International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 03, Issue: 01 (JANUARY– FEBRUARY, 2017)

Block Cipher Symmetric Key Based Encryption Algorithm

Ankita Lutoria[1], Prof. Alesh Sharma[2]
Department of Computer Science & Engineering
Technocrats Institute of Technology, Bhopal, India
[1]anki.lutoria@gmail.com, [2]aleshsharma06@gmail.com

Abstract: - As our technologies are advancing day by day, there is always a requirement to modify and updates our existing algorithms accordingly. Whenever a word security comes, confidentiality of our secured data is always required. Many algorithms have been proposed to ensure this need, but there is always a competition to design an algorithm which should be better in some parameters to other. In this research, authors have studied many such algorithms and after deep study on that, proposed their own algorithm called which is better in terms of space, time and security. Authors also implemented and presented their result which shows its efficiency compare to other algorithms.

Keywords - *Encryption, decryption, plain text, cipher text, symmetric key and stream cipher.*

1. INTRODUCTION

The increased use of internet has made world too small in terms of communication. By this communication system transmission of various types of data from one end to another end becomes easier. At one end this is a huge thing but at another end there is also a high risk of information outflow. It is very difficult to control this information outflow completely, but there are certain methods of data hiding through which secure transmission of information becomes possible.

This process of information hiding is called encryption. Several encryption methods have been introduced time by time. Each such method has its own importance in terms of security and encryption time. Cryptography is a set of techniques that provides security to the data being transmitted over the network. It is the study of mathematical techniques that includes the aspects of information security, such as privacy, integrity of data and entity authentication. Confidentiality of data provides keeping information covert from all and can be seen only by the authorized user. Data integrity ensures information has not been altered by unauthorized or unknown means throughout its life cycle. Also there are certain characteristics of cryptographic algorithm. These are level security, performance, and ease of implementation. The term performance refers to the algorithm efficiency calculated in a specific mode of an operation. Ease of implementation refers to the difficulty of realizing the algorithm in practical implementation. There are several aspects of security. They are security service, security mechanism, and security attack. Security service refers to a service that increases the processing of data, system security and information transfers of an organization. Security mechanisms are those which are designed to detect, prevent, or recover from a security attacks. Security attack means any action that can cause harm to the security of data possessed by an organization. Encryption is the technique that covers all these aspects and is a process of converting plaintext to cipher text. To do this it encryption process involves a key. A key is a small or large string of characters that allows a sender to encode the data. Also this key allows the receiver to decode messages sent to him or her. There are certain types of encryption techniques. These include classical techniques, modern techniques, and public-key encryption techniques. Classical techniques are again categorized as substitution and transposition techniques. Substitution techniques are again subdivided in Caesar cipher, mono-alphabetic cipher and poly alphabetic cipher. Block cipher, stream cipher and DES algorithm comes under the modern techniques. In Public-key encryption the RSA algorithm is there. Digital Signatures is also a part of cryptography that looks like in functionality as the hand-written signature and digital certificates are related to an ID -card or some other official documents. There are several applications of cryptography based on communication, identification, secret sharing, electronic commerce, key recovery and remote access. For securing information and protecting data, modern cryptography provides essential techniques.

1.1 Introductory Terms

Encryption: encryption is the process of converting readable form of data into scrambled form called the cipher text. Decryption: It is a process of converting files or documents from an encrypted form (cipher text) to an unencrypted form (plaintext). It is opposite of encryption technique. Plain Text: Plaintext is the original message or filet on which an encryption algorithm is applied. Cipher Text: It is an outcome of the encryption process data, scrambled into unreadable form. Symmetric Key: It involves use of same key for communication by both sender and receiver. Stream Cipher: It is the type of symmetric key encryption in which data is encrypted bit-by-bit.

1.2 Cryptographic Algorithm categories

1.2.1 Symmetric key

Sender and Receiver share a same key. An undisclosed piece of information used to encrypt or decrypt the message. If a key is covert, than only sender or receiver can read the message. If both sender and receiver has secret key, than they may send each other private message. The task of privately choosing a key before communication however can be problematic.

1.2.2 Asymmetric key

Defining the algorithm for solving the key exchange problem which uses two keys, each key is used to encrypt the message. If one is used to encrypt a message, another key must be used to decrypt it. This makes it possible to receive secure message by simply publishing one key (public key) and keeping another secret (private key). Any one may encrypt a message using public key, but only the owner of the corresponding private key is able to read it.

1.3 Goals of cryptography

The main goals of cryptography are [11] confidentially or privacy: Keeping information secret from all and give access to those who are authorized to see it. Confidentially means protection of transmitted data from passive attacks. Data integrity: Ensuring that information has not altered by an unauthorized or unknown means. One must have the ability to detect insertion or some substitution in information by illicit parties. This insertion, deletion, or substitution is called Data manipulation. Authentication: It is a service associated with identification. This function applies to both entities and information. Non-repudiation: It prevents denying of message from either sender or receiver. Thus, whenever any message is transfer then receiver prove it that the message was send by the suspected sender. Similarly, when a message is received, the sender can prove the suspected receiver is receiving that message.

2. LITERATURE SURVEY

In order to provide high security to the data with minimum encryption time several researchers have proposed encryption/decryption algorithm. Symmetric encryption includes conventional block cipher. In symmetric encryption the sender's key remains same as that of the receiver's key. On applying the block cipher algorithm on the plain text cipher text block is obtained and the length of both the block remains same. There are several conventional block cipher algorithms like DES, AES, IDEA and other commonly used encryption algorithm. DES (Data Encryption Standard) uses a 64-bit plain text block as input where 56-bit are used as key and an additional 8-bit are parity bits. The encryption process can be simply summarized as follows: First, plaintext block is divided into two blocks; loop function and sub-key are applied on the half of them; then the output is XOR to the other half; the two halves are exchanged. This process will continue. A total of 16 cycles are performed in DES, including XOR, replacement, substitution, shift operations these four basic operations. Improved DES algorithm is a common Triple DES. Triple DES use 168-bit keys encryption and decryption plaintext block three times.

AES (Advanced Data Encryption Standard) is encryption standard of the 21st century which was designed to replace DES. In AES length of plaintext block and key can be 128-bit, 192-bit, or 256-bit. AES performs multiple rounds of repeat and transformations. The encryption process is performed as : input plaintext is copied to state array for a round of key and output is obtained, then the round function is executed N times to transform the state array, the last transformation is different from the first N-1 times, the final output of the state array is the cipher text.

In Research Paper [1], Akhil Kaushik, Manoj Barnela and Anant Kumar has proposed a new encryption/ decryption algorithm called BEST. It is a simple Encryption/Decryption algorithm which uses multiple random keys to encrypt a single block of data. Use of multiple keys increases the security of the data since it is easy to guess a single key but it is very difficult to guess multiple keys in same sequence. Complexity to break the key is $2^{32}*2^{10}*2^{24} = 2^{64}$. It becomes very difficult to solve 2^{64} in reasonable time (2010).

In Research Paper [2], Neeraj Khanna, Joyshree Nath, Joel James, Amlan Chakrabarti, Sayantan, chakraborty and Asoke Nath proposed an encryption/ decryption algorithm called NJJSAA. To encrypt and decrypt any file NJJSAA uses a bit manipulation method. It is a symmetric key method that uses 256 block cipher text. It takes variable length key having maximum 128 bits which is used to generate two parameters: Random number and encryption number. The combination of these two parameters is used to generates a randomize key having 256 characters. The Randomized key used in NJJSAA increases the security. It needs 2^{256} combination to break the randomized key (2011).

In Research Paper [3] Dripto Chatterjee et.al presented an extension of MSA algorithm. They overcome the weakness of MSA algorithm developed by nath et.al by applying a square key matrix of size 256 by 256. Each cell contains all possible combination of 2-lettered words (ASCII code 0-255). This method will be suitable for encryption of file size 2MB or less. If the file size is

very big then author suggest to choose a small encryption number so that speed of the system can be increased (2011).

In Research Paper [4], Debanjan Das, Megholova Mukherjee, Neha and Joyshree Nath introduced a method which is based on an integrated symmetric key cryptographic, called DJMNA which combines two different methods called (I) Modified Generalized Vernam Cipher (MGVC) and (ii) DJSA method. Generalized Vernam Cipher that uses the concept of "feedback" effect also it reverses the file during encryption process, thus it become very hard to decrypt the data by applying any brute force method (2011).

In Research Paper [5], Aasif Hasan, Neeraj Sharma attempt to create a new method named Name based encryption (NBE) which provides great security level with lesser time complexity. This enhanced technique combines stream ciphering and symmetric ciphering technique. Also a dynamic key concept has been used in the proposed algorithm in which key is decided at the time of encryption. (2014).

In Research Paper [6], Akhil Kaushik Krishan Gupta and Satvika discusses a novel approach to encrypt small amount of data, practically useful for the small scale organizations. It involves the concept of ASK cipher. A concept of bit compression has been used in order to transmit fewer amounts of data over the unsecure channel. Author also shows that their Algorithm performs excellent for smaller organizations (2014).

In Research Paper [7], Md Asif Mushtaque and Harsh Dhiman has proposed a new encryption/ decryption algorithm called AMEA. Author shows that, the proposed algorithm is space & time efficient as well as extremely secure. It performs well for minimum bandwidth channel whose transmission capacity is limited. The algorithm also presents a new concept like random key selection with transposition for better security of data.

3. PROPOSED METHOD

3.1Proposed Algorithm

3.1.1 Encryption Process

1. A random size key is entered by user.
2. This random size key is used to generate a random number (n), by applying the following steps:

a. First, sum all the ASCII value of characters in key.
b. Next, divide the sum by key length and resultant remainder is random number (n).
3. Now, convert the key into binary number format called Key1.
4. Next, by XORing all the bits of Key1 by its random number n^{th} position bits generate a different key called Key2
5. Also, left rotate Key1 by n times and key received called Key3.
6. Now, convert the plaintext in to binary number format (By default all the characters are represented in 8bit format, but to compress the data, this algorithms represent each characters in 7-bit format because all the English characters used in a text can be represented by 7 bit number format)
7. Next, Divide the binary plaintext into equal chunks of binary key size (Last chunk may contain some lesser bits)
8. Repeat the following steps for each chunk:
   a. XOR plaintext with Key1
   b. Left rotate result of step a by n times.
   c. XOR result of step b with Key2
   d. Left rotate result of step c by n times.
   e. XOR result of step d with Key3
9. Result of binary cipher text of chunk first, repeat step 8 for each chunk. If the last chunk have less bits than make all the three keys equal to chunk size during last chunk operation.
10. Now, make the binary cipher text equal to 8 bit multiple sizes by padding 0 at last if required.
11. Last, convert the whole binary cipher text into 8 bit character.

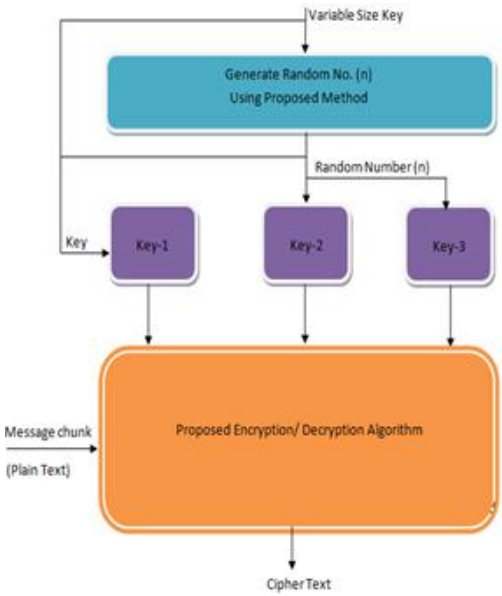

Figure 4: Block diagram of Proposed Algorithm

3.1.2 Decryption Process:

Decryption algorithm is just a reverse process of encryption algorithm.

1. A same key is entered by user.
2. This random size key is used to generate a random number (n), by applying the following steps:

a. First, sum all the ASCII value of characters in key.
b. Next, divide the sum by key length and resultant remainder is random number (n).

3. Now, convert the key into binary number format called Key1.
4. Next, by XORing all the bits of Key1 by its random number n^{th} position bits generate a different key called Key2
5. Also, left rotate Key1 by n times and key received called Key3.
6. Now, convert the Cipher text in to binary number format (By default all the characters are represented in 8bit format.
7. Next, Divide the binary cipher text into equal chunks of binary key size (Last chunk may contain some lesser bits)
8. Repeat the following steps for each chunk:
   a. XOR cipher text with Key3
   b. Left rotate result of step a by n times.
   c. XOR result of step b with Key2
   d. Left rotate result of step c by n times.
   e. XOR result of step d with Key1
9. Result is binary plaintext of chunk first, repeat step 8 for each chunk. If the last chunk have less bits than make all the three keys equal to chunk size during last chunk operation.
10. Now, make the binary cipher text equal to 7 bit multiple sizes by removing 0 from the last.
11. Last, convert the whole binary cipher text into 7 bit character.

4. RESULT ANALYSIS

There are multiple researchers that work on many encryption and decryption algorithm to make it better in terms of security, space & time evaluation. Here I experimentally evaluate AMEA algorithm [7] and proposed algorithm and compare it in terms of throughput, time and space complexity.

4.1 Evaluation Method and Experimental Result of AMEA & Proposed algorithm

Encryption algorithm plays a very important role in network information security. It is essential to evaluate the performance of encryption algorithms. Usually the evaluation includes three parts: security, space and time efficiency. We analyzed the AMEA algorithm [7] and proposed algorithm on these three parameters. In this section, we discussed the experimental results of AMEA algorithm [7] and proposed algorithm on these three parameters with comparison graph.

A. Encryption Speed Evaluation

The encryption speed is the computational quantity that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption speed is used to compute the throughput per unit time of an encryption process. To calculate the encryption speed, total plaintext in bytes is divided by the encryption time. The main work for encryption speed evaluation is to examine the performed encryption time for certain plaintext. Table 1 show the encryption time of AMEA algorithm [7] on various file size.

Table1: Encryption Time and throughput of AMEA Algorithm and proposed algorithm

	AMEA Algorithm		Proposed Algorithm	
	Execution Time	Throughput (Bytes/Sec)	Execution Time	Throughput (Bytes/Sec)
5 KB	0.156	32576.9	0.110	46200.0
10 KB	0.483	20447.2	0.170	58094.8
15 KB	0.937	16008.5	0.35	42857.1
20 KB	1.747	11306	0.480	41150.0
25 KB	2.074	12054	0.65	38461.5

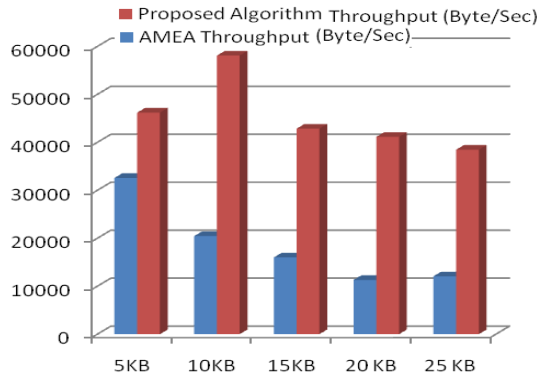

Figure 5: Throughput of AMEA algorithm and Proposed Algorithm

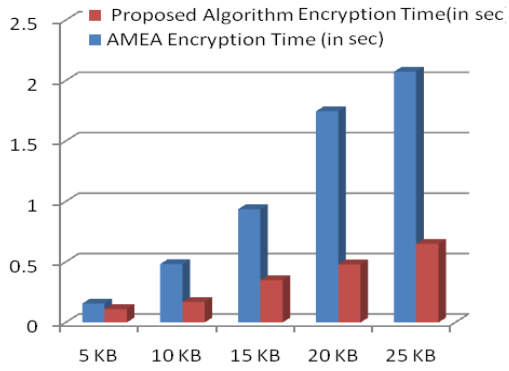

Figure 6: Encryption Time of AMEA algorithm and Proposed Algorithm

Here, it is clearly seen that as file size increases, the encryption speed (throughput) of algorithm decreases. Our algorithm shows the better results as compared to AMEA algorithm.

B. Encryption Security

Information security is the chief concern of the strength of any encryption algorithm. And to provide security to

the data key plays a major role. Higher the complexity of the key less is the chances of information leakage. As discussed, key strength of AMEA is not so powerful. For analyzing the strength of encryption algorithm, Avalanche Effect is calculated. [2] According to the avalanche effect, if the single bit is changed in key, the output must change by 50%. The algorithm close to avalanche effect is more secure against cryptanalysis.

Table 2: Avalanche Effect of AMEA & Proposed algorithm

Avalanche Effect		
Sample	**AMEA Algorithm**	**Proposed Algorithm**
5 KB	34.72	47.97
10 KB	32.71	48.33
15 KB	36.23	48.92
20 KB	34.18	49.37
25 KB	39.87	50.12

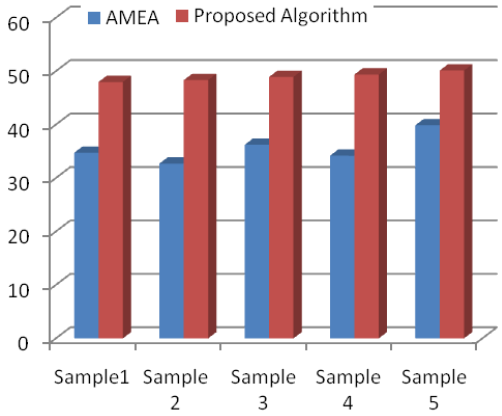

Figure 7: Avalanche Effect of AMEA algorithm and Proposed Algorithm

Table 3: Space Evaluation of AMEA algorithm and Proposed Algorithm

Space Requirement (In Bytes)		
Plain Text File Size	**AMEA Algorithm**	**Proposed Algorithm**
5082	5082	4446
9876	9876	8642
14266	14266	12842
19752	19752	17282
24832	24832	21610

Here, on analyzing the avalanche effect, it is clear from table 2 and figure--- that robustness of the AMEA algorithm is low as its avalanche effect is very low and our proposed algorithm is very robust.

C. Space Evaluation

Space evaluation is required to identify how much space is needed after encryption to store or transmit the cipher text; it is obvious that if the space requirement is more than it will need more time to transmit the data.

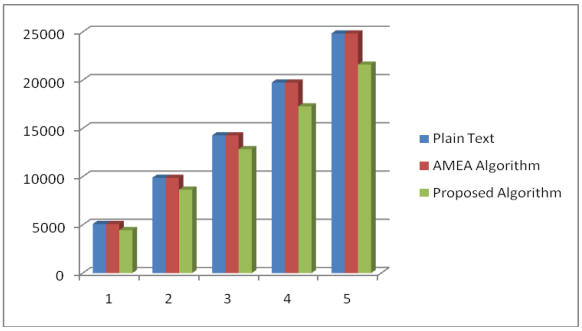

Figure 8: Space Requirement of AMEA algorithm and Proposed Algorithm

Again, it is clearly seen here that space required to store the cipher text is equivalent as to store the plaintext.

5. CONCLUSION & FUTURE SCOPE

Now a day's security of data that has to be transmitted from one location to another location is very challenging task, since transmission of this type of data is very frequent. Observation from literature survey it that there is multiple works has been done on encryption techniques. Some techniques provides the facility to increase the level of security through secure encryption key , some work well in terms of space complexity and some makes their encryption process enough hard so that no one decrypt it by using any brute force method. To sum up, all the previous techniques are useful for real-time encryption application. Each technique is different in its way, and suitable for different applications. New encryption technique is developing everyday therefore prompt and secure conventional encryption techniques will always work out with high rate of security. Here I show the result of algorithm implemented in .net frame work. Following point of Algorithm that makes it fit for sending secure data over the channel. The encryption speed (throughput) of algorithm not decreases as file size increases. Avalanche effect showed that the key strength of Proposed Algorithm is very much powerful. Space requirement to store the cipher text is less as compared to store the plaintext. Results prove that our proposed algorithm shows the better result from AMEA in term of security, space and time. We can use our algorithm in many

application such as mobile ad hoc network, cloud computing, and real time application such as banking services and online payment gateway. Future scope of this research work is to make it more efficient in terms of security, time and space. It can also be integrated with other algorithm to get more benefits.

REFERENCES

[1]. Akhil Kaushik, Manoj Bamela and Anant Kumar "Block Encryption Standard for Transfer of Data" IEEE International Conference on Networking and Information Technology 2010

[2]. Neeraj Khanna, Joel James, Joyshree Nath, Sayantan Chakraborty, Amlan Chakrabarti and Asoke Nath : "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 03-06 June 2011, Page 125-130.

[3]. Dripto Chatterjee et.al "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" IEEE International Conference on Communication Systems and Network Technologies, 2011.

[4]. Das, Debanjan, et al. "An Integrated Symmetric key Cryptography Algorithm using Generalized modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm." Information and Communication Technologies (WICT), 2011 World Congress on. IEEE, 2011.

[5]. Hasan, Aftab, and Neelam Sharma. "A new method towards encryption schemes (Name-based-encryption algorithm)." Optimization, Reliability, and Information Technology (ICROIT), 2014 International Conference on. IEEE, 2014.

[6]. Kaushik, Akhil, and Kunal Gupta. "Ask cipher for small amount of data."Optimization, Reliability, and Information Technology (ICROIT), 2014 International Conference on. IEEE, 2014.

[7]. Mushtaque, Md Asif and Harsh Dhiman. "Implementation of new encryption algorithm with random key selection and minimum space complexity."Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in. IEEE, 2015.

[8]. Dragos Trinca, "Sequential and Parallel Cascaded Convolution Encryption with Local Propagation: Toward Future Directions in Cryptography", Proceedings of The third International Conference on information Technology-New Generations. (ITNG.06), 0-7695-2497- 4 / 2006, IEEE Computer Society.

[9]. Ashwak M. AL-Abiachi, Faudziah Ahmad, Ku Ruhana A Competitive Study of Cryptography Techniques over Block Cipher" IEEE UKSim 13th International Conference on Modeling and Simulation 2011.

[10]. Data Encryption Standard: http:// csrc. nist.gov /publications/fips/fips 46-3 /fips- 46-3.pdf

[11]. Advanced Encryption Standard http://csrc. nist. gov/ publications /fips /fips197/fips- 197.pdf.

[12]. Adam J. Elbirt, Christof Paar. "An Instruction-Level Distributed Processor for Symmetric-Key Cryptography" IEEE Transactions on Parallel and distributed Systems, Vol. 16, No. 5, May 2005.

[13]. G. RAMESH and Prof. Dr. R. UMARANI "UMARAM: A Novel Fast Encryption Algorithm for Data Security in Local Area Network" IEEE ICCCCT'2010.

[14]. William Stallings, "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.