ISSN:0975-9646

A Critical Analysis of Some Symmetric Key Block Cipher Algorithms

Sunil Mankotia[#1] and Manu Sood[#2]

[#]*Department of Computer Science, Himachal Pradesh University, Shimla*
Himachal Pradesh, India

Abstract- **In this era of information technology and e-commerce security is the key aspect while transmitting confidential information over insecure network like internet. In order to protect the information, various security mechanisms are used. Cryptography is a technique of protecting secure information from unwanted individuals by converting it into unintelligible form. It is an emerging technology in the area of network security. In this paper critical analysis of some of the symmetric key block cipher algorithms DES, 3DES, AES, IDEA, Blowfish and RC2 is presented.**

Keywords: Cryptography, Encryption, DES, 3DES, AES, IDEA, Blowfish, RC2.

I. INTRODUCTION

Cryptography is a technique of protecting secure information from unwanted individuals by converting it into unintelligible form. It is an art to transform the messages to make them secure and immune against security attacks. Cryptography is used for secure communication in the presence of third parties to maintain information securities such as confidentiality, authentication, data integrity, access control and non-repudiation. In the modern era of Information Technology security is the key aspect while transmitting confidential information over the unsecured network. To overcome this problem we need some encryption techniques which can protect our confidential information. Cryptographic Algorithms provides end to end information security over unsecured communication networks. There are number of encryption techniques which can be broadly divided into two categories: Symmetric Key Encryption and Asymmetric Key Encryption. In Symmetric key Encryption same key is used to encrypt and decrypt data, while Asymmetric Key Encryption uses two different keys; public and private keys. Public key for encryption purpose and private key for decryption. Symmetric algorithms are of two types Block Ciphers and Stream Ciphers. Figure 1 shows the general overview of the modern cryptographic techniques

II. CRYPTOGRAPHIC ALGORITHMS

In the present study we will discuss only Block Cipher Algorithms. The reviewed cryptographic algorithms are as under:

A. Data Encryption Standard (DES):

Data Encryption Standard (DES) is a block encryption algorithm published by NIST (National Institute of Standard and Technology). It encrypts data blocks of 64 bits each by taking a 56 bit key. It uses same key for encryption and decryption. A 16 cycle Feistel system is used with an overall 56 bit key permuted into 16 48-bit sub keys, 1 for each cycle. To decrypt, the same algorithm is used but the order of round keys are in reverse order. It was adopted in 1974 since that time many attacks were reported which has made DES an insecure algorithm.

B. Triple DES (3DES)

3DES was designed to overcome the flaws in DES without creating a new crypto system. Triple DES is considered to be DES- three times. It simply extends the key size from 56 bits to 168 bits (i.e.56 X 3=168) to make it resistant from brute-force attack. It has two variants; one with two keys and other with three keys. Triple DES is slower than other block encryption method but it is reliable due to longer key length as it reduces many attacks.

C. Advanced Encryption Standard (AES)

AES is also known as Rijndael algorithm developed by NIST in late 90's. It was perceived that 56-bit key of DES was not safe against the brute force attack and 64-bit blocks were also considered to be weak. AES encrypts data blocks of 128 bits using variable key length of 128,192 or 256 bits in 10, 12 or 14 rounds depending upon the key size.

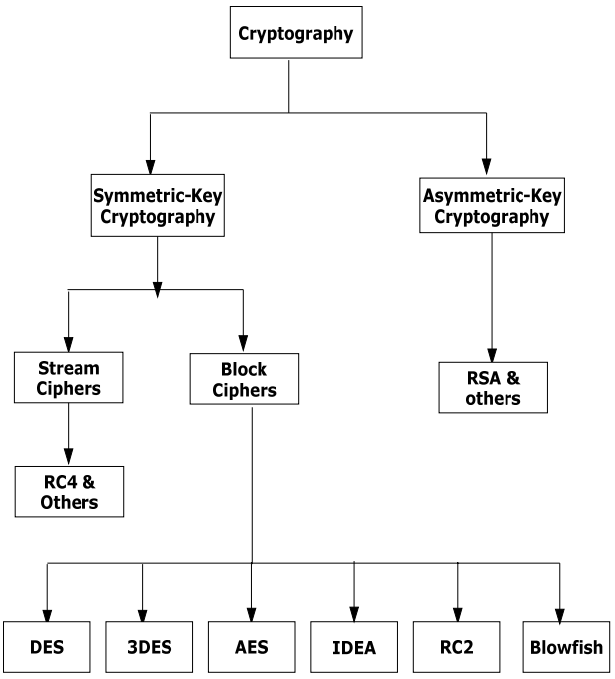

Fig. 1: Classification of Cryptographic Techniques

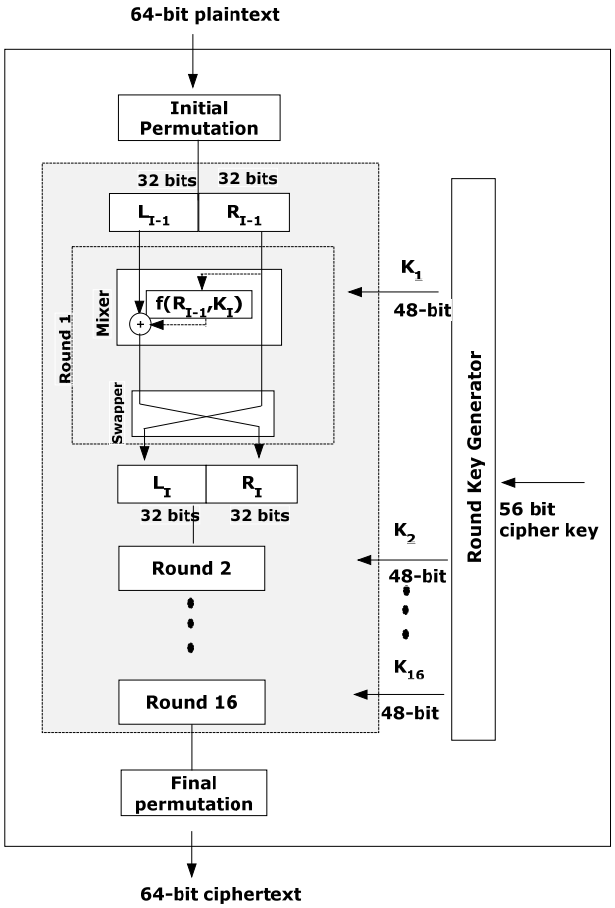

Fig. 2: General structure of DES Algorithm

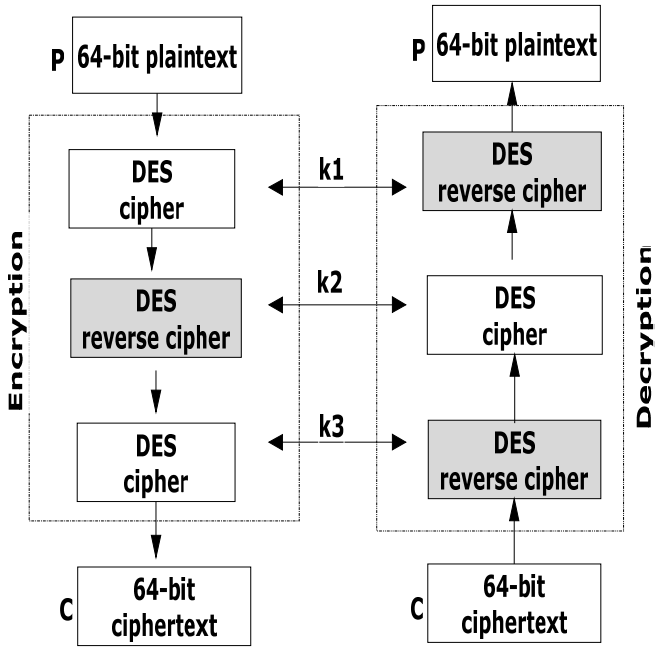

Fig. 3: Structure of 3DES with three keys (k1, k2 and k3).

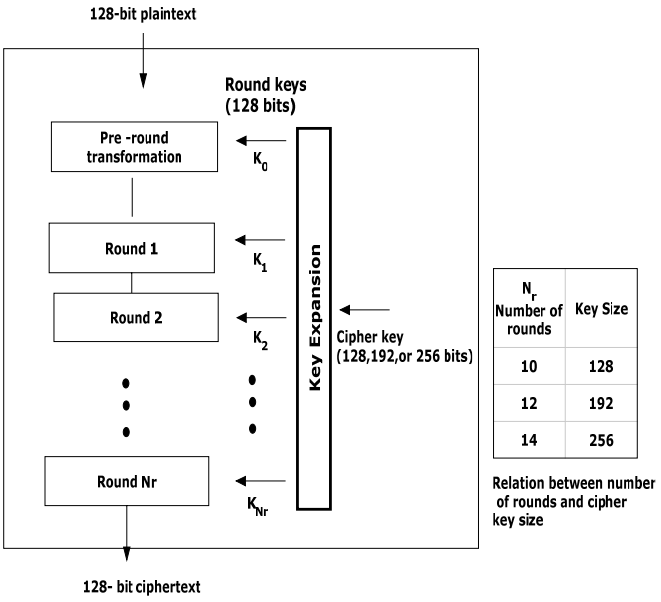

Fig. 4: General Structure of AES.

A round of AES consists of four operations i.e. Substitutions, Permutations, Mixing and Adding Key:

1) *SubBytes (Substitute Byte transformation):*

AES contains data blocks of 16 bytes. In sub-byte transformation each byte of data block is transformed into another block using 8-bit substitution box.

2) *ShiftRows transformation:*

The shift rows operations shifts the last three rows of the state cyclically, which results in scrambling of row data.

3) *MixColumns transformation:*

The mix column operation operates at column level. It transforms the each column of the state to a new column. The last round for encryption does not involve the mix column transformation.

4) *AddRoundKey transformation:*

It is a bit wise XOR between the 128 bits of present state and 128 bits of the round key.

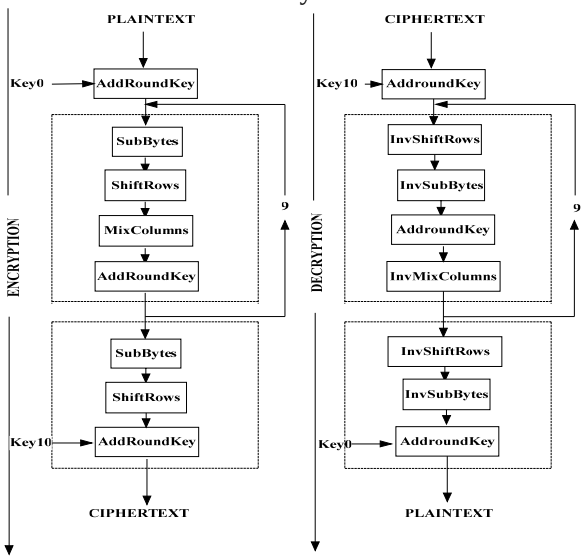

Fig. 5: Structure of each round at encryption and decryption site of AES.

Decryption involves all the transformations performed in encryption but using the inverse functions i.e. inverse shift rows, inverse substitute bytes, add round key and inverse mix columns.

D. IDEA (International Data Encryption Algorithm)

IDEA is a block cipher which operates on a 64 bit plaintext blocks. It is based on the concept of substitution-permutation structure that uses block cipher of 64 bit plaintext and a key with128 bits. The algorithm used for encryption and decryption is the same. The plaintext of 64 bits is divided into four parts (each of 16 bits). These four parts became the input for first round which consists of mixing operations from different algebraic groups. The three algebraic operations which are performed in each round are XOR, Addition modulo 2^{16} and multiplication modulo $2^{16}+1$. All these operations operate on 16 bit sub blocks. There are eight such rounds. The final step is an output transformation which produces four cipher text blocks of 16 bits each. These blocks are combined to generate the 64 bit cipher text block.

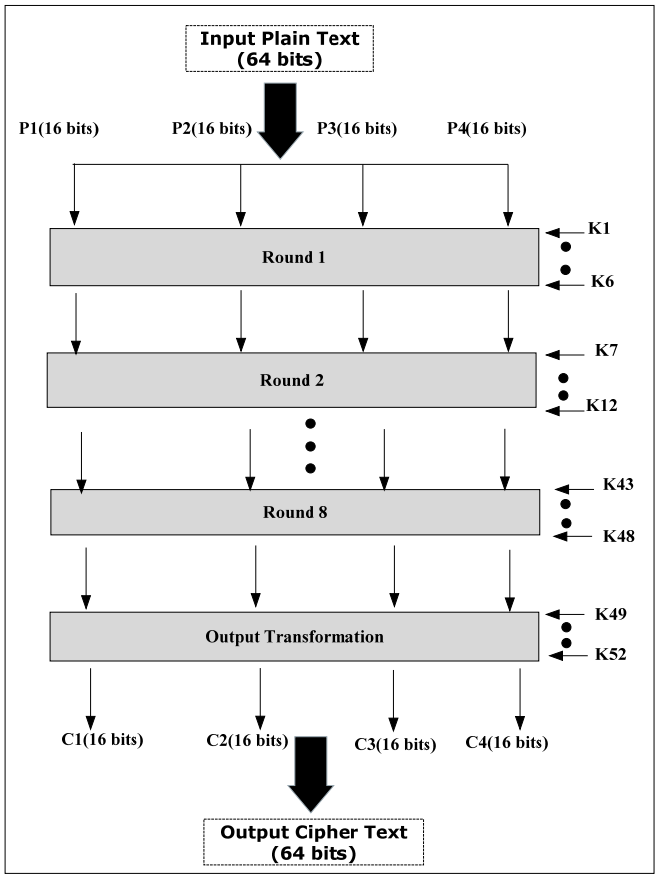

Fig. 6: General Structure of IDEA

E. Blowfish

Blowfish was developed by Bruce–Schneider in 1993 as an alternative to the existing encryption algorithms. It is a symmetric key block cipher which uses 64 bit block size and a variable key length from 32 bits to 448 bits. It has 16 or less rounds. It is the fastest block ciphers developed till date. No attack is known to be successful against Blowfish; however it suffers from weak key problems. Moreover space requirement for Blowfish is also very less; it can execute in less than 5KB memory.

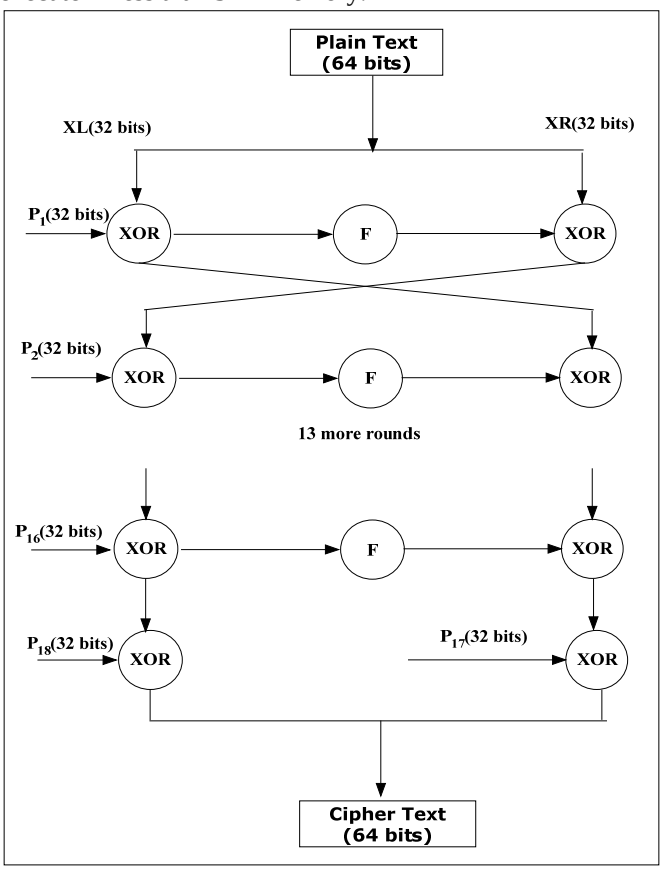

Figure 7: Structure of Blowfish (encryption site)

The function F in the figure 7 can be defined as:
F[a,b,c,d]=((S1,a + S2,b) XOR S3,c) +S4, d.
Where a, b, c and d are 8-bit sub blocks of 32-bit XL block and S1, S2, S3 and S4 are S-box substitutions.

F. RC2

RC2 is a variable key size block cipher which uses 64 bits blocks. It was designed to replace DES. It is considered to be three times faster than DES. It accepts a variable length key from 0 bytes to the maximum string length that the computer system can support. It uses 16 rounds of one type (Mixing) and two rounds of other type (Mashing). The encryption speed of the algorithm is independent of its key size. It was proposed to replace DES.

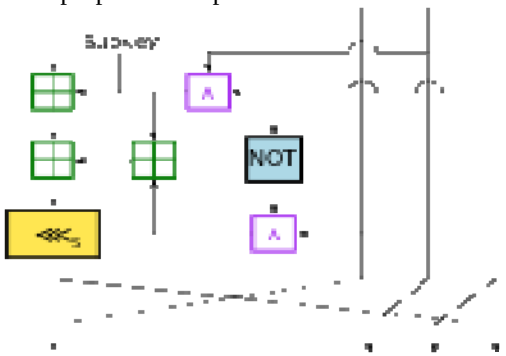

Figure 8: One round of MIXING in RC2

III. LITERATURE SURVEY

Simar Preet Singh and Raman Maini have done a comparison of data encryption algorithms using simulation. The results showed that BLOWFISH has better performance than other commonly used encryption algorithms AES showed poor performance results compared to other algorithms as it requires more processing power. The comparison also reveals that 3DES requires always more time than DES because of its three phase encryption technique. BLOWFISH has not known any security weak point so far and is considered as an excellent encryption technique/algorithm.[1]

E. Thambiraja et al in their paper on various most common encryption techniques have surveyed on various existing encryption techniques. All the techniques are useful for real time encryption each technique is unique in its own way which might be suitable for different applications. Gurpreet and Supriya studied about encryption algorithms for information security. Four different algorithms were studied and on the basis of this study they found that AES algorithm is most efficient in terms of speed, time, throughput and avalanche effect. [2]

Hamdan O. Alanazi et al in their paper made a comparison of three symmetric block ciphers DES, 3DES and AES on nine parameters. The result shows that DES is vulnerable to brute force attack and no more secure as the 56 bit key space can be easily calculated with today's computing power. 3DES is the extension of DES with three different keys, which is secure as its effective key length is 168 bits, but with two keys effective key length reduces to 112 bits which is less secure. 3DES takes three times CPU power than DES which lowers its performance. AES outperforms 3DES in both in software and hardware. It uses 128-bit fixed length blocks and works with 128,192 and 256 bit keys. It shows the superiority of AES over DES and 3DES. [3]

Dr. Prerna Mahajan and Abhishek Sachdeva in their study on encryption algorithms found that AES algorithms consumes least encryption time while RSA consumes the longest encryption time they also found that decryption of AES algorithms is better than other algorithms using simulation results they evaluated that AES is much better than DES and RSA. [4]

Kumar et al evaluated the power consumption analysis of BLOWFISH, AES, IDEA and Rijndael algorithms experiments shows that BLOWFISH consumes least amount of power than other algorithms. IDEA and Rijndael consumes less power than AES but more than BLOWFISH. The result also showed superiority of BLOWFISH algorithms.[5]

Abdel-Karim Al Tamimi compared the performance of Data encryption algorithms using simulator on request processes per second and response time. Simulation results showed that BLOWFISH has better performance than other common encryption algorithms used.AES showed poor performance results compare to other algorithms since it requires more processing power.[6]

Anjula Gupta and Navpreet Kaur Walia had reviewed various cryptography algorithms. They have found that the throughput value of BLOWFISH is greater than all other symmetric algorithms. The experimental results of many papers reveals that BLOWFISH has better performance and efficiency than all other block ciphers.[7]

According to Pratap Chnadra Mandal BLOWFISH algorithm is superior to other algorithms in terms of Throughput, processing time and power consumption. Secondly AES has advantage over 3DES and DES in terms of throughput and decryption time. Thirdly 3DES has the least performance among AES, DES, BLOWFISH and 3DES. Singh et al evaluate the performance of four symmetric algorithms; AES, DES, 3DES and BLOWFISH in terms of throughput and encryption/ decryption time. BLOWFISH gave better performance than AES, DES and 3DES in terms of encryption/ decryption time and throughput.[8]

Sumitra presented comparative analysis of AES and DES security algorithms and found that different machines take different times for encryption/decryption of same algorithms over same data packet. Results showed that AES more secure as compare to DES.[9]

Md Imran Alam et al made a performance and efficiency analysis of different block cipher algorithms of symmetric key cryptography using data, audio and video files and compared their encryption and decryption time. It was found that RC2 was faster for small sized data files as compared to Blowfish. However throughput and power consumption of Blowfish was greater than 3DES, DES, CAST-128, IDEA and RC2.[10]

IV. CRITICAL ANALYSIS

On the basis of detailed study of different symmetric key block ciphers discussed above, an attempt is made to critically analyse them. DES being one of the early encryption algorithms suffers from some weak points. It uses same algorithm for encryption and decryption but the order of the keys is reversed in latter process. With rapid increase in processing speed of CPU and other advances in computing the key space of 56 bit key is considered no more secure from brute force attack. To overcome this weakness TripleDES (3DES) was designed by increasing the key length from 56 bits to 112 bits (with two keys) and 168 (with three keys) without making a new algorithm. The main controversy was that the original algorithm of DES was never designed to work like the way it works in 3DES, which results in low throughput in comparison to DES. However, no serious problem was discovered in this design and 3DES is still used in many Internet protocols. RC2 uses flexible key within the range of 8 bits to 1024 bits and block of 64 bits. It was also designed to replace DES. The interesting thing about this algorithm is that it performs with same speed irrespective of key length. It is vulnerable to related-key attack using 2^{34} chosen plaintexts. IDEA uses the concept of confusion and diffusion by mixing operations from different algebraic groups. It operates on 64-bit block. IDEA's key length is 128 bits which is more than twice as that of DES which make it resistant from brute force attack. It is also found that IDEA becomes immune to differential cryptanalysis after only four of its eight rounds. A class of weak keys exist for IDEA but the chance of such weak key is very small. Blowfish is

considered to be the most secure and fastest algorithm among all the algorithms discussed in the present study. No attack is successful against Blowfish, but it has some weak key problems too.AES uses variable length key (128,192 or 256 bits) and works with a block of 128 bits. It is considered as flexible as it provides the option to use different sized keys and blocks in multiples of 32-bits within a range of 128-256 bits. It was designed to replace 3DES and is considered superior in terms of speed and efficiency.

To conclude the analysis, all the techniques are unique in their own way and are improved versions over the previous ones. DES proved to be insecure with passage of time and many new techniques have been proposed and adopted from time to time to overcome its shortcomings. Different hardware and software applications are using different cryptographic techniques as per the suitability of the environment in which they are employed. Hence, no cryptographic technique is considered to be complete in all respects, every technique has its own strong and weak points.

V. COMPARISON ANALYSIS

On the basis of different encryption algorithms studied in this paper a comparison on common factors is presented in the Table below:

TABLE I
COMPARISON OF VARIOUS ALGORITHMS ON SOME COMMON FACTORS

Factors	DES	3DES	AES	IDEA	BLOWFISH	RC2
Key Length	56 bits	168 bits for three keys 112 for two keys	128, 192 or 256 bits	128 bits	32 to 448 bits; 128 by default	8 to 1024 bits; 64 bits by default
Block Size	64 bits	48 bits	128 bits	64 bits	64 bits	64 bits
Number of Rounds	16	48	10 for 128 12 for 198 14 for 256	8	16	16 (Mixing) +2 (Mashing)
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Key Used	Same Key for encrypt and decrypt	Same Key for encrypt and decrypt	Same Key for encrypt and decrypt	Same Key for encrypt and decrypt	Same Key for encrypt and decrypt	Same Key for encrypt and decrypt

VI. CONCLUSIONS AND FUTURE SCOPE

The present paper provides the general overview of some symmetric key block ciphers and their algorithms which are used in modern cryptography. The present study provides better understanding and working of these algorithms. In future, comparative or performance analysis can be made by taking different parameters to outline the strengths and weaknesses of various algorithms. Through the understanding of shortcomings of these algorithms, some new encryption algorithms can be proposed by making amendments in the existing algorithms.

REFERENCES

[1] Simar Preet Singh and Raman Maini, "Comparison of Data Encryption Algorithms", International Journal of Computer Science and Communication, Vol. 2, No. 1, January-June 2011, pp. 125-127.

[2] E. Thambiraja, G. Ramesh and Dr. R. Umarani, " A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012, pp. 226-233.

[3] Hamdan O. Alanazi, B. B. Zaidan, A. A. Zaidan, Hamid A. Jalab, M. Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine factors", Journal of Computing, Volume 2, Issue 3, March 2010, pp. 152-157.

[4] Dr. Prerna Mahajan and Abhishek Sachdeva, " A study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013, pp. 15-22.

[5] Deepak Kumar Dakate and Pawan Dubey, "Performance comparison of Symmetric Data Encryption Techniques", International Journal of Advanced Research in Computer Engineering and Technology, Volume 3, No. 8, August 2012, pp. 163-166.

[6] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms."

[7] Anjula Gupta and Navpreet Kaur Walia, " Cryptography Algorithms: A Review", International Journal of Engineering Development and Research, Volume 2, Issue 2,Year 2014, pp. 1667-1672

[8] Pratap Chnadra Mandal, "Superiority of Blowfish", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012, pp. 196-201.

[9] Sumitra, "Comparative Analysis of AES and DES security Algorithms", International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013, pp. 1-5.

[10] Md Imran Alam and Mohammad Rafeek Khan, " 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.

[11] William Stallings, "Cryptography and Network Security: Principles and Practices", Pearson Education/Prentice Hall of India, Fifth Edition.

[12] Atul Kahate, "Cryptography and Network Security", McGrawHill, Second Edition.

[13] Bruice Schneier, "Applied Cryptography", Wiley Publications, Second Edition.

[14] Behrouz A Forouzan, "Data Communications and Networking", Tata McGraw Hill, Fourth Edition.