Comparative Analysis Of Encryption Algorithms For Data Communication

[1]Shashi Mehrotra Seth, [2]Rajan Mishra
[1]Dept. of CS & IT, MERI College of Engg. & Tech., ASANDA (near Sampla), Bahadurgarh, Haryana, India

Abstract
Information Security has become an important issue in data communication. Encryption has come up as a solution, and plays an important role in information security system. 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 computation time. This paper performs comparative analysis of three algorithm; DES, AES and RSA considering certain parameters such as computation time, memory usages and output byte. A cryptographic tool is used for conducting experiments. Experiments results are given to analyses the effectiveness of each algorithm

Keywords
Encryption, secret key encryption, public key encryption, RSA, DES, AES encryption.

I. Introduction

For secure communication over public network data can be protected by the method of encryption. Encryption converts that data by any encryption algorithm using the 'key' in scrambled form.
Only user having access to the key can decrypt the encrypted data [4].
Encryption is a fundamental tool for the protection of sensitive information. The purpose to use encryption is privacy (preventing disclosure or confidentiality) in communications. Encryption is a way of talking to someone while other people are listening, but such the other people cannot understand what you are saying [6].
Encryption algorithms play a big role in providing data security against malicious attacks. In mobile devices security is very important and different types of algorithms are used to prevent malicious attack on the transmitted data. Encryption algorithm can be categorized into symmetric key (private) and asymmetric (public) key [1].
In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA).Public key encryption is biased on mathematical function, computationally intensive and is not very efficient for small mobile devices [10, 5].
The present scenario uses encryption which includes mobile phones, passwords, smart cards and DVDs. It has permeated everyday life and is heavily used by much web application.

A. DES Algorithms

DES is a block cipher, with a 64-bit block size and a 56-bit key. DES consists of a16-round series of substitution and permutation. In each round, data and key bits are shifted, permutated, XORed, and sent through,8 s-boxes, a set of lookup tables that are essential to the DES algorithm. Decryption is essentially the same process, performed in reverse [3].

B. AES Algorithm

AES uses 10, 12, or 14 rounds. The key size that can be 128,192 or 256 bits depends on the number of rounds. AES uses several rounds in which each round is made of several stages.
To provide security AES uses types of transformation. Substitution permutation, mixing and key adding each round of AES except the last uses the four transformations [11].

C. RSA Algorithm

RSA is a commonly adopted public key cryptography algorithm [12]. The first, and still most commonly used asymmetric algorithm RSA is named for the three mathematicians who developed it, Rivest, Shamir, and Adleman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules. Since it was introduced in 1977, RSA has been widely used for establishing secure communication channels and for authentication the identity of service provider over insecure communication medium. In the authentication scheme, the server implements public key authentication with client by signing a unique message from the client with its private key, thus creating what is called a digital signature. The signature is then returned to the client, which verifies it using the server's known public key [9].
Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power[2]. This paper examines a method for evaluation performance of various algorithms. A performance characteristic typically depends on both the encryption key and the input data.A comparative analysis is performed for those encryption algorithms at different sizes of data blocks, finally encryption/decryption speed.
The paper is organized as follows: Section1 covers the introduction part. Section 2 covers literature reviews. In section 3 experimental set up design of experiments is covered .In section 4 result analysis is performed. We conclude briefly in section 5.

II. Literature Review

It was shown in [5] that energy consumption of different common symmetric key encryption on hand held devices. It is found that after only 600 encryption of a 5 MB file using triple –DES the remaining battery power is 45% and subsequent encryption are not possible as the battery dies rapidly.
It was concluded in [7] that AES is faster and more efficient algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes.
A study in [8] is conducted for different popular secret key algorithms as DES, AES, and Blowfish. They were implemented, and their performance was compared by encryption input files of varying contents and sizes.

III. Experimental Design

The five text files of different sizes are used to conduct five experiments, where a comparison of three algorithms AES, DES

and RSA is performed. A cryptography too is use to conduct experiments.

A. Evaluation Parameters

Performance of encryption algorithm is evaluated considering the following parameters.

A. Computation Time
B. Memory usage
C. Output Bytes

The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a 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. Comparisons analyses of the results of the selected different encryption scheme are performed.

IV. Experimental Results and Analysis

Experimental result for Encryption algorithm AES, DES and RSA are shown in table1, which shows the comparison of three algorithm AES, DES and RSA using same text file for five experiment, output byte for AES and DES is same for different sizes of files. By analyzing the table 1, we noticed the RSA has very smaller output byte compare to AES and DES algorithm. Time taken by RSA algorithm is much higher compare to the time taken by AES and DES algorithm. Variation in memory usage is noticed. It does not increase according to size of file in all algorithms.

By analyzing Fig. one which shows time Taken for encryption on various size of text file by three algorithms i:e AES, DES and RSA, it is noticed that RSA algorithm takes much longer time compare to time taken by AES and DES algorithm . DES algorithm consumes least time for encryption. AES and DES algorithm show very minor difference in time taken for encryption.

Fig. 2 which show memory usages by AES, DES and RSA algorithm. It is notice that RSA algorithm memory usages are highest for all sizes of text file while memory usage is least.

Fig. 3 shows the size of output byte for each algorithm used in experiment. The result of Fig. shows same size of output byte for different size of text file in case of all three algorithms.

Table 1: Comparisons of AES, DES and RSA of Time, Memory and Output byte.

DATA	ALGO.	TIME (SEC)	MEMORY (KB)	OUTPUT BYTE
FILE 1 (68KB)	AES	2.2	81,912	131,072
	DES	1.8	85,261	131,072
	RSA	9.4	91,814	65,536
FILE 2 (105)	AES	2.1	62,544	131,072
	DES	1.8	67,531	131,072
	RSA	10.5	77,117	65,536
FILE 3 (124 KB)	AES	2.2	53,902	131,072
	DES	2	55,395	131,072
	RSA	11.4	57,178	65,536
FILE 4 (235KB)	AES	2.4	16,679	131,072
	DES	2.1	21,189	131,072
	RSA	16.2	26,891	65,536
FILE 5 (435KB)	AES	2.6	34,207	131,072
	DES	2.4	42,113	131,072
	RSA	24.4	44,321	65,536

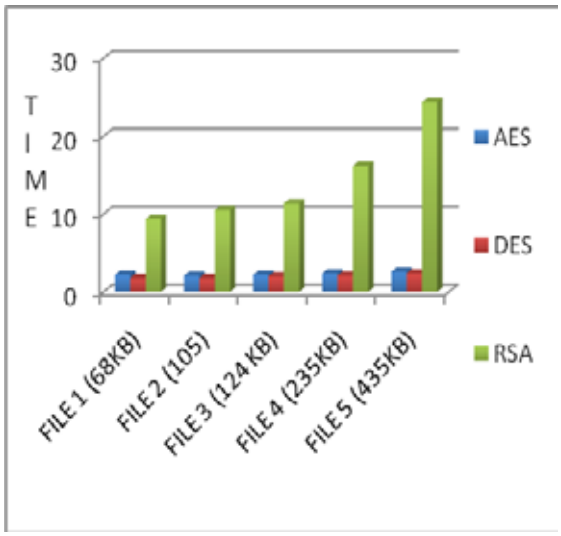

Fig. 1: Comparison of Computation Time among AES, DES and RSA

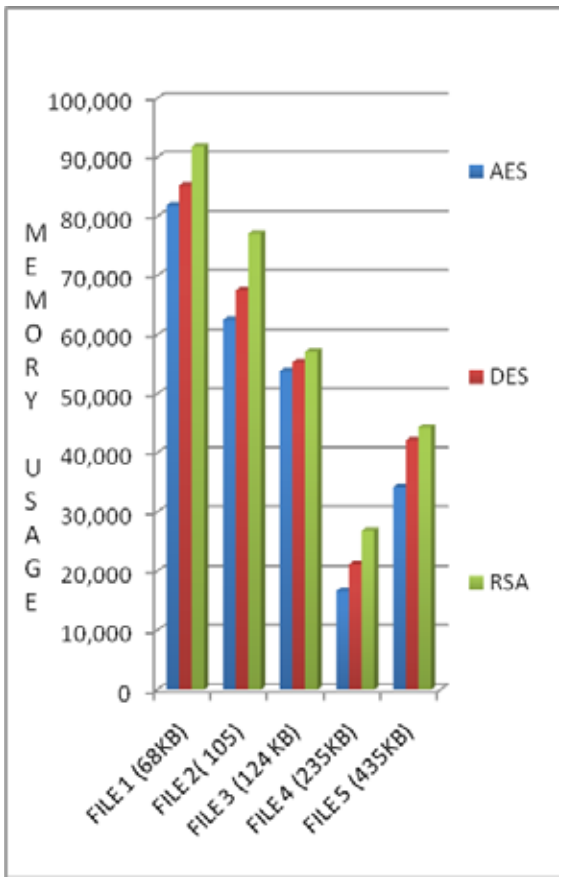

Fig. 2: Comparison of Memory usage by AES, DES and RSA

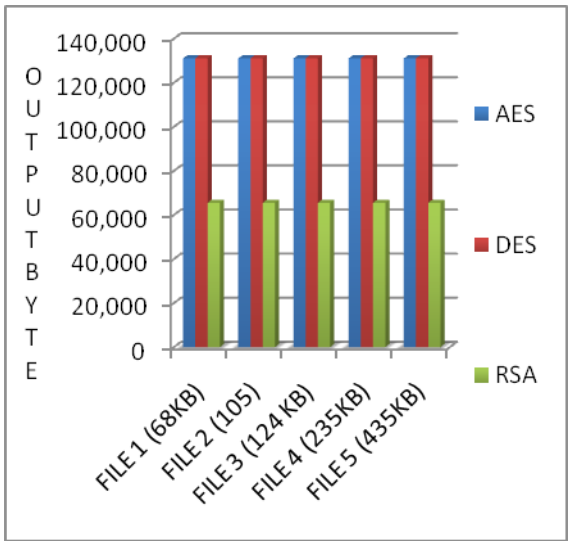

Fig. 3: Comparison of Output Byte used by AES, DES and RSA

V. Conclusion

Encryption algorithm play an important role in communication security where encryption time, Memory usages output byte and battery power are the major issue of concern. The selected encryption AES, DES and RSA algorithms are used for performance evaluation.

Based on the text files used and the experimental result it was concluded that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm.

RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm.

Our future work will include experiments on image and audio data and focus will be to improve encryption time and less memory usage.

References

[1] DiaasalamaAbdElminaam, HatemMohamadAbdual Kader, Mohly Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", international journal of network security vol.10,No.3,pp,216-222,May 2010.

[2] Diaasalama, Abdul kader, MohiyHadhoud, "Studying the Effect of Most Common Encryption Algorithms", International Arab Journal of e-technology, vol 2,no.1,January 2011.

[3] Erik Olson, Woojin Yu, "Encryption for Mobile Computing"

[4] Anoop MS, "Public key Cryptography (Applications Algorithm and Mathematical Explanations)"

[5] P.Ruangchaijatupon, P.Krishnamurthy, "Encryption and power consumption in wireless LANs-n," The Third IEEE workshop on wireless LANS, pp. 148-152, Newton, Massachusetts, sep. 27-28, 2001.

[6] Marshall D.Abrams, Harold J.podell on Cryptography.

[7] S. Hirani, Energy Consumption of Encryption schemes in wireless device Thesis, university of Pittsburgh, Apr. 9, 2003, Retrieved Oct.1, 2008.

[8] A.Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.Bn

[9] Andrea Pellegrini, Valeria Bertacco, Todd Austin on topic Fault-Based attack of RSA Authentication

[10] Hardjono, security in wireless LANS and MANS, Artech house Publisher, 2005.

[11] NeetuSettia. "Cryptanalysis of modern Cryptography Algorithms". International Journal of Computer Science and Technology. December 2010.

[12] R.Rivest, A. Shamir, L.Adleman. "A method for obtaining digital signatures and public-key cryptosystems"z. Communications of the ACM, Feb 1978.

Shashi Mehrotra Seth received her M.Tech degree in Computer Engineering. She has more than 7 years of teaching experience. Presently she is working as Assistant Professor and Head of the Department of CS & IT in MERI College of Engineering & Technology, Bahadurgarh Haryana. Her area of specialization is Data Mining, Soft Computing and Security. She has presented papers in national & international conferences and has received awards for her work. She has also published papers in national and international journals and conference proceedings.

Rajan Mishra is pursuing his Bachelor's degree in Computer science from MERI college of Engineering Haryana, INDIA. He is working as budding researcher in field of research on topic Data security .