Evaluating the Performance of Encryption Algorithms for Security

Madhumita Panda
Assistant Professor, Computer Science
SUIIT, Sambalpur University, Odisha, India

Abstract- With the fast progression of digital data exchange information security has become an important issue in data communication. Many efficient encryption standards exist for securing classified data from cyber threats. Two common types of encryption algorithms are Symmetric and Asymmetric. With Symmetric encryption, the same key is used to cipher and decipher data while with Asymmetric algorithms, we have different key for encryption and decryption. 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 sizes of text 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- *RSA, DES, AES, BLOWFISH, Performance Metrics.*

I. INTRODUCTION

Data security has been a major concern in the today's information technology era. 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. The important method used to provide the confidentiality is 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**.** 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 keys used cryptographic algorithms are classified as asymmetric algorithms (public key) and symmetric algorithms (secret key).In Symmetric key encryption only one key is used to encrypt and decrypt data. Some examples of symmetric key algorithms include RC2, DES, 3DES, RC5, Blowfish, and AES, which use certain- or variable-length key. The symmetric key algorithms are further classified as block ciphers (AES, Blowfish) that works on blocks of a specified length and stream ciphers (RC4, Salsa20) that work bitwise on the data. A stream cipher can be seen as a block cipher with a block length of 1 bit. Asymmetric key encryption include two keys private key and public key . Public key is used for encryption and private key is used for decryption (E.g. RSA and Digital Signatures). However, public key encryption is based on mathematical functions, and is not very efficient for small mobile devices [2]. Also Asymmetric encryption algorithms are almost 1000 times slower than symmetric encryption algorithms, because they require more computational power[3]. The present work has compared both symmetric (AES, DES, Blowfish) as well as Asymmetric (RSA) cryptographic algorithms by taking different sizes of text 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 IV concludes 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 [4]. 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.

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 [5]. RSA operations can be decomposed in three broad steps: key generation, encryption and decryption.

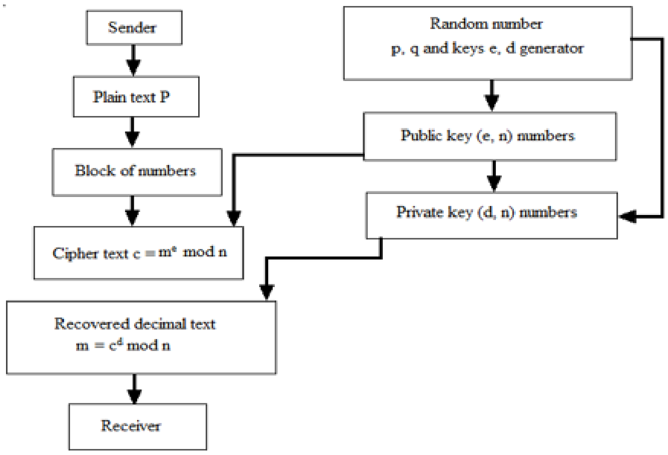
Sender
Plain text P
Block of numbers
Cipher text c = m^e mod n
Random number p, q and keys e, d generator
Public key (e, n) numbers
Private key (d, n) numbers
Recovered decimal text m = c^d mod n
Receiver

Fig. 1. RSA Algorithm

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: $c = m^e (\mathrm{mod}\ n)$.

Decryption: $m = c^d (\mathrm{mod}\ n)$.

B.DES

Data Encryption Standard (DES) is a symmetric key block cipher and was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). The flow of DES algorithm is shown in Fig.2. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block [6] [7]. There are variants like 3DES [8], AES [9] by enhancing DES function.

C.AES

AES (Advanced Encryption Standard) is a symmetric block encryption standard recommended by NIST (National Institute of Standards and Technology) [10] [11] is used for securing information. It uses the same key for both encryption and decryption. It has variable key length of 128, 192, or 256 bits; default 256 [12]. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size [13] [14] [15] [16]. Also, AES has been carefully tested for many security applications [15][16].

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

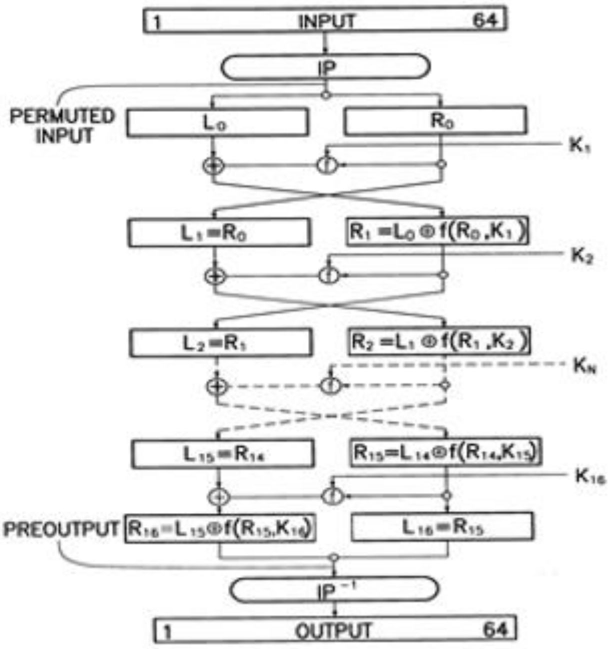

Fig. 2.DES Algorithm

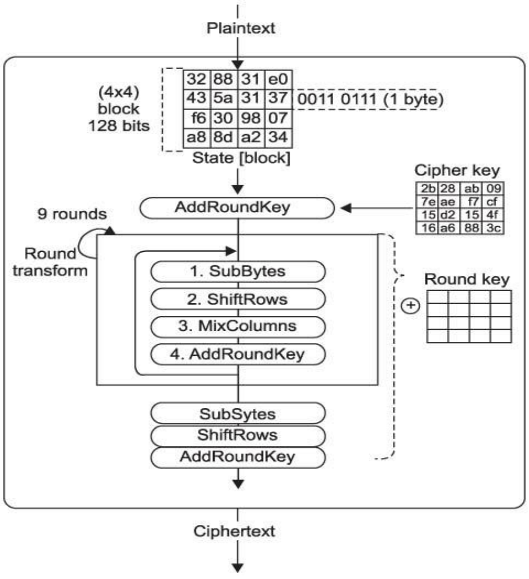

Fig. 3.AES Algorithm

D.BLOWFISH

Bruce Schneier, one of the world's leading cryptologists, designed the Blowfish algorithm [17] and made it available in the public domain. Blowfish is a symmetric key cryptographic algorithm that encrypts 64 bit blocks with a variable length key of 128-448 bits. Blowfish is the better than other algorithms in throughput and power consumption [18] [19].

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

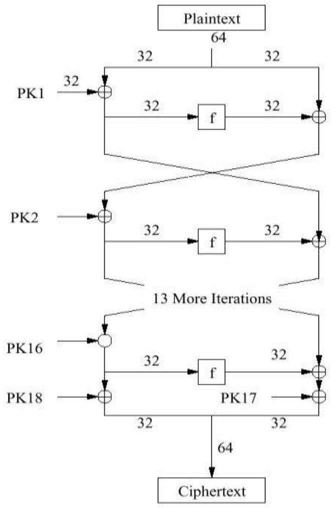

Fig. 4.Blowfish Algorithm

II. SIMULATION RESULTS AND ANALYSIS

The performance comparison of the algorithms mentioned above was conducted with different sizes of text files. 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

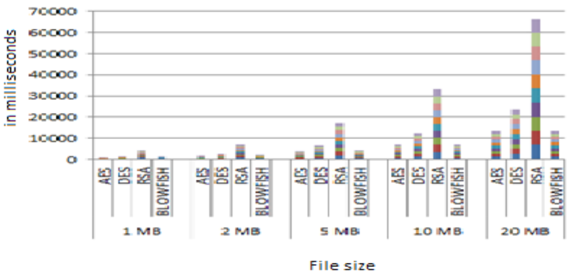

Fig.5. Graph for Encryption runtime of Text Files.

TABLE II. 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

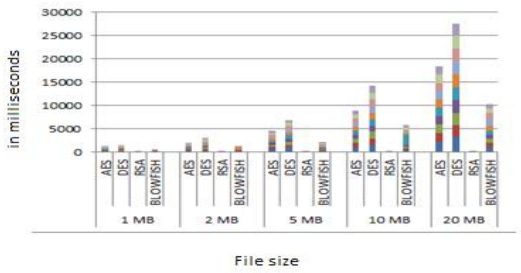

Fig.6. Graph for Decryption runtime of Text Files

TABLE III.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

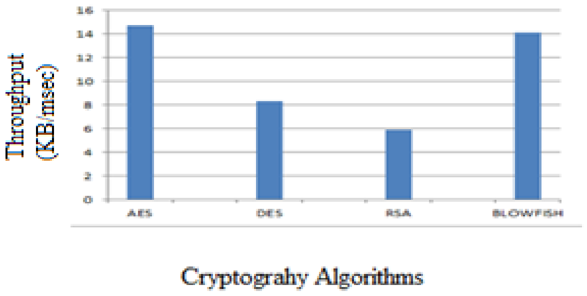

Fig.7.Graph for Throughput of Text Files.

From the tabular results of Table I and II,we have concluded that AES is taking less time to encrypt text 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 [20].So as seen from Fig.7.the throughput Graph of AES is better in case of text files encryption, 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 three algorithms in terms of both throughput and encryption-decryption time. A proposed direction for the future work could be to perform the same experiments on audio& video as well.

V. 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]. 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.

[3]. 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.

[4]. 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.

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

[6]. http://www.vocal.com/cryptography/rc4-encryption-algoritm/

[7]. Prashanti.G, Deepthi.S & Sandhya Rani.K. "A Novel Approach for Data Encryption Standard Algorithm". International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249- 8958, Volume-2, Issue-5, June 2013, pp. 264.

[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]. Vineet Kumar Singh, Dr. Maitreyee Dutta "ANALYZING CRYPTOGRAPHIC ALGORITHMS FOR SECURE CLOUD NETWORK" International Journal of advanced studies in Computer Science and Engineering IJASCSE Volume 3, Issue 6, 2014.

[11]. Dr. Prerna Mahajan & 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.

[12]. Priyanka Arora, Arun Singh, Himanshu Tyagi " Evaluation and Comparison of Security Issues on Cloud Computing Environment" in World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012.

[13]. Gurpreet Kaur, Manish Mahajan, "Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms ", Gurpreet Kaur et al. Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.782-78

[14]. Randeep Kaur, Supriya Kinger "Analysis of Security Algorithms in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 3, March 2014, ISSN 2319 – 4847.

[15]. 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.

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

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

[18]. Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[19]. Manpreet Kaur, Rajbir Singh "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 70– No.18, May 2013

[20]. 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.