Volume-4, Issue-1, February-2014, ISSN No.: 2250-0758
International Journal of Engineering and Management Research
Available at: www.ijemr.net
Page Number: 132-134

Comparative Analysis of DES, AES, RSA Encryption Algorithms

Priteshkumar Prajapati[1], Nehal Patel[2], Robinson Macwan[3], Nisarg Kachhiya[4], Parth Shah[5]
[1, 2, 3, 4,5]Department of Information Technology, INDIA

ABSTRACT

As the increasing growth of the computing technology and network technology, it also increases data storage demands. Data Security has become a crucial issue in electronic communication. Secret writing has come up as a solution, and plays a vital role in data security system. It uses some algorithms to scramble data into unreadable text which might be only being decrypted by party those having the associated key. These algorithms consume a major amount of computing resources such as memory and battery power and computation time. This paper accomplishes comparative analysis of encryption standards DES, AES and RSA considering various parameters such as computation time, memory usages. A cryptographic tool is used for performing experiments. Experiments results are given to analyses the effectiveness of symmetric and asymmetric algorithms.

Keywords— Encryption, secret key encryption, public key encryption, DES, AES, RSA encryption, Symmetric

I. INTRODUCTION

For secure correspondence over open system information can be ensured by the technique for encryption. Encryption changes over that information by any encryption calculation utilizing the 'key' in mixed frame. Just client approaching the key can unscramble the scrambled information [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, 14].

Encryption calculations assume a major part of giving information security against pernicious assaults. In cell phones, security is imperative and diverse sorts of calculations are utilized to avoid the pernicious assault on the transmitted information. Encryption calculation can be sorted into the symmetric key and asymmetric key [1].

In Symmetric keys encryption or secret key encryption, just a single key is utilized to encode and unscramble information. In Asymmetric keys, two keys are utilized; private and public keys. The public key is utilized for encryption and a private key is utilized for decoding (e.g. RSA).Public key encryption is one-sided on numerical capacity, computationally serious and isn't extremely effective for little cell phones [10, 5].

The present scenario uses encryption which includes pen drive, mobile phones, passwords and smart cards. 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 16-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, 14].

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 following types of transformation Substitution, permutation, mixing and key adding each round of AES except the last uses the four transformations. [11, 14].

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, and 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, 14].

Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power [2, 14]. 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 rest of paper is organized as follows: 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 is found 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, 15] 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, 16] 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.

In [13] compares and find out faster algorithm among popular secret key algorithms DES, 3DES, AES, Blowfish, RC2, and RC6.

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 cryptographic tool is use to conduct experiments.

A. Evaluation Parameters

Performance of encryption algorithm is evaluated considering the following parameters.

A. Computation Time

B. Memory usage

The Computational time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text. It is used to calculate the throughput of an encryption scheme, is calculated as the total plaintext in bytes encrypted divided by the encryption/decryption 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 experiments i.e. 32KB, 64KB, 128KB, 256KB, and 512KB. By analyzing the table 1, we noticed the 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.1 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. AES and DES algorithm showvery minor difference in time taken for encryption.

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

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

Data (KB)	Time (Sec.)			Memory (KB)		
	DES	AES	RSA	DES	AES	RSA
32	1.81	2.02	9.45	84,261	80,912	90,814
64	1.83	2.13	10.53	66,531	61,544	76,117
128	2.03	2.29	11.41	54,395	52,902	55,178
256	2.14	2.47	16.27	22,189	15,679	25,891
512	2.43	2.63	24.44	41,113	33,207	43,321

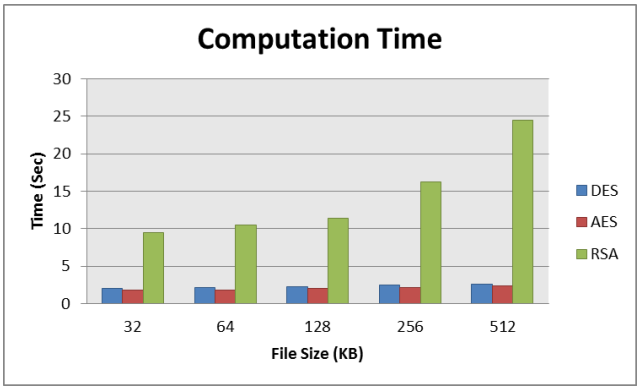

Fig. 1: Comparison of Computation Time among AES, DESand RSA

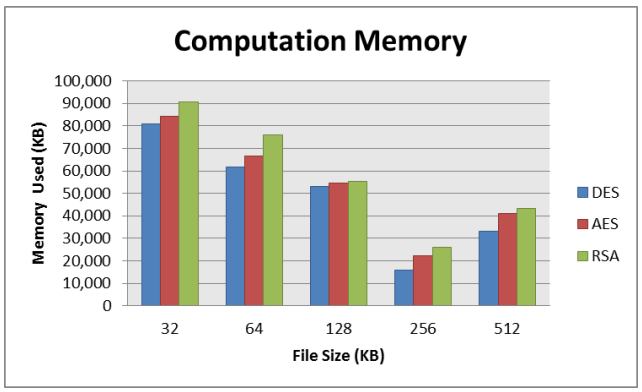

Fig. 2: Comparison of Memory usage by AES, DES and RSA

V. CONCLUSION

Encryption algorithm plays an important role in communication security where encryption time, Memory usages 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 AES and DES algorithm consumes least encryption timecompare to RSA and DES algorithm has least memory usage while encryptiontime difference is very minor in case of AES algorithm and DES algorithm.When data size increases then asymmetric cryptographic algorithm performs slower compare to symmetric algorithm.

REFERENCES

[1] Diaasalama Abd Elminaam, 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 MobileComputing"
[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] S. Hirani, Energy Consumption of Encryption schemes in wireless device Thesis, university of Pittsburgh, Apr. 9, 2003, Retrieved Oct.1, 2008.
[7] A.Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.
[8] Andrea Pellegrini, Valeria Bertacco, Todd Austin on topic Fault-Based attack of RSA Authentication.
[9] Hardjono, security in wireless LANS and MANS, Artech house Publisher, 2005.
[10] NeetuSettia. "Cryptanalysis of modern Cryptography Algorithms".International Journal of Computer Science and Technology. December 2010.
[11] R.Rivest, A. Shamir, L.Adleman. "A method for obtaining digital signatures and public-key cryptosystems"z. Communications of the ACM, Feb 1978
[12] Elminaam, D. S. A., Kader, H. M. A., &Hadhoud, M. M. (2008). Performance Evaluation of Symmetric Encryption Algorithms. IJCSNS International Journal of Computer Science and Network Security, 8(12), 280-286.
[13] Seth, S. M., & Mishra, R. (2011). "Comparative analysis of encryption algorithms for data communication." International Journal of Computer Science and Technology
[14] Chehal, R., Singh, K., & Singh, K. (2012). Efficiency and security of data with symmetric encryption algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, 2(8).
[15] Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2008). Performance evaluation of symmetric encryption algorithms. IJCSNS International Journal of Computer Science and Network Security, 8(12), 280-286.
[16] Mahajan, P., & Sachdeva, A. (2013). A study of encryption algorithms AES, DES and RSA for security. Global Journal of Computer Science and Technology.