed Algorithm (PA)"** bycopying 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 torepresent 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 CryptographyAlgorithm 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 blocksize) 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	DJSA algorithm	Data Encryption through AES Methodology	Proposed Algorithm
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 comparisons of text file

Plain Text in Size	DJSA symmetric Key algorithm	Data Encryption through 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

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 keyCryptography Algorithm using extended MSA method: DJSA symmetric key algorithm"** and **"Effect of Security Increment to Symmetric Data Encryption through AESMethodology"**, respectively and green line is for **"Proposed Algorithm"**. According to the graph, there is a tendency thatencryption/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

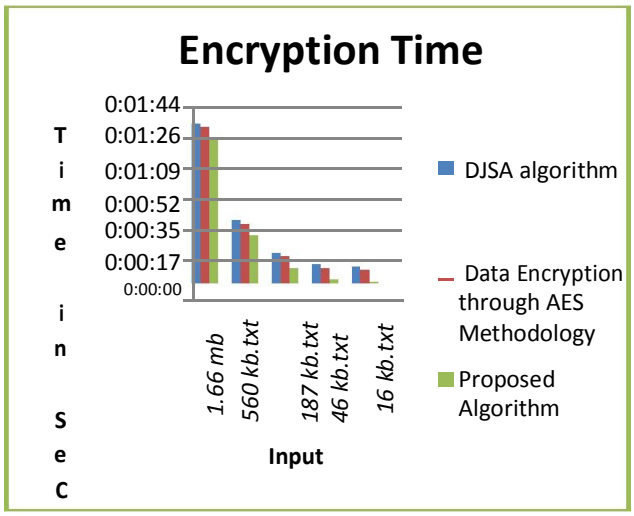

Figure 5: Encryption time comparison of text files between various algorithms with proposed algorithm

5. Conclusion and Future Enhancement

From the result its isclear that our "proposed technique" is better 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] DriptoChatterjee, JoyshreeNath, SuvadeepDasgupta, AsokeNath "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] Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms "2009 International Conference on Computational intelligence and security.

[3] 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

[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