Performance Analysis of Encryption Algorithms for Security

Madhumita Panda
Lecturer ,Computer Science
SUIIT, Sambalpur University
Odisha, India
mpanda.suiit@gmail.com

***Abstract*-With the fast progression of digital data exchange information security has become an important issue in data communication.Encryption algorithms play an important role in information security system. These algorithms use techniques to enhance the data confidentiality and privacy by making the information indecipherable which can be only be decoded or decrypted by party those possesses the associated key.But at the same time ,these algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. So we need to evaluate the performance of different cryptographic algorithms to find out best algorithm to use in future. This paper provides evaluation of both symmetric (AES, DES, Blowfish) as well as asymmetric (RSA) cryptographic algorithms by taking different types of files like Binary ,text and image files. A comparison has been conducted for these encryption algorithms using evaluation parameters such as encryption time, decryption time and throughput. Simulation results are given to demonstrate the effectiveness of each.**

***Keywords*-Cryptography;Encryption; Decryption; Private key encryption; Public key encryption; RSA; DES;AES; BLOWFISH; Performance Metrics.**

I. INTRODUCTION

The demand for the ubiquitous personal communications is driving the development of new networking techniques. Information Security has now become a very important aspect of data communication as people spend alarge amount of time connected to a network. One of the primary reasons that intruders are successful is that most of the information they acquire from a system is in a form that can be read and understood. To improve the security of the data being transmitted various techniques are employed. The important method used to provide the confidentialityis through the use of Cryptography which is the art and science of protecting information from undesirable individuals by converting it into a form indiscernible by its attackers while it is stored and transmitted [1]. It is a fundamental building block for building information systems**.** It relates to the study of mathematical techniques related to the aspects of information security such as the confidentiality, data integrity, and authentication of the data[2]. In cryptographic terminology, the data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text.The process of retrieving the plaintext from the cipher text is called decryption. A system or product that provides encryption and decryption is called cryptosystem [1].

Depending on the number security keys used to encrypt/decrypt data, cryptographic algorithms are classified as asymmetric algorithms (public key) and symmetric algorithms (secret key).InSymmetric key encryptiononly one key is used to encrypt and decrypt data. The key should be distributed before transmission between entities. Therefore key plays an important role in Symmetric key encryption. Strength of Symmetric key encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using shorter key. The weakness of symmetric algorithms is in sharing ofsymmetric keybetween sender and receiver.The representative symmetric key cryptography algorithms include RC2, DES, 3DES, RC5, Blowfish, and AES, which use certain- or variable-length key. Thesymmetric key algorithms are further classified as blockciphers (AES, Blowfish) that works on blocks of a specifiedlength and stream ciphers (RC4, Salsa20) that work bitwise onthe data. A stream cipher can be seen as a block cipher with ablock length of 1 bit.In Asymmetric key encryption two keys ,private key andpublic key are used. Public key is used for encryption and private key is used for decryption (E.g. RSA and Digital Signatures). However, public

978-1-5090-4620-1/16/$31.00 ©2016 IEEE

key encryption is based on mathematical functions, and is not very efficient for small mobile devices [3]. Also Asymmetric encryption algorithms are almost 1000 times slower than symmetric encryption algorithms ,because they require more computational power[4].Major advantage of Asymmetric encryption is thatit takesaway the security risk of key sharing which was a problem in secret key cryptography.

The present work has compared both symmetric (AES,DES,Blowfish) as well as Asymmetric(RSA) cryptographic algorithms by taking different types of files like Binary ,text and image files. A comparison has been conducted for these encryption algorithms based on three different parameters such as encryption time, decryption time and throughput. Simulation results are given to demonstrate the effectiveness of each algorithm.

The rest of the paper is organised as follows.Section II gives a brief overview of the algorithms used in the paper.Section III presents the simulation results and analysis.Finally section IVconcludes the paper giving some future work.

II.OVERVIEW OF ALGORITHMS

The algorithms chosen for implementation here are AES,DES,BLOWFISH and RSA.

A.RSA

A method to implement a public key crypto system whose security is based on the difficulty of factoring large prime numbers was proposed in [5]. RSA is an asymmetric cryptographic algorithm named after its creators Rivest, Shamir &Adelman. It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. It generates two keys: public key for encryption and private key to decrypt message .The algorithm comprises of three steps, first step is key generation which is to be used as key to encrypt and decrypt data, second step is encryption, and third step is decryption. Key size is 1024 to 4096 bits.

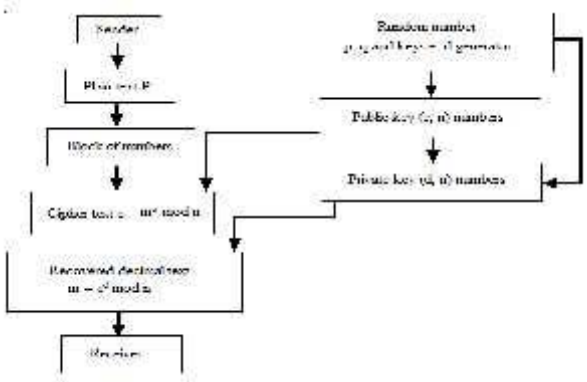

Fig. 1. RSA Algorithm

It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose. Sender encrypts the message using Receiver's public key and when the message gets transmit to receiver, then receiver can decrypt it using his own private key [6]. RSA operations can be decomposed in three broad steps: key generation, encryption and decryption.

Key Generation

1. Choose two distinct large random prime numbers p & q such that $p \neq q$.

2. Compute $n = p \times q$.

3. Calculate phi, $\varphi = (p - 1)(q - 1)$ where φ is Euler's Totient Function

4. Select public exponent e such that $1 < e < \varphi$ and $\gcd(e, \varphi) = 1$

5. Compute private exponent $d = e^{-1} \bmod \varphi$

6. Public key is {n, e}, private key is d.

Encryption**:** $c = m^e \pmod n$.

Decryption: $m = c^d \pmod n$.

B.DES

Data Encryption Standard (DES) is a symmetric key block cipher. The key length is 56 bits and block size is 64 bit length. DES was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It was developed by an IBM team around 1974 and adopted as a national standard in 1997 [7]. The flow of DES algorithm is shown in Fig.2.DES can operate

in different modes - CBC, ECB, CFB and OFB, making it flexible. The algorithm starts with an initial permutation, sixteen rounds block cipher and a final permutation. DES application is very popular in commercial, military, and other domains in the last decades. There are variants like 3DES [8], AES [9] by enhancing DES function.

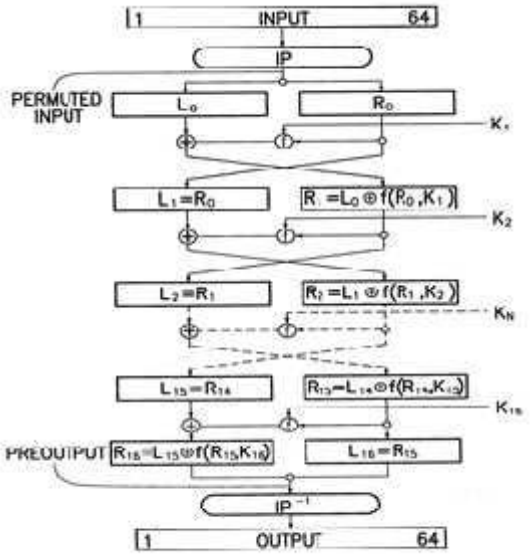

Fig. 2.DES Algorithm

C.AES

The US National Institute of Standards and Technology (NIST) recommended the use of Advanced Encryption Standard to replace Data Encryption Standard in 1998. AES algorithm was developed in 1998 by Joan Daemen and Vincent Rijmen, which is a symmetric key block cipher.It is a variable bit block cipher and uses variable key length of 128, 192 and 256 bits. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications [10][11].

Each processing round as shown in Fig. 3.involves four steps:

• Substitute bytes – Uses an S-box to perform a byte by byte substitution of the block,

• Shift rows – A simple permutation,

• Mix column – A substitution method where data in each column from the shift row step is multiplied by the algorithm's matrix and

• Add round key – The key for the processing round is XORed with the data.

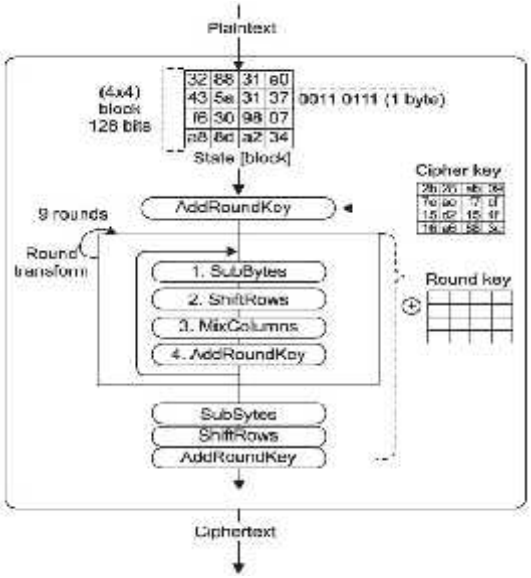

Fig. 3.AES Algorithm

D.BLOWFISH

Bruce Schneier, one of the world's leading cryptologists, designed the Blowfish algorithm [12] and made it available in the public domain. The algorithm was first introduce in 1993, and has not been cracked yet .It is a symmetric key block cipher with key length variable from 32 to 448 bits and block size of 64 bits and having a fiestal network . It can be optimized in hardware applications due to its compactness. The algorithm as shown in Fig.4.consists of two parts: a key-expansion part and a data- encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totalling 4168 bytes[12]. The data encryption occurs via a 16-round Feistel network [13] . It is only suitable for application where the key does not change often, like communications link or an automatic file encryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

These are the following steps for Blowfish encryption algorithm:-

- X is 64 bits input data
- X is divided into two equal parts x1 and x2
- For i=0 to 15
  X1=x1 xor Pi
  X2=f(x1) xor x2

- Swap x1 and x2
- Swap x1 and x2(undo the previous step)
- X1=x2xor P18
- X2=x2 xor P17
- Combine x1 and x2

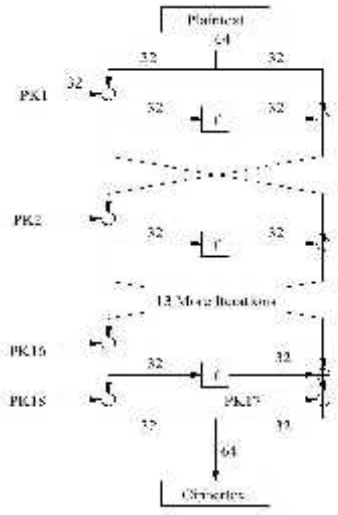

Fig. 4.Blowfish Algorithm

III.SIMULATION RESULTS AND ANALYSIS

The performance comparison of the algorithms mentioned above was conducted with three different types of files(text,Binary,Image). The performance matrices are–

a) Encryption time
b) Decryption time
c) Throughput.

The values for each criterion was logged and graphically plotted to represent the results for conclusion.

The simulation was conducted on a laptop with windows 64bit, processor i3 and CPU 1.90GHzwith 4 GB of RAM**.** Random sizes of files 1, 2, 5, 10 and 20 MB was generated as the test subjects.Java 1.7.0_65 (64 -Bit) was used as the language of choice for implementation. The AES/DES/Blowfish algorithms were run in the cipher block chaining (CBC) mode with key size of 128 bits, 64 bits and 128 bits**.**For each of the data blocks the encryption/decryption was repeated 10 times and the time requirement were logged for each run. Following which the average time taken was computed and used for the calculation of throughput of each algorithm.

TABLEI.Data table for Encryption runtime of Text Files

FILE	AES (in msec)	DES (in msec)	RSA (in msec)	BLOWFISH (in msec)
1 MB	80	136.2	425.6	133.2
2 MB	154.7	269.6	710.9	192.6
5 MB	376.1	665.4	1710.9	373.6
10 MB	683.7	1236.2	3017.1	702.5
20 MB	1350.5	2356.5	6641	1355.2

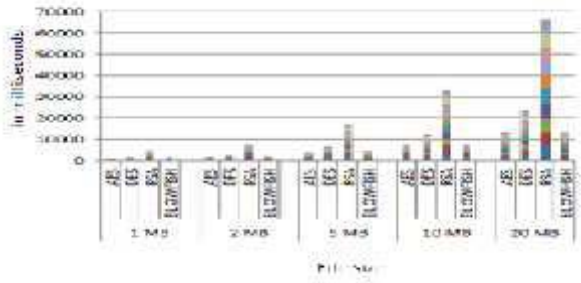

Fig.5. Graph for Encryption runtime of Text Files.

TABLEII. Data table for Decryption runtime of Text Files

FILE	AES (in msec)	DES (in msec)	RSA (in msec)	BLOWFISH (in msec)
1 MB	118.9	144.6	3.8	50.2
2 MB	197.6	269.6	3.5	126.3
5 MB	457.7	690.9	3.7	210.7
10 MB	897.5	1294.6	3.7	575.4
20 MB	1844.5	2744.2	4.0	1025.5

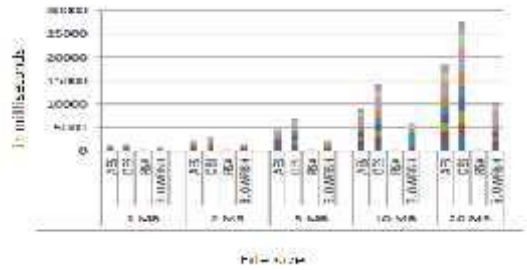

Fig.6. Graph for Decryption runtime of Text Files

TABLEIII.Data table for Throughput of Text Files

FILE	AES (in msec)	DES (in msec)	RSA (in msec)	BLOWFISH (in msec)
1 MB	80	136.2	425.6	133.2
2 MB	154.7	269.6	710.9	192.6
5 MB	376.1	665.4	1710.9	373.6
10 MB	683.7	1236.2	3017.1	702.5
20 MB	1350.5	2356.5	664.1	1355.2
Average Time	2645	4663.4	6528.6	2757.1
Throughput (KB/msec)	14.7	8.3	5.9	14.1

Fig.7.Graph for Throughput of Text Files.

- From the tabular results of Table I and II,we have concluded that AES is taking less time to encrypttext files and RSA is taking less time to decrypt the text files.

- 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 .As throughput increases,Power Consumption decreases [14].So as seen from Fig.7.the throughput Graphof **AES** is better in case of text files encryption, than other three algorithms.

TABLEIV.Data table for Encryption runtime of Binary Files

FILE	AES (in msec)	DES (in msec)	RSA (in msec)	BLOWFISH (in msec)
1 MB	74.6	120.8	393.3	150.5
2 MB	136.2	256.5	734.8	220.9
5 MB	393.4	687.4	1773.7	439.1
10 MB	711.2	1264.9	3446.1	731.3
20 MB	1362.6	2316.6	6868.5	1376.4

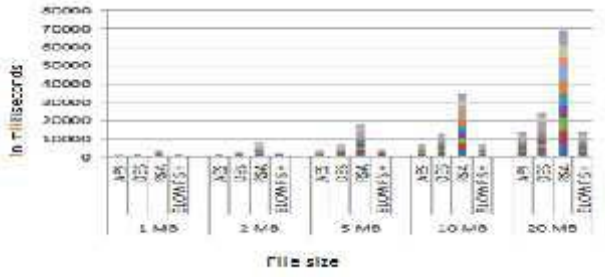

Fig.8. Graph for Encryption runtime of Binary Files

TABLE V.Data table for Decryption runtime of Binary Files

FILE	AES (in msec)	DES (in msec)	RSA (in msec)	BLOWFISH (in msec)
1 MB	111.1	156.5	3.6	44.2
2 MB	196.8	281.3	3.3	84.7
5 MB	460.4	673.6	3.6	203.8
10 MB	876.8	1451.7	3.6	408.6
20 MB	1791.9	2556.9	3.8	923.7

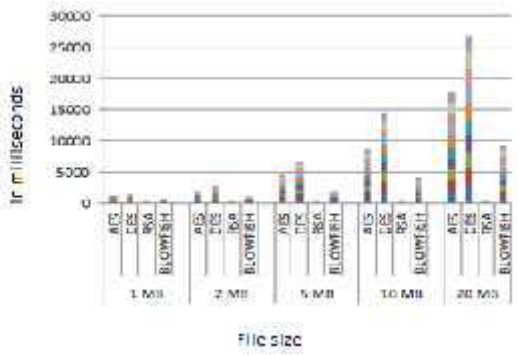

Fig.9.Graph for Decryption runtime of Binary Files

TABLEVI.Data table for Throughput of Binary Files

FILE	AES (in msec)	DES (in msec)	RSA (in msec)	BLOWFISH (in msec)
1 MB	74.6	120.8	393.3	150.5
2 MB	136.2	156.5	734.8	220.9
5 MB	393.4	687.4	1773.7	439.1
10 MB	711.2	1264.9	3446.1	731.3
20 MB	1362.6	2316.6	6868.5	1376.4
Average Time	2677.4	4646.2	13216.4	2918.2
Throughput (KB/msec)	14.5	8.3	2.9	13.3

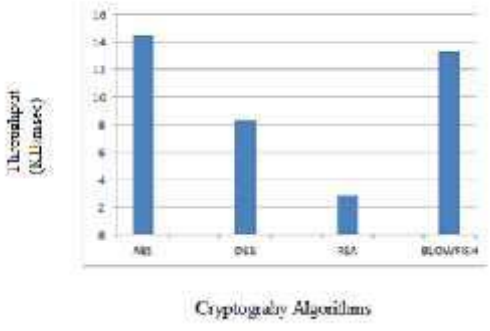

Fig. 10. Graph for Throughput of Binary Files

- From the results of Table IV and V, it can be seen that **AES** is taking less time to

encrypt the Binary Files and **RSA** is taking less time to decrypt the Binary Files.

- As seen from the throughput graph of Fig.10, **AES** is better than other three algorithms.

TABLEVII.Data table for Encryption runtime of Image Files

FILE	AES (in msec)	DES (in msec)	RSA (in msec)	BLOWFISH (in msec)
1 MB	102.6	161.3	481.5	156.4
2 MB	178.3	245	691.5	230
5 MB	206.8	356.8	1031.7	250
10 MB	294.6	480.4	1437.1	336.3
20 MB	406.5	669.3	1816	440.4

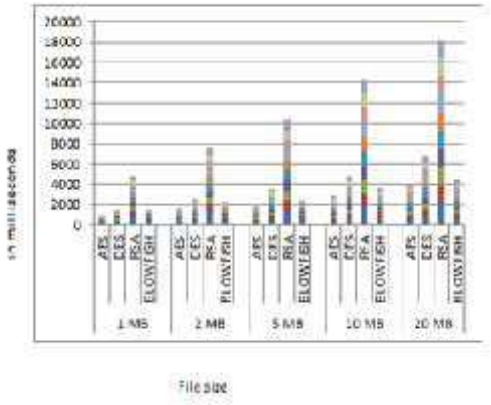

Fig. 11.Graph for Encryption runtime of Image Files

TABLEVIII. Data table for Decryption runtime of Image Files

FILE	AES (in msec)	DES (in msec)	RSA (in msec)	BLOWFISH (in msec)
1 MB	159.8	175.2	4.1	65.5
2 MB	256.1	276.6	4.5	92.7
5 MB	311	400.8	4.7	123.8
10 MB	398.6	554.6	4.7	169.9
20 MB	485.4	696.9	4.7	218.5

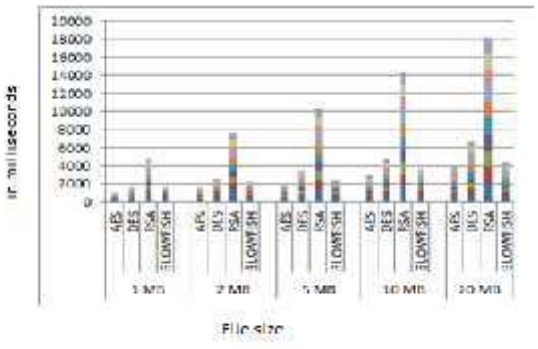

Fig.12. Graph for Decryption runtime of Image Files

TABLEIX.Data table for Throughput of Image Files

FILE	AES (in msec)	DES (in msec)	RSA (in msec)	BLOWFISH (in msec)
1 MB	102.6	161.3	481.5	156.4
2 MB	178.3	245	691.5	230
5 MB	206.8	356.8	1031.7	250
10 MB	294.6	480.4	1437.1	336.3
20 MB	406.5	669.3	1816	440.4
Average Time	118.8	1912.8	5457.8	1413.1
Throughput (KB/ms)	12.9	8.0	2.8	10.8

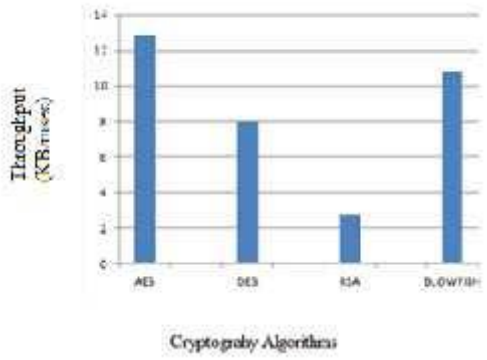

Fig. 13. Graph for Throughput of Image Files

- From the results ofTable VII and VIII we have concluded that **AES** is taking less time to encrypt an image files and **RSA** is taking less time to decrypt the image files.

- As seenfrom Fig.13 throughput of AES is better in case of image files than other three algorithms

IV. CONCLUSION AND FUTURE WORK

This paper presents the performance evaluation of some selected symmetric and asymmetric algorithms. From the presented simulation results,it was concluded that AES has better performance than other algorithms in terms of both throughputand encryption-decryption time. A proposed direction for the future work could be to perform the same experiments on audio& video as well. Also for more faster encryption, we can first go for some compression algorithm and then encryption.

References

[1].Panda, Madhumita, and Atul Nag. "Plain Text Encryption Using AES, DES and SALSA20 by Java Based Bouncy Castle API on Windows and Linux."Advances in Computing and Communication Engineering (ICACCE), 2015 Second International Conference on. IEEE, 2015.

[2].Jeeva, A. L., Dr V. Palanisamy, and K. Kanagaram. "Comparative analysis of performance efficiency and security measures of some encryption algorithms." International Journal of Engineering Research and Applications (IJERA) ISSN (2012): 2248-9622.

[3].Elminaam, DiaaSalama Abdul, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud. "Performance evaluation of symmetric encryption algorithms." IJCSNS International Journal of Computer Science and Network Security 8.12 (2008): 280-286.

[4]. Ramesh, Archana, and A. Suruliandi. "Performance analysis of encryption algorithms for Information Security." Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on.IEEE, 2013.

[5].R.L.Rivest,A.Shamir,and L.Adleman,"A method for obtaining digital signatures and public-key cryptosystems",Communications of the ACM,21(2):120-126,1978.

[6]. Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." International Journal of Computer Applications 67.19 (2013).

[7]. "Data Encryption Standard," Federal Information Processing Standards Publication No. 46, National Bureau of Standards, January 15, 1977.

[8]. William C. Barker, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," NIST Special Publication 800-67 Version 1.1, May 2008.

[9].Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." D r. Dobb's Journal, March 2001, pp. 137-139.

[10]. D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[11].Gurpreet Singh, SupriyaKinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[12].Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008, http://www.schneier.com/blowfish.html

[13]."BLOWFISHalgorithm" http://pocketbrief.net/related/BlowfishEncryption.pdf

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