Volume 4, Issue 8, August 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Comparative Analysis of Symmetric Key Encryption Algorithms

Narender Tyagi
Research Scholar
Department of Computer Science
Himachal Pradesh University Shimla, India

Anita Ganpati
Associate professor
Department of Computer Science
Himachal Pradesh University Shimla, India

Abstract- Computer networks were primarily used by university researchers for studying e-mail, and by corporate employees for sharing printers. Security was not an important issue at that time. But now as billions of ordinary citizens are using networks for banking, shopping, and filling their income tax returns. Network security has become an important issue and potentially massive problem in data communication. Most security problems are intentionally caused by malicious people trying to gain some benefit or harm someone. Encryption has come up as a solution, and plays an important role in information security system. In this paper a detailed theoretical study has been made on the DES, 3DES, AES and Blowfish symmetric encryption algorithms. A comparative analysis on the above symmetric encryption algorithms has been made. These algorithms consume a significant amount of computing resources such as CPU time, memory and battery power. The comparison is made on the basis of these parameters: speed, block size, and key size etc. Blowfish has better performance than other DES, 3DES, and AES algorithms.

Keywords- Encryption, Decryption, Cryptography, Data Encryption standard(DES), Asymmetric Encryption standard(AES), Symmetric Encryption, Asymmetric Encryption

I. INTRODUCTION

In the era of Information technology, billions of ordinary citizens are using networks for entertainment, education, and banking, shopping, and filling their Income tax returns. Network security is looming on the horizon as a potentially massive problem. Network security problem can be divided roughly into four intertwined areas: Secrecy, authentication, non-repudiation and integrity control [19].Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce [7].

Cryptography is the study of Secret (crypto-) writing (-graphy) that is concealing the content of message from all except the sender and the receiver and to authenticate the correctness of message to the recipient. It is concerned with making sure that nosy people cannot read, or worse, modify messages intended for other recipients [19]. Cryptography is the field of network security which provides methods or algorithms to secure the information by hiding its meaning. It means that cryptography can convert the information from its readable form to unreadable form. If anyone tries to change or read information illegally than he cannot do so because the information is not readable until it is reconverted to readable form which is only possible by the mechanism of cryptography. Overall, Cryptography is an area which has been used around for centuries and has helped in securing information. It has evolved over time and it is still evolving as peoples can see through the researches going on in the area[22]. The process of cryptography is described in figure 1:

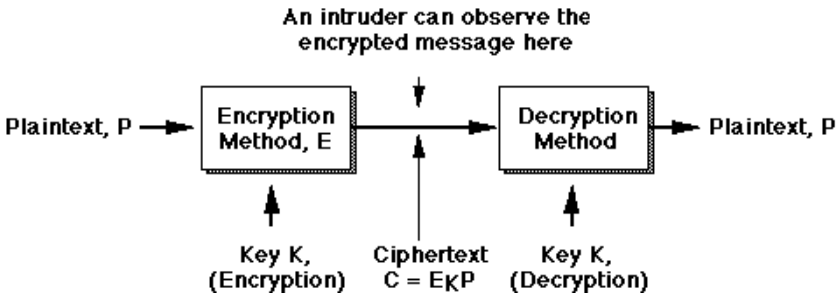

Figure 1: Cryptography Process

From figure 1, it is observed that it is useful to have a notation for relating plaintext, ciphertext, and keys. The term $C = E_K(P)$ represents the encryption of the plaintext P using key K gives the ciphertext C. Similarly, $P = D_K(C)$ represents of decryption of C to get the plaintext P again. It follows that

$$D_K(E_K(P)) = P$$

A fundamental rule of cryptography is that one must assume that the cryptanalyst knows the general method of encryption used. The cryptanalyst knows how the encryption method, E works [19]. Basic Terminology used in cryptography are: Plain text – It is the original message; Cipher text – It is the coded message; Cipher - The algorithm for transforming plaintext to cipher text; Key – The info used in cipher known only to sender/receiver; Encipher (encrypt) – Process of converting plaintext to cipher text; Decipher (decrypt) – Process of recovering cipher text from plaintext; Cryptography - The study of encryption principles/methods; Cryptanalysis (code breaking) – The study of principles/methods of deciphering Cipher text without knowing key; Cryptology –It is the field of both cryptography and cryptanalysis. The Objectives of Cryptography are [7]: Confidentiality, Authentication, Integrity, and Non-Repudiation. Cryptography Algorithms are used to prevent malicious attack on the transmitted data. On the basis of key used, cryptography algorithms are divided into two groups.

The process of encryption and decryption of information by using a single key is known as secret key cryptography or symmetric key cryptography. In symmetric key cryptography, the same key is used to encrypt as well as decrypt the data. The main problem with symmetric key algorithm is to exchange the secret key between the sender and the receiver. A secure channel is also required between the sender and the receiver to exchange the secret key [19]. Symmetric algorithms are of two types: Block ciphers and Stream ciphers [24]. In cryptography, a block cipher is a deterministic algorithm operating on fixed-length groups of bits, called *blocks*, with an unvarying transformation that is specified by a symmetric key. Many block ciphers have a Feistel structure. Such a structure consists of a number of identical rounds of processing. In each round, a substitution is performed on one half of the data being processed, followed by a permutation that interchanges the two halves. The original key is expanded so that different key is used for each round [19][24]. A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (key stream). In a stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the key stream, to give a digit of the cipher text stream. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. Stream ciphers are mainly of two types: Self-synchronizing stream ciphers calculate each bit in the key-stream as a function of the previous n bits in the key stream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit key-stream it is. Synchronous stream ciphers generate the key-stream in a fashion independent of the message stream but by using the same key-stream generation function at sender and receiver [7][19].

In Asymmetric key cryptography different keys are used for encryption and decryption. Asymmetric cryptography refers to a cryptographic algorithm which requires two separate keys, one of which is *secret* (or *private*) and one of which is *public*. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt cipher text or to create a digital signature [7] [19].

II. SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS

In the recent years, there has been a great need for much improved techniques of securely transmitting and storing information. The field of cryptography encompasses some of these requirements and has been focus of a growing research effort. The core of this field is the efficient realization of cryptography algorithms in software and/or hardware. The introduction of such algorithms started at the 70's. Some commonly used symmetric key encryption algorithms are described as:

A. Data Encryption Standard (DES)

DES was the result of a research project set up by International Business Machines (IBM) Corporation in the late 1960's which resulted in a cipher known as LUCIFER. The altered version of LUCIFER was put forward as a proposal for the new national encryption standard requested by the National Bureau of Standards (NBS). It was finally adopted in 1977 as the Data Encryption Standard –DES. DES is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. Once a plain-text message is received to be encrypted, it is arranged into 64 bit blocks required for input. If the number of bits in the message is not evenly divisible by 64, then the last block will be padded [19][24].

DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks, L_i and R_i which are then passed into 16 rounds (the subscript i in L_i and R_i indicates the current round). Each of the rounds are identical and the effects of increasing their number are twofold - the algorithms security is increased and its temporal efficiency decreased. Clearly these are two conflicting outcomes and a compromise must be made. For DES the number chosen was 16, probably to guarantee the elimination of any correlation between the ciphertext and either the plaintext or key. At the end of the 16th round, the 32 bit L_i and R_i output quantities are swapped to create what is known as the pre-output. This [R16, L16] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit ciphertext [21] [23].

B. Triple Data Encryption Standard (3DES)

In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Because of the availability of increasing computational power, the key size of the original DES cipher was becoming

subject to brute force attacks; Triple DES was designed to provide a relatively simple method of increasing the key size of DES to protect against such attacks, without designing a completely new block cipher algorithm. Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Private Encryptor, we simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user provided key into three subkeys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key [22].

C. Advanced Encryption Standard (AES)

AES emerged as a powerful replacement of DES during a competition held by National Institute of Standard and Technology (NIST). The competition was organized to develop a substitute of existing DES. Rijndael: an algorithm designed by Daemen and Rijmen was judged the best and announced to be new AES. NIST choose Rijndael, due to its simplicity and high performance. It is fast, compact, and has a very simple mathematical structure [4].AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits; called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds [23].

The main loop of AES performs the following functions: 1. SubBytes () 2. ShiftRows () 3. MixColumns () 4. AddRoundKey (). The first three functions of an AES round are designed to thwart cryptanalysis via the Methods of "confusion" and "diffusion." The fourth function actually encrypts the data. AES formats plaintext into 16 byte (128-bit) blocks, and treats each block as a 4x4 State array. It then performs four operations in each round. The arrays contains row and column information used in the operations, especially MixColumns () and Shiftrows (). AES can be attacked using the Timing analysis Attack. This occurs when Malice (the malicious Alice) runs the Sub-Bytes method on different data and observes the time it takes for each execution.

D. Blowfish

Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use [17]. Blowfish is a variable length key, 64 bit block cipher. The algorithm consists of two parts: a key expansion part and a data-encryption part. Key expansion converts a key of at most 448 bits into several sub-key arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, and a key and data dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round [13].

The time consuming sub-key generation process adds considerable complexity for a brute-force attack. The sub-keys are too long to be stored on a massive tape, so they would have to be generated by a brute-force cracking machine as required. Since the key size is larger it is complex to break the code in the Blowfish algorithm.

III. REVIEW OF LITERATURE

Network security and cryptography challenges and issues are discussed by various researchers. In this section various literature reviews of different researchers are presented.

Singh et al. [16] made the comparison between DES, 3DES, AES and Blowfish symmetric algorithms. The comparison had been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithms encryption/decryption speed. It was concluded that Blowfish has better performance than other commonly used encryption algorithms. AES showed poor performance results as compared to other algorithms, because it required more processing time.

Cornwell [5] discussed the design of Bruce Schneier's Blowfish encryption algorithm along with a performance analysis and possible attacks. It was concluded about the effectiveness of Blowfish with the other well known algorithms DES, 3DES, and AES. It was concluded that Blowfish is able to provide long term data security without any known backdoor vulnerability or ability to reduce the key size. For the future scope Blowfish was considered safe and effective design although future reevaluations will be needed.

Tamimi [18] compared DES, 3DES, AES and Blowfish symmetric algorithms. The performance of these algorithms under different settings, and different data loads were considered. This study used two modes of operation i.e. ECB and CBC for calculating execution time of each algorithm. This study used C# programming language for simulation. It was concluded that Blowfish has better performance than other commonly used encryption algorithms. AES showed poor performance results as compared to other algorithms, because it required more processing time. CBC mode had added extra time, but it was relatively negligible.

Nadeem [11] discussed the popular secret key algorithms DES, 3DES, AES (Rijndael), Blowfish and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented in Java programming language, and were tested on different hardware platforms, to present the comparison. The two different machines were: P-II 266 MHz and P-IV 2.4 GHz. It was concluded that Blowfish had an advantage over other algorithms. Also it showed that AES has better performance than DES and 3DES. Also it was concluded that 3DES needs 3 times than DES to process the same amount of data.

Dhawan [6] compared the performance of the different encryption algorithms by conducting experiments inside .NET framework. The comparison was performed on the following algorithms: DES, 3DES, RC2, and AES (Rijndael). It was concluded that AES outperformed other algorithms in both the number of requests processes per second in different user loads, and in the response time in different user-load situations.

Singh et al. [15] performed a comparison between the most common four encryption algorithms namely; AES, DES, 3DES and Blowfish in terms of security and power consumption. Experiment results of comparison were carried out over different data types like text, image, audio and video. The simulation results showed that AES has a better performance than other common algorithms. AES is supposed to be better algorithm which was compared to original Blowfish Algorithm. But adding additional key and replacing the old XOR by new operation '#' as a purposed by this study to give more robustness to Blowfish Algorithm and make it stronger against any type of intrusion. This advance Blowfish Algorithm is more efficient in energy consumption and security to reduce the consumption of battery power device.

Agrawal et al. [2] made a detailed study 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. It was concluded that the supremacy of Blowfish algorithm over DES, AES and Triple DES on the basis of key size and security. The F function of Blowfish algorithm provides a high level of security to encrypt the 64 bit plaintext data. Also the Blowfish algorithm runs faster than other popular symmetric key encryption algorithms.

Seth et al. [14] made a comparative analysis of three algorithms**,** DES, AES and RSA considering certain parameters such as computation time, memory usages and output byte. A cryptographic tool was used for conducting experiments. It was concluded that RSA consumes longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm. Based on the text files used and the experimental result it was concluded that DES consume least encryption time and AES has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm.

Mandal et al. [9] made the comparison between four most commonly used Symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of parameters: round block size, key size, encryption/decryption time, and CPU process time in the form of throughput and power consumption. It was concluded that blowfish is better than other algorithms. Also AES has advantage over the other 3DES and DES in terms of throughput and decryption time. 3DES has least performance among all mentioned algorithms.

Apoorva et al. [4] compared most common symmetric cryptography algorithms: AES, TWOFISH, CAST-256 and BLOWFISH. The comparison took into consideration the behavior and performance of algorithms when different data loads were used. The comparison was made on the basis of these parameters: speed, block size, and key size. It was concluded that blowfish is superior to other algorithm as it takes less time. Although when the data size was very small this difference was not clearly visible. But for file having size greater than 100 KB, it was very clearly visible.

Abdul et al. [1] discussed six most common encryption algorithms such as AES (Rijndael), DES, 3DES, RC2, BLOWFISH and RC6. These algorithms were compared and performance was evaluated. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. It was concluded that there is no significant difference when the results are displayed either in Hexadecimal Base encoding or in Base 64 encoding. Secondly in the case of changing packet size, it was concluded that BLOWFISH has better performance than other common encryption algorithms used, followed by RC6. Also in the case of changing data type such as image instead of text, it was found that RC2, RC6 and BLOWFISH has disadvantage over other algorithms in terms of time consumption. Also, it was found that 3DES still has low performance compared to algorithm DES. Finally in the case of changing key size, it can be seen that higher key size leads to clear change in the battery and time consumption.

Thakur et al. [20] discussed a fair comparison between three most common symmetric key cryptography algorithms: DES, AES and Blowfish. The main concern was the performance of the algorithms under different settings, the presented comparisons takes into consideration the behavior and performance of the algorithms when different data loads are used. The comparison was made on the basis of these parameters: speed, block size, and key size. Simulation program was implemented using java programming. It was concluded that blowfish has better performance than other common encryption algorithms used.

Marwaha et al. [10] discussed three algorithms DES, 3DES and RSA. DES and 3DES are symmetric key cryptographic algorithms and RSA is an asymmetric key cryptographic algorithm. Algorithms have been analyzed on their ability to secure data, time taken to encrypt data and throughput the algorithm requires. Performance of different algorithms was different according to the inputs. It was concluded that confidentiality and scalability provided by 3DES over DES and RSA is much higher and makes it suitable even through DES consumes less power memory and time to encrypt and decrypt the data but on security from DES can be easily broken by brute force technique as compared to 3DES and RSA, making it the last secure algorithm.

Alam et al. [3] discussed performance and efficiency analysis of different block cipher algorithms (DES, 3DES, CAST-128, BLOWFISH, IDEA and RC2) of symmetric key cryptography. Block cipher algorithms has been compared based on the factors: input size of data(in the form of text, audio and video), encryption time, decryption time, throughput of encryption and decryption of each block cipher and power consumption. It was concluded that 3DES has more power consumption and less throughput than the DES due to its triple phase characteristics. Throughput of CAST-128 was

better than DES, 3DES and IDEA. RC2 was faster for smaller sizes of input data as compared to BLOWFISH algorithm because it has only one P-Box for key expansion loaded into memory as compared to BLOWFISH which has one P-Box and four S-Boxes. Throughput value of BLOWFISH was greater than 3DES, DES, CAST-128, IDEA and RC2. Power consumption value of BLOWFISH was least. 3DES having the least throughput and maximum power consumption value as compared to all block cipher discussed in this paper. From the experimental results it was also concluded that by taking input data in the form of text, audio as well as video throughput of encryption and decryption of all block ciphers discussed here was almost same in all three forms of data. It was concluded by analyzing Encryption/Decryption time, Encryption/Decryption throughput and power consumption value that BLOWFISH has better performance and efficiency than all other block ciphers compared in this paper.

Saini [12] make a performance analysis of various algorithms- DES, AES, RC2, Blowfish, 3DES and RC6. It was concluded from the simulation outcomes that best algorithm are those that are well known and well documented because they are well tested and well studied. A good cryptographic system strikes a balance between what is possible and what is acceptable.

IV. NEED OF STUDY

Information security has become an important issue in data communication. Internet and network applications are growing very fast, so to protect such sensitive data has become the demand of the day. Encryption has come up as solution, and plays an important role in information security system. This art and science of achieving security is known as Cryptography .This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. These algorithms consume a significant amount of computing resources such as CPU time, memory and battery power and consumption time. Encryption algorithms are available in various settings like different key sizes, different block sizes etc. It is very difficult and confusing to decide which algorithm will work better in our application. Hence it is necessary to give performance analysis of various algorithms so that it will be easy to end user to choose the right algorithms for his requirements. This study compared different symmetric encryption algorithms on various parameters. Hence it will be helpful to information security providers to choose the better algorithm.

V. OBJECTIVES OF THE STUDY

The broad objective of the study is to analyze the various symmetric encryption algorithms: DES, 3DES, AES and Blowfish. However the specific objectives of the study are:

1. To have a deeper understanding of cryptography process
2. To perform a comparative analysis of symmetric encryption algorithms of cryptography

VI. RESEARCH METHODOLOGY

In order to meet the objective theoretical approach has been used. The theoretical approach is based on review of secondary data acquired from literature survey, books, research papers and articles on the internet.

VII. ANALYSIS

Based on literature review by various researchers a theoretical analysis was made on the selected algorithms. Encryption algorithms play an important role in communication security where memory usages, output byte and battery power are the major issue of concern. The selected algorithms DES, 3DES, AES and Blowfish are used for performance evaluation.

Table 1: Comparative Analysis of Symmetric Encryption Algorithms

Features	DES	3DES	AES	Blowfish	References
Created By	IBM in 1975	IBM in 1978	Joan Daeman, Vincet Rijmen in 1998	Bruce Schneier in 1998	Stallings [17], Forouzan [7], Schneier [13]
Algorithm Structure	Feistel Network	Feistel Network	Substitution, Permutation Network	Feistel Network	Stallings[17], Schneier [13]
Block size	64 bit	64 bit	128 bit	64 bit	Stallings [17], Forouzan [7]
Rounds	16	48	10,12,14	16	Stallings [17], Schneier [13]
Key length	56 bits	112, 168 bits	128, 192 or 256 bits	32 bits to 448 bits	Stallings [17], Forouzan [7], Agrawal et al. [2], technet [25]
Computational Speed	Fast	Moderate	Fast	Very fast	Jeeva et al. [8] Agrawal et al. [2]
Tunability	No	No	No	Yes	Jeeva et al. [8]
Encryption	Medium	Low	High	Very High	Seth et al. [14]

Throughput					Alam et al. [3]
Decryption Throughput	Medium	Low	High	Very High	Seth et al. [14] Alam et al. [3]
Power Consumption	Low	Highest	Medium	Lowest	Marwaha et al. [10] Alam et al. [3]
Memory Usage	High	Very High	Medium	Very low	Seth et al. [14] Mandal et al. [9]
Security against attacks	Brute force	Brute force, Chosen plain text, known plain text	Chosen plain text, known plain text	Dictionary Attack	Jeeva et al. [8] Agrawal et al. [2] Cornwell[5]
Confidentiality	Low	High	High	Very High	Marwaha et al. [10] Cornwell [5]

It is evident from Table 1that Algorithmic structure of DES and 3DES and Blowfish is same, follows Fiestel Network developed by Cryptography researcher Horst Feistel in the early 70's. However AES adopted Substitution, Permutation Network. The block size is the basic unit of data that can be encrypted or decrypted in one operation. Larger Block size means greater security (all other factor being equal) but reduced encryption/decryption speed for a given algorithm. The greater security is achieved by greater diffusion. Generally, a block size of 64 bit has been considered as reasonable tradeoff and was nearly universal in block cipher design. Block size used for DES, 3DES and Blowfish is same, 64 bits. However Block size of AES is 128. Larger block size is more secure. However large block size is more costly to implement (in terms of gates or low level instructions). Number of round is also a important criteria of algorithm security. Multiple rounds offer increasing security. The essence of the Feistel cipher is that a single round offers inadequate security. Number of round in DES and Blowfish is 16. 3DES has 48 rounds, means 3 times than DES. However in AES it depends on the key length: 16 bytes key length have 10 rounds, 24 bytes key length have 12 rounds, and 32 byte key length have 14 rounds. In the encryption/decryption methodologies the key management is the important aspect that shows how data is encrypted/ decrypted. Symmetric key encryption is subject to key search attacks also called brute force attacks. In these attacks, the attacker tries each possible key until the right key is found to decrypt the message. Most attacks are successful before all possible keys are tried. Longer key lengths decrease the possibility of successful attacks by increasing the number of combinations that are possible. The symmetric algorithm: DES, 3DES, AES and Blowfish uses a variable key length. Due to its longest key length Blowfish is the best performer.

The encryption time is considered the time that an encryption algorithm takes to produce cipher text from plain text. Encryption time is used to calculate the throughput of an encryption scheme, is calculated as the total plaintext in bytes encrypted divided by the encryption time. The analysis shows that Blowfish algorithm consumes least encryption time, 3DES consumes longest encryption time in symmetric algorithms. Encryption time of AES is more as compare to DES. It was concluded on the basis of Encryption Throughput that Blowfish has better performance and efficiency than all other block cipher: DES, 3DES, and AES. The decryption time is considered the time that a decryption algorithm takes to produce cipher text from plain text. Decryption time is used to calculate the throughput of a decryption scheme, is calculated as the total ciphertext in bytes decrypted divided by the decryption time. The analysis shows that Blowfish algorithm consumes least decryption time, 3DES consumes longest decryption time in symmetric algorithms. Decryption time of AES is more as compare to DES. It was concluded on the basis of decryption throughput that Blowfish has better performance and efficiency than all other block cipher: DES, 3DES, and AES. Power Consumption is very important criteria for selection of encryption algorithms for small hand held and battery driven devices. In case of symmetric key algorithms, 3DES consume more power as compare to DES and AES. However power consumption of Blowfish is least as compare to DES, 3DES, and AES. From Blowfish and AES we found that Blowfish consumes very less power near about 16% of the power which is consumed for AES. In case of symmetric key algorithms, 3DES has more memory usage as compare to DES and AES. Memory usage of AES is less in comparison to DES, and 3DES. However Blowfish has least memory usage.

Cryptography security defines whether encryption scheme is secure against brute force and different plaintext-cipher text attack. The analysis shows that in case of symmetric algorithms, AES is more secure than DES, 3DES. However Blowfish is considered more secure than all other block cipher: DES, 3DES, and AES. It was concluded that Blowfish is able to provide long term data security without any backdoor vulnerability or ability to reduce the key size. Confidentiality of DES is low due to small key length. It is concluded that AES can be used in circumstances where there is need for high security. In case of performance aspects, Blowfish can be used. The confidentiality of Blowfish is high as compared to other all mentioned algorithms.

It can be concluded from the data in the Table 1 that Blowfish is tunable and encryption/decryption throughput is high as compare to DES, 3DES and AES algorithms. Also power consumption and memory usage of Blowfish is low as compare to DES, 3DES and AES algorithms.

VIII. CONCLUSIONS

It is concluded from the above comparison that Blowfish is superior to other algorithms: DES, AES and Triple DES on the basis of key size and security. The F function of Blowfish algorithm provides a high level of security to encrypt the 64 bit plaintext data. Also the Blowfish algorithm runs faster than other popular symmetric key encryption algorithms: DES, 3DES, and AES. It is concluded that Blowfish gives better performance than DES, 3DES, and AES in terms of encryption time, decryption time and throughput. 3DES has least performance among all mentioned algorithms. Our future work will include experiments/simulation on the above parameters on different file sizes of text, audio and video data and focus will be to improve encryption ratio and reduce memory usage.

REFERENCES

[1] Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Volume 8, 2009, pp. 58-64.

[2] Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, pp. 877-882.

[3] Alam Md Imran, Khan Mohammad Rafeek. "Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013, pp.713-720.

[4] Apoorva, Kumar Yogesh, "Comparative Study of Different Symmetric Key Cryptography", IJAIEM, vol. 2, Issue 7, July 2013, pp. 204-206.

[5] Cornwell Jason W, "Blowfish Survey", Department of Computer science, Columbus State university, Columbus, GA, 2010.

[6] Dhawan Priya, "Performance Comparison: Security Design Choices", Microsoft Developer Network October 2002.

[7] Forouzan Behrouz A., "Data Communications & Networking", Fourth Edition, 2008, New York: Tata McGraw-Hill.

[8] Jeeva AL, Palanisamy, Dr. V., Kanagaram K. "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms ", International Journal of Engineering Research and Applications(IJERA), Volume 2, Issue 3, May-June 2012, pp. 3033-3037.

[9] Mandal Pratap Chandra, "Superiority of Blowfish Algorithm" IJARCSSE, volume 2, Issue 9, September 2012, pp. 196-201.

[10] Marwaha Mohit, Bedi Rajeev, Singh Amritpal, Singh Tejinder, "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology/IV/III/July-Sep, 2013/16-18.

[11] Nadeem Aamer, "Performance Comparison of Data Encryption Algorithms", Oct 2008.

[12] Saini Bahar, "Survey On Performance Analysis of Various Cryptographic Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014, pp. 1-4.

[13] Schneier B., "Applied Cryptography", John Wiley& Sons Publication, New York, 1994.

[14] Seth Shashi Mehrotra, Mishra Rajan, "Comparative analysis of Encryption algorithm for data communication", International Journal of Computer Science and Technology, vol. 2, Issue 2, June 2011, pp. 292-294.

[15] Singh Gurjeevan, Kumar Ashwani, Sandha K.S. "A Study of New Trends in Blowfish Algorithm" International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 2, pp.321-326.

[16] Singh S Preet, Mani Raman, "Comparison of Data Encryption Algorithms", International Journal of Computer science and Communications, Vol. 2, No.1, January-June 2011, pp. 125-127.

[17] Stallings William, "Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Prentice Hall, 2011.

[18] Tamimi A. Al., "Performance Analysis of Data Encryption Algorithms", Oct 2008.

[19] Tanenbaum Andrew S., "Computer Networks", Third Edition, Prentice Hall India, 2000.

[20] Thakur Jawahar, Kumar Nagesh. "DES, AES and Blowfish Symmetric Key Cryptography algorithm Simulation Based Performance Analysis", IJETAE, vol. 1, Issue 2, DEC. 2011, pp. 6-12.

WEB REFERENCES

[21] [TropSoft] "DES Overview", http://wwwtropsoft.com/strongenc/des.html
"3DES Overview", http://wwwtropsoft.com/strongenc/des3.html

[22] http://en.wikipedia.org/wiki/History_of_cryptography accessed on 20/07/2014 at 11 AM.

[23] http://media.wiley.com/product_data/excerpt/94/07645487/07645487.94.pdf

[24] http://www1.cse.wustl.edu/~jain/index.html

[25] technet.microsoft.com/en-us/library/cc961628.aspx

