A Review of Some Popular Encryption Techniques
Dr. Madhu Goel¹, Rupinder Kaur²
Assistant Professor & HOD¹, P.G. Scholar²
Department of Computer Science & Engineering
Kurukshetra Institute of Technology & Management, Kurukshetra, Haryana, India

Abstract: This paper focuses on the different kinds of symmetric key encryption techniques that exist in present world for securing data communication. It also frames all the techniques related to variety of encryption like image encryption, information encryption, double encryption. It aims to explain the performance parameters that are used in encryption processes and analyzing on their security issues. It helps people to protect their sensitive information from thefts so considered as one of the best tool when it is transmitted via insecure communication channels.

Keywords: Encryption, Decryption, Cryptography, Network Security, Block Ciphering Algorithm.

I. INTRODUCTION
The high growth in the networking technology leads a common culture for interchanging of the digital images very drastically. Hence it is more vulnerable of duplicating of digital image and re-distributed by hackers. Therefore the images has to be protected while transmitting it, sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft. In recent days of Internet, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the internet. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the image security. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, multimedia systems, medical imaging, Tele-medicine and military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered. This paper holds some of those recent existing encryption techniques and their security issues.

A. Basic Terms Used in Cryptography
• Plain Text
The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send “Hello Friend how are you” message to the person Bob. Here “Hello Friend how are you” is a plain text message.
• Cipher Text
The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non-readable message before the transmission of actual message. For example, “Ajd672#@91ukl8*^5%” is a Cipher Text produced.
• Encryption
A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.
• Decryption
A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.
• Key
A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text “President” then Cipher Text produced will be “Suhvlghqw”.

B. Purpose of Cryptography
Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography. [1]

- **Confidentiality**
  Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

- **Authentication**
  The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

- **Integrity**
  Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

- **Non Repudiation**
  Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

- **Access Control**
  Only the authorized parties are able to access the given information.

C. Classification of Cryptography
Encryption algorithms can be classified into two broad categories- Symmetric and Asymmetric key encryption.

- **Symmetric Encryption**
  In symmetric Cryptography the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6, BLOWFISH.

![Fig. 1: Overview of Most Common encryption algorithm](image)

II. PURPOSED WORK
Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices has done by D. S. Abdul.Elminaam et al., (2009) presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. Several points can be concluded from the Experimental results. First; in the case of changing packet size with and without transmission of data using different architectures and different WLANs protocols, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. DES and 3DES are known to have worm holes in their security mechanism, Blowfish and AES do not have any so far [5]. Evaluation of Performance Characteristics of Cryptosystem Using Text Files designed by Challa Narasimham and Jayaram Pradhan (2008) - They performed the performance comparison for variable sized text files as input. An analysis on computational running times results in significant difference among the methods. He believe in that the performance of DES, especially in decryption method is very high than the alternatives. Despite the key distribution, DES is more suitable to the application, which has the decryption as the highest priority. He has proposed and performed the test cases on the two PKCS methods i.e., RSA and NTRU Though the encryption, decryption and complexity are high in NTRU, the RSA provides the highest security to the business.
application. He presented all these parameters with computational running times for all the methods, so as to select the appropriate method [7].

Abdel-Karim and his colleague Al Tamimi presented simulation results showed that Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, which makes it an excellent candidate to be considered as a standard encryption algorithm. AES showed poor performance results compared to other algorithms since it requires more processing power.

P. Prasithsangaree and his colleague P. Krishnamurthy have analyzed the Energy Consumption of RC4 and AES Algorithms in Wireless LANs in the year 2003. They have evaluated the performance of RC4 and AES encryption algorithms. The performance metrics were encryption throughput, CPU work load, energy cost and key size variation. Experiments show that the RC4 is fast and energy efficient for encrypting large packets. However, AES was more efficient than RC4 for a smaller packet size. From the results, it appears that we can save energy by using a combination of RC4 and AES to provide encryption for any packet size. The tradeoffs with security are not completely clear [9].

Comparative Analysis of AES and RC4 Algorithms for Better Utilization has designed by Nidhi Signal, J.P.S.Raina in the year (2011). The performance metrics were throughput, CPU process time, memory utilization, encryption and decryption time and key size variation. Experiments show that the RC4 is fast and energy efficient for encryption and decryption. Based on the analysis done as part of the research, RC4 is better than AES we compare the encryption time of AES and RC4 algorithm over different packet size. RC4 takes less time to encrypt files w.r.t. AES. In AES, CFB and CBC takes nearly similar time but ECB takes less time then both of these [10].

Efficiency and Security of Some Image Encryption Algorithms Marwa Abd El-Wahed et.al (2008) – worked in this paper, four image encryption algorithms have been studied by means of measuring the encryption quality, the memory requirement, and the execution time of the encryption. In addition, the security analysis of these schemes is investigated from cryptographic viewpoint; statistical and differential attacks. The results are compared, focusing on those portions where each scheme is performed differently. A Comparative Study of Two Symmetric Encryption Algorithms across Different Platforms designed by S. A. M. Rizvi et.al. All algorithms run faster on Windows XP. The CAST runs slower than AES for text. Blowfish encrypts images most efficiently on all 3 platforms, even CAST runs faster on Windows XP for image data. But on Windows Vista and Windows 7, AES and CAST perform at the similar speed. CAST performs better than BLOWFISH and AES on Windows XP for encrypting audio files, but on Windows Vista and Windows 7, there is no significant difference in performance of CAST and AES, however BLOWFISH encrypts audio files at less speed for audio files[12].

Throughput Analysis of Various Encryption Algorithms presented by Gurjeewan Singh et al.,(2011)- For experiment a Laptop with 2.20 GHz C.P.U., 4GB RAM Core-2-Dou Processor and Windows 7 Home Premium (32-Bit) is used in which the performance data are collected. In this experiment software encrypts the text file size that ranges from 20 Kb to 99000 Kb. Their implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm. The performance matrices are throughput. The throughput of encryption as well as decryption schemes is calculated but one by one. In the case of Encryption scheme throughput is calculated as the average of total plain text in k bytes divided by the average Encryption time and in the case of Decryption scheme throughput is calculated as the average of total cipher text is divided by the average Decryption time. This work presents the performance evaluation of selected symmetric algorithms. The selected algorithms are AES, 3DES, Blowfish and DES. The presented simulation results show the numerous points. Firstly it was concluded that Blowfish has better performance than other algorithms followed by AES in terms of throughput. Secondly 3DES has least efficient of all the studied algorithms [15].

Shashi Mehrotra Seth and her colleague Rajan Mishra(2011) jointly has done a Comparative Analysis Of Encryption Algorithms For Data Communication. The authors analyse the performance of encryption algorithm is evaluated considering the following parameters like Computation Time, Memory usage and Output Bytes, RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm [17].


Idrus.S.Z, Aljunid.S.A, Asi.S.M (2008), done the research [22]work in the different browsers for evaluate the Performance Analysis of Encryption Algorithms Text Length Size. The authors study of security measure level has been proposed for a web programming language to analyze four Web browsers. This study consider of
Monika Agrawal et al. 2012 gives a detailed study[24] of the popular symmetric key encryption algorithms such as DES, TRIPLE DES, AES, and Blowfish. Symmetric Key algorithms run faster than Asymmetric Key algorithms such as RSA etc and the memory requirement of Symmetric algorithms is lesser than Asymmetric encryption algorithms. Further, the security aspect of Symmetric key encryption is superior than Asymmetric key encryption.
Ezedin Barka and his colleague Mohammed Boulmalf conducting two experiments[25] scenarios that were conducted for the purpose of establishing a baseline and for understanding the impact of adding encryptions, with different key sizes, used by WEP and WPA security protocols on UDP and TCP WLAN traffic. While the first experiment was for measuring the throughput under normal conditions (No encryption applied), the second experiment was to analyze the variation of traffic throughputs over an Infrastructure network when encryption is applied. The general observations taken from these experiments are: Throughput decreases when security, WEP and WPA are enabled. This is due to the fact that encryption operations performed by these protocols increase the amount of data transmitted and slow down the rate of data being sent or received.
G. Ramesh et.al designed al algorithm in the year 2010 named as UMARAM[27]. The UMARAM is a Symmetrical encryption algorithm. The key generation generates 16-keys during 16-rounds. One key of them is used in one round of the encryption or decryption process. The new algorithm uses a key size of 512-bits to encrypt a plaintext of 512-bits during the 16-rounds. In this Algorithm, a series of transformations have been used depending on S-BOX, different shift processes, XOR-Gate, and AND-Gate. The S-Box is used to map the input code to another code at the output. It is a matrix of 16×16×16. The S-Box consists of 16-slides, and each slide having 2-D of 16×16. The numbers from 0 to 255 are arranged in random positions in each slide.
G. Ramesh et.al designed an algorithm in the year 2010 named as UR5[28]: A block encryption algorithm is proposed in this approach. In this Algorithm, a series of transformations have been used depending on S-BOX, XOR-Gate, and AND-Gate. The proposed algorithm encrypts a plaintext of size 64-bits by a key size of 64-bits. It uses eight rounds for encryption or decryption process. It overcomes some drawbacks of the other algorithms. The Tiny Encryption Algorithm (TEA) was created by David Wheeler and Roger Needham of Cambridge University and published in 1994. It was designed for simplicity and performance, while seeking an encryption strength on par with more complicated and resource-intensive algorithms such as DES (Data Encryption Standard). Wheeler and Needham summarize this as follows: “it is hoped that it can easily be translated into most languages in a compatible way... it uses little set up time and does... enough rounds to make it secure... it can replace DES in software, and is short enough to write into almost any program on any computer”[30]. Wheeler, David J. and Needham, Roger M. TEA Extensions. (XTEA) Computer Laboratory, Cambridge University, England, October, 1997. They proposed 64 bit block cipher, which features 128 scheduled keys. The keys are scheduled dynamically at runtime, and require no memory. Assuming that all five bits used in the rotation count have a probability of 1/2 and each key word has a probability of 1/4, each scheduled key would have a probability of 1/128[31].
Kazumaro Aoki, Tetuya Ichikawaz, Masayuki Kanday, Mitsuru Matsuiz, Shiho Moriaiz, Junko Nakajimaz, Toshio Tokitaz jointly have done a research work on block cipher Camillia which supports 128-bit block size and 128-, 192-, and 256-bit keys, i.e. the same interface specications as the Advanced Encryption Standard (AES). Efficiency on both software and hardware platforms provides high level of security. It implemented in assembly language which can encrypt on a Pentium III (800MHz) at the rate of more than 276 Mbits per second, which is much faster than the speed of an optimized DES implementation. The hardware design, which includes both encryption and decryption, occupies approximately 11K gates, which is the smallest among all existing 128-bit block ciphers[32].

III. CONCLUSION

In this paper the existing encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way; which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

REFERENCES


Abdel-Karim Al Tamimi,” Performance Analysis of Data Encryption Algorithms”


Dr. S.A.M Rizvi1 Dr. Syed Zeeshan Hussain2 and Neeta Wadhwa” A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms”,


