ISSN 2278-5612

Block Cipher Based Cryptographic Algorithm For Data Security

Mohamed Salim Trigui[1], Syed Hamid Hasan[2], Anser Ghazzaal Ali Alquraishee[3]
Information Security Research Group
Faculty of Computing and Information Technology, Department of Information Systems
King Abdulaziz University, Kingdom of Saudi Arabia
shhasan@kau.edu.sa

ABSTRACT

The process of protecting the accessibility, reliability, and secrecy of information is called Information security. We see a great increase in accessing of computer databases for stored information. Increasing number of companies are storing individual and business information on computers. Most of this information is not meant for the public eyes and is very sensitive. The following paper discusses the development of a block cipher based cryptographic algorithm that uses the logical gates like XOR and other shifting operations. The results of the experiment prove the algorithm to be efficient and secure.

Keywords: Cryptography, decryption/encryption, Data Integrity.

Council for Innovative Research

Peer Review Research Publishing System

Journal: International Journal of Management & Information Technology

Vol. 8, No. 3
editor@cirworld.com
www.cirworld.com, member.cirworld.com

ISSN 2278-5612

1. INTRODUCTION

The key function of any decryption/encryption program is to generate the encryption keys. Nowadays, there are many commercial applications of cryptography. Cryptography provides high level of security for groups and individuals if we are to protect confidential information. Yet, providing confidentiality is not the only key aim of cryptography, but it is also aimed at providing solution to issues like: non-repudiation, authentication and data integrity. Cryptography allows sending of information in a secure manner so that only the intended/authorized receiver of the information receives the information sent. Work is being done on finding cryptographic algorithms that provide the above mentioned features. Yet, discovery of these algorithms is not an easy task as the algorithmic research must consider elements such as: space & time complexity, feature of the algorithms and security. Fig 1 represents conventional encryption model.

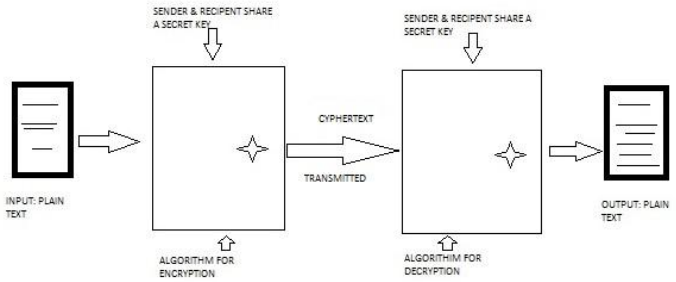

Fig 1 - The Conventional Encryption Model

Security Services: The following services are to be considered when referring to information security:

- Accessibility (permanence, non-erasure)
- Access control (preventing resources misuse)
- Non-repudiation (non-changeability of data)
- Reliability (ensuring data not altered)
- Authentication (Tracking originator and receiver).
- Confidentiality (secrecy).

We will now be discussing the recently developed technique called, “DJSA symmetric key algorithm that is based on the extended MSA method” [1]. The approach suggests use of symmetric keys method, in which a key generator generates a random key initially that is utilized for encryption of the source file. The technique is primarily a substitution technique in which four characters are taken from the source file and searched in a key matrix that is random, once the encrypted message is obtained the data it is stored in a separate file. Nath proposed a search technique in MSA algorithm that is used for searching the character form a key matrix. The technique makes it possible to encrypt the message a number of times over. All possible combination of 2 characters that have an ASCII code between 0 -255 in a random manner are included in the key matrix. The key matrix’s pattern is dependent on the user entered text key. The approach proposes a unique algorithmic method of obtaining the encryption number and the randomization number user entered original text key.

The technique was given a lengthy trial run and found it extremely difficult for matching the 2 parameters described above from two separate text keys. That implies, in order to break the encryption, the exact key text pattern must be known. Decryption of a file would require exact knowledge of the key matrices additionally in order to ascertain this random matrix, it is theoretically required to have 65536! trials run, thus making it impossible to trace. The technique was applied on almost all possible kinds of files such as oracle database, audio file, video file, pdf file, image file, text file, FoxPro file, access database, excel file, word file and executable files with complete success in encryption and decryption of the files. The technique can be utilized for encryption of digital signatures and watermarks before they are embedded in any cover file for making the complete system fully secure. We are going to discuss the technique in detail in the next section.

We would also be discussing the recently developed technique called, “Effects of Security Increments to Symmetric Data Encrypting via AES Methodology” [09]. The technique discusses symmetric cipher algorithms that are similar to Rijndael but have some uncommon things. One of the major differences is, Rijndael algorithm started with a block size of 128 bits, and the block size was increased by adding columns [10], while the other algorithm started with 200 bit.

2. PROPOSED WORK

Under this section we are going to present a new symmetric cryptographic algorithm that is based on the blocks. This technique uses a random number to generate the preliminary key, and then the proposed algorithm, along with the encryption numbers, is applied to encrypt the source file with the key. The approach primarily uses the substitution method based on blocks. The technique supports encryption of the message a number of times. A suggested key block would contain all probable (n) character words that have ASCII values between 0-255 in a random fashion. The key matrix’s pattern is dependent on the user entered text key. The technique was tried

many time and found it extremely difficult for matching the 2 parameters described above from two separate text keys. . . Decryption of a file would require exact knowledge of the key matrices additionally in order to ascertain this random matrix, it is theoretically required to have 65536! trials run, thus making it impossible to trace. For now the method can only be used for Text, MS Word & Excel files.

2.1 Encryption used

The Encryption approached used here is symmetric. As we now know that there are two parts of the symmetric encryption approach First the cryptographic technique that uses symmetric block cipher and the second cryptographic technique that uses symmetric Stream cipher. In the proposed technique we opted for block cipher technique based on its security and efficiency. A common key, known as the private key, exists between the receiver and the sender. <Done> The concept of private keys utilizes symmetric keys under which the plain text is converted to encrypted text (also called cipher text) with the use of the private keys and the decryption of the cipher text into plain text is carried out suing the same private keys. There is a trivial link between the encryption and the decryption keys, in a manner that they are identical or one key can be easily transformed into the other. These keys, in real world, represents the common secret amongst 2 or more entities and is utilized to maintain information private and secure. Symmetric cryptography's pictorial representation can be seen in fig 2.

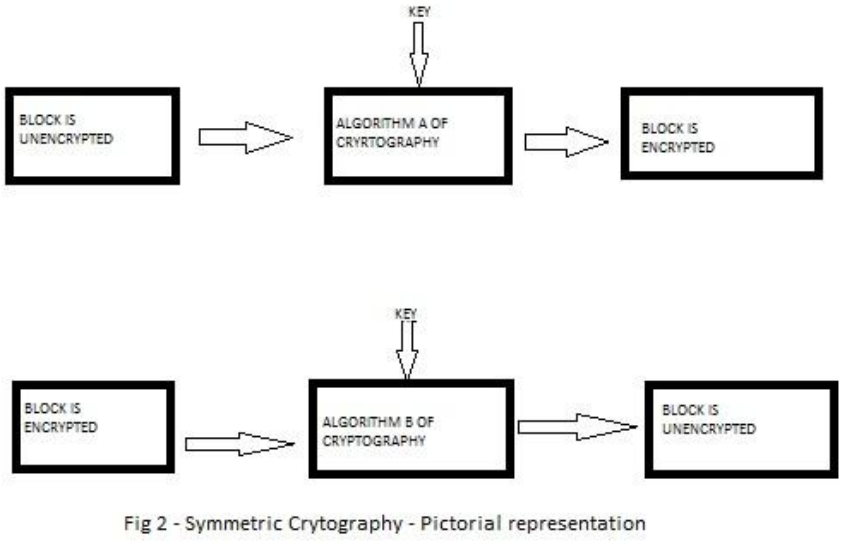

Fig 2 - Symmetric Crytography - Pictorial representation

Why Symmetric Decryption & Encryption:-

- The process of encryption is kept simple.
- The same encrypting algorithm can be shared by all the involved partners rather than developing and exchanging separate algorithms.
- The key length controls Security.
- Higher data throughput rate can be achieved.
- The key length is relatively short.
- It can be used as the basis of developing other cryptographic mechanisms.
- Stronger ciphers can be produced via a combination of Symmetric-key cipher.
- This mode of encryption has a known history of usage and results.

Proposed Steps for Key Generation:

1. A private 256 X 2 bit or 64 char key need to be selected or created.
2. The selected key size would vary between 512 bit to 128 bit or 64 to 16 char.
3. Any char with ASCII code between 0 and 255 can be chosen.
4. 512 bits key means 64 * 8 key length.
5. The 64 byte is divided into four block of 16 byte each, e.g. Key-BlockA, Keu-BlockB, Key-BlockC, and Key-BlockD.
6. XOR operation is applied between BlockA and BlockC. Resulting in new BlockAC.
7. XOR operation is applied between BlockB and BlockAC. Resulting in new BlockBAC.
8. XOR operation is applied between BlockBAC and BlockD. Resulting in new BlockDBAC.
9. Steps 7, 8, 9 are repeated till we get a (random number by 4).
10. End.

Proposed steps for the Algorithm:

1. Select 16 byte plane text (length may vary between 16 and 64 byte as required).
2. Insert 16 byte key (length dependent on value of plane text)

3. XOR operation is applied on the key (BlockDBAC) and plain text block. The results are stored in the Cipher_BlockA.
4. The rightcircular shift is applied alongwith 3 value. The result is stored in the Cipher_BlockB.
5. XOR operation is applied on the Cipher_BlockB and Key-BlockB. The result is stored in the Cipher_BlockC.
6. XOR operation is applied on Cipher_BlockC and Key-BlockD. The result is stored in the Cipher_BlockD.
7. Cipher-BlockD is now treated as plain text input for the following rounds.
8. Step 1 to 7 are repeated till we get an (Encryption Number / 4).
9. Exit.

3. RESULT COMPARISON

While executing two parameters are being used First is value of encryption time and second is time to decrypt, this is demonstrated in table 1 and 2. We are not going to compare time taken to encrypt a plaintext using various cryptographic algorithms against the proposed algorithm. The same Plaintext block is used as an input for the each of the cycles, the algorithms used are

1. "**DJSA symmetric key algorithm that is based on the extended MSA method"**
2. **"Data Encryption through AES Methodology"** and
3. **"Proposed Algorithm (PA)"**

Then, the time taken by each algorithm for execution of the task is measured numerically. Practically, the cryptographic algorithms' complexity is not the only factor deciding the execution time, it also depends on the size of the plain text block.

For the test following were the block sizes for the algorithms

1. 265bit for PA
2. 128 bit for DJSA symmetric key algorithm that is based on the extended MSA method.
3. 128-bit for Data Encryption through AES Methodology.

The test were run through various kinds of data files like images, PDF and text of different sizes and content. However, the following tables depict the results of the Text file type only.

Time taken to Encrypt and Decrypt the different Text file is shown respectively in the tables 1 and 2

Plain Text	DJSA – Time (Min.Sec)	AES Method – Time (Min.Sec)	PA – Time (Min.Sec)
1.68 mb	1.28	1.18	1.1
565 kb	0.35	0.33	0.26
192 kb	0.16	0.14	0.08
53 kb	0.1	0.07	0.06
21 kb	0.09	0.06	0.02

Time taken to Encrypt.- Table 1

Plain Text	DJSA – Time (Min.Sec)	AES Method – Time (Min.Sec)	PA – Time (Min.Sec)
1.68 mb	1.28	1.18	1.1
565 kb	0.35	0.33	0.26
192 kb	0.16	0.14	0.08
53 kb	0.1	0.07	0.06
21 kb	0.09	0.06	0.02

Time taken to Decrypt.- Table 2

Tables 1 and 2 are represented graphically in Fig 1 and 2 where blue line represents time taken to encrypt and decrypt the text file by "DJSA symmetric key algorithm that is based on the extended MSA method" while the red line is for the "AES Methodology for Data Encryption" and the green line represents the "Proposed Algorithm(PA)". The graph clearly shows that with the increase in the file size, the time taken by the different algorithms to encrypt and decrypt the target files, increases. However, we can also see that the time taken by the Proposed Algorithm is considerably less as compared to the other cryptographic algorithms when applied to the same file size.

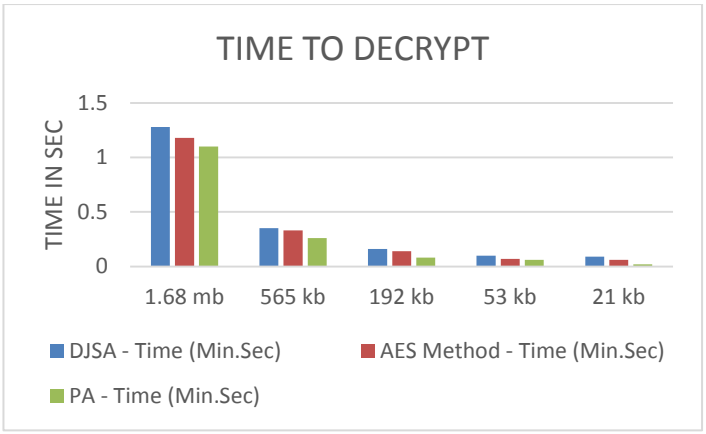

Fig 5: Time Taken to Encrypt

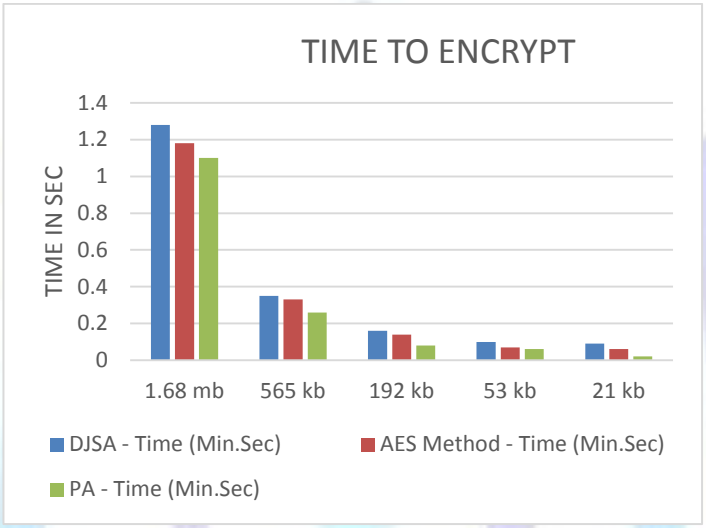

Fig 6: Time Taken to Decrypt

Proposed Technique Characteristic: The Proposed Algorithm has the following visible characteristics:

1. Flexibility.
2. Time efficiency.
3. Distribution.
4. Integration.
5. Availability.
6. Robustness.
7. Efficiency.
8. Security.
9. Simplicity.

CONCLUSION

The results clearly shows that the Proposed algorithm has far better results than the standard techniques vis-à-vis the “Symmetric Key DJSA algorithm based on MSA method and the and “Data Encryption through AES Methodology”. The proposed algorithm can be used by any user who lays emphasis on the value of security in Data and information technology. Since the method is fundamentally the block_cipher method hence it takes small time even for files that are large in size. The key and outstanding feature of proposed method is that it is practically impenetrable and makes the Data as secure as it can be. We would propose the application of this cryptographic algorithm for encrypting and ecrypting of data in any public domain application where data needs to be sent across not very reliable channels or where data is highly confidential like public sector, Military and banks etc.

REFERENCES

[1] 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.

[2] 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.
[3] Symmetric 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-Verlag.
[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 Journal of Computer Science and Security, Volume (1) : Issue (1).
[8] T Morkel, JHP Eloff “ ENCRYPTION TECHNIQUES: A TIMELINE APPROACH” published in Information and Computer Security Architecture (ICSA) Research Group proceeding.
[9] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.
[10] 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.
[11] [Rijn99]Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999.