International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 06 (November- December, 2016)

A Review on Different Cryptographic Encryption Decryption Algorithm

Ankita Lutoria
M Tech Student Department of CSE
Technocrats Institute of Technology, Bhopal, India
anki.lutoria@gmail.com

Prof. Alesh Sharma
Department of CSE
Technocrats Institute of Technology, Bhopal, India
aleshsharma06@gmail.com

Abstract: - As the technology is advancing day by day so the use of internet. Internet makes 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 point this is a huge thing but at another end there is also a high risk of information outflow. To control this information outflow completely is very difficult; therefore several methods of information hiding are used to achieve successful transmission of data over the internet without any harm. This process of hiding the information is called encryption. Different encryption methods have been introduced time by time. Each such method has its own importance in terms of security and encryption time. This paper surveys all such kinds of encryption methods that exists and also do the comparative analysis of all the techniques together as a literature survey.

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

1. INTRODUCTION

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.

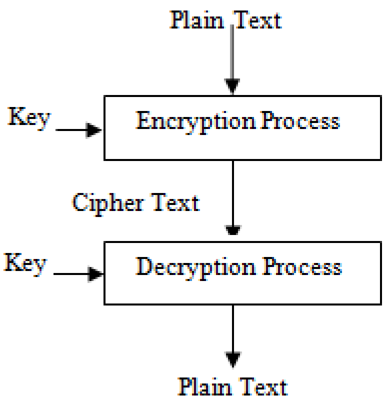


Figure 1: Encryption and Decryption

1.1 Cryptographic Algorithm categories

1.1.1 Symmetric key

Sender and Receiver share a key. A secret piece of information used to encrypt or decrypt the message. If a key is secret, than nobody other than sender or receiver can read the message. If sender and receiver each has secret key, than they may send each other private message. The task of privately choosing a key before communication however can be problematic.

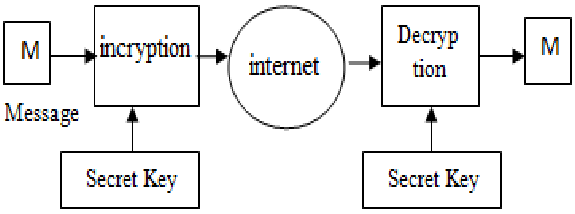


Figure 2 Process of Symmetric Key Encryption Algorithm

1.1.2 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 private key is able to read it.

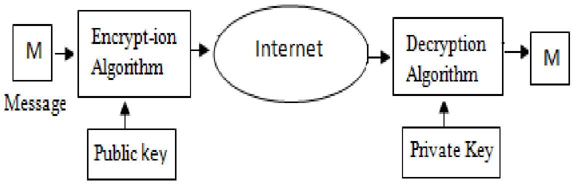


Figure 3 Process of Asymmetric Key Encryption Algorithm

1.2 Goals of cryptography

The main goals of cryptography are [11] Confidentiality or privacy: Keeping information secret from all and giving access to those who are authorized to see it. Protection of transmitted data from passive attacks is called Confidentiality. Data integrity: Ensuring that information has not been 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 proves it that the message was in fact 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

Many researchers have proposed encryption/decryption algorithm to provide high security with minimum time. Conventional block cipher comes under symmetric encryption in which sender's key is same as to the receiver's key. By the Block cipher algorithm we can get a cipher text block from a plaintext block and both of the two blocks have the same length. Conventional block cipher algorithms including DES, AES, IDEA and other commonly used encryption algorithm. DES (Data Encryption Standard) uses a 56-bit key and an additional 8-bit parity bit, and the length of its plaintext block is 64-bit. The encryption process can be simply summarized as follows: First, divide the plaintext block into two blocks; using loop function on the half of them and sub-key; then XOR the output to the other half; and exchange the two halves. This process will continue. DES conducted a total of 16 cycles, using 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 by which the U.S. National Institute of Standards and Technology want to replace DES. In AES plaintext block and key's length can be 128-bit, 192-bit, or 256-bit. It has multiple rounds of repeat and transformations. The encryption process is as follows : copy the input plaintext to state array for a round of key additional and get output, then execute N times the round function 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. It uses multiple random keys to encrypt a block of data. The use of multiple keys increases the security since it is easy to guess a single key but it becomes very hard to guess multiple keys in same sequence. Complexity to break the key is $2^{32}*2^{10}*2^{24} = 2^{64}$. It is near to impossible 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 has presented an encryption/ decryption algorithm called NJJSAA. In this paper they presented a bit manipulation method for data encryption and decryption of any file. It is a symmetric key method which uses 256 block cipher text. It uses variable length key having maximum 128 bits. This key is used to generate two parameters: Random number and encryption number and the combination of these two is used to generate a randomize key having 256 characters. This Randomized key used in NJJSAA increases the security. It needs 2^{256} combination to crack this randomized key (2011).

In Research Paper [3] Dripto Chatterjee et.al presented an extension of MSA algorithm. They conquer the weak point 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). Author's method will also be appropriate 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 key method based on an integrated symmetric key cryptographic, called DJMNA which combines two different methods (i) Modified Generalized Vernam Cipher (MGVC) and (ii) DJSA method. Generalized Vernam Cipher uses the concept of "feedback" effect and it reverses the file during encryption, so it becomes very difficult for the attacker to decrypt the data by applying any brute force method(2011).

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

In Research Paper [6], Akhil Kaushik Krishan Gupta and Satvika discuss an innovative method to encrypt small amount of data that is practically useful for the small scale organizations. Author used the conception of ASK cipher. It is based on the theory of bit compression, therefore fewer amounts of data is transferred over the unsecure channel. Author also shows that their Algorithm performs outstanding for smaller organizations (2014).

In Research Paper [7], Md Asif Mushtaque and Harsh Dhiman has proposed a new concept for encryption/ decryption algorithm called AMEA. Author show that, the algorithm presented in the paper is space & time efficient as well as very secure. It is fine for lower bandwidth channel which has limited transmission capacity. The algorithm has new feature like random key selection with transposition for improved security of data.

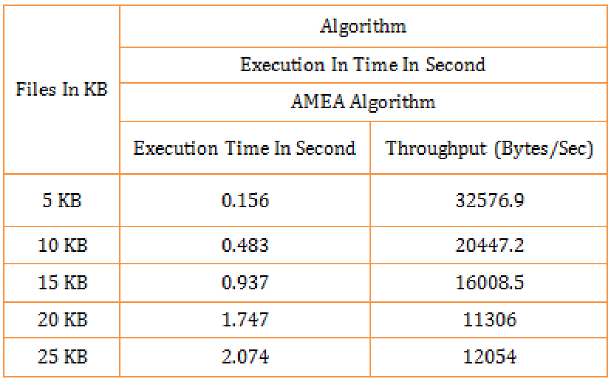
3. COMPARATIVE ANALYSIS

There are various researchers who work on several encryption and decryption algorithms so as to make it more efficient in terms of security, space & time evaluation. Here I experimentally evaluate AMEA algorithm [7] and take it as a base algorithm for my future work.

3.1 Evaluation Method and Experimental Result of AMEA

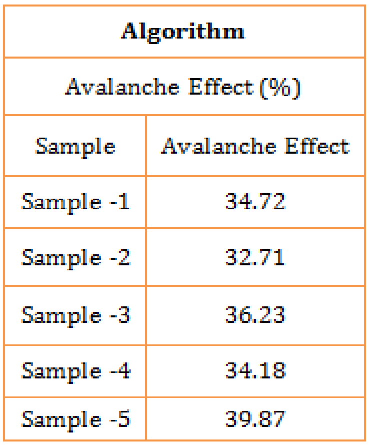
Encryption algorithm has a significant role in network information security. It is crucial to estimate the performance of encryption algorithms. Generally this estimation includes three parts: security, space and time efficiency. We analyzed the **AMEA algorithm** [7] on these three parameters. In this section, we discuss the experimental results on **AMEA algorithm** [7] **on** these three parameters.

Table1: Encryption Time and Speed of AMEA Algorithm



Files In KB	Algorithm	
	Execution In Time In Second	
	AMEA Algorithm	
	Execution Time In Second	Throughput (Bytes/Sec)
5 KB	0.156	32576.9
10 KB	0.483	20447.2
15 KB	0.937	16008.5
20 KB	1.747	11306
25 KB	2.074	12054

Table 2: Avalanche Effect of AMEA algorithm



Algorithm	
Avalanche Effect (%)	
Sample	Avalanche Effect
Sample -1	34.72
Sample -2	32.71
Sample -3	36.23
Sample -4	34.18
Sample -5	39.87

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 calculate the throughput per unit time of an encryption scheme. The encryption speed is calculated as the total plaintext in bytes 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. Here, it is clearly seen that encryption speed (throughput) of algorithm decreases as file size increases.

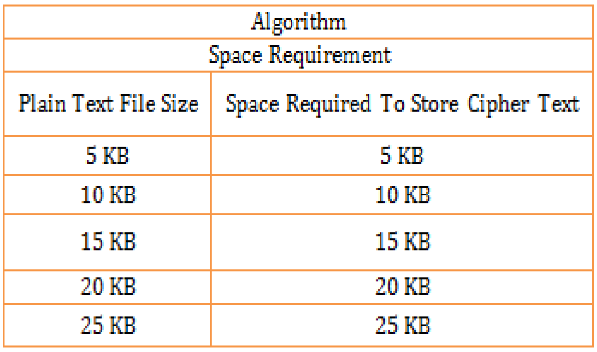
B. Encryption Security

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. 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 shows the avalanche effect of AMEA algorithm [7]. Here, on analyzing the avalanche effect, it is clear that robustness of the algorithm is low as its avalanche effect is very low.

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

Table 3: Space Evaluation of AMEA algorithm



Algorithm	
Space Requirement	
Plain Text File Size	Space Required To Store Cipher Text
5 KB	5 KB
10 KB	10 KB
15 KB	15 KB
20 KB	20 KB
25 KB	25 KB

4. CONCLUSION

Now a day's security of data that is being transmitted from one place to another location is a very tough task, because transmission of such type of data is very regular. Observation from this survey paper depicts that there are multiple works that has been done on encryption techniques. Though some techniques provides the ability to increase the level of security through secure encryption key , while some works well in terms of space complexity and some makes their encryption process sufficient tough so that no one can decrypt it by using any brute force method. To sum up, all the techniques are useful for real-time encryption. Every technique is unlike in its way, and appropriate for different applications. New encryption technique is being developed each day therefore prompt and secure conventional encryption techniques will always work out with high rate of security. Here I have shown the result of AMEA algorithm implemented in .net frame work. Following are the points of AMEA Algorithm that makes it not fit for sending secure data over the transmission channel. The encryption speed (throughput) of algorithm decreases as file size increases. Avalanche effect showed that the key strength of AMEA in not much powerful. Space requirement to store the cipher text is equal as to store the plaintext. So there is need of an algorithm that will show the better result from AMEA in term of security, space and time.

REFERENCES

[1]. Akhil Kaushik, Manoj Bamela And Anantkumar "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 (Jammu) 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, Page 89-94.

[4]. Das, Debanjan, Et Al. "An Integrated Symmetric Key Cryptography Algorithm Using Generalised 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.