International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-2, February 2016
ISSN: 2395-3470
www.ijseas.com

Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security

Kalyani P. Karule [1], Neha V. Nagrale [2]

[1] P.G. Student, Department of Computer Science and Engineering, Yeshwantrao Chavan College of Engineering, Hingna Road, Nagpur-441110, India.

[2] P.G. Student, Department of Computer Science and Engineering, Yeshwantrao Chavan College of Engineering, Hingna Road, Nagpur-441110, India.

Abstract

Security of data means protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorized users. Information Security is an important issue in data communication. Encryption comes up as a solution, and plays an important role in information security system. This security mechanism uses some algorithms to mix-up data into unreadable text which can only be decrypted by party who possesses the associated keys. These algorithms consume a considerable amount of computing resources such as memory and computation time. This paper performs comparative analysis of two algorithm; AES and RSA considering certain parameters such as encryption time, memory usages. A cryptographic tool is used for conducting experimentation on various types of data files with extension such as .jpeg, .txt, .doc and .pdf. Experimental results are given for comparative analysis of performance of both the algorithms.

Keywords: *Data Security, AES, RSA, Encryption, Comparative analysis.*

1. Introduction

Cryptography technique often used to secure the data transmission and storing between user and cloud storage services. For secure communication over the public network data can be protected by the methods of encryption. Encryption converts that data by any encryption algorithm using the key in mixed-up form. Only user having access to the key can decrypt the encrypted data [3].

Encryption is an essential tool for the protection of sensitive data. The purpose to use encryption is privacy (preventing disclosure or confidentiality) while transfer of data. Encryption algorithms play an important role in providing security of data against malicious attacks. In mobile devices security is very important and different types of algorithms are used to defend from malicious attack on the transmitted data. Encryption algorithm can be categorized into symmetric key (private) and asymmetric key (public) [10].

In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data (files) (e.g. AES). 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).

1.1 AES Algorithm

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

1.2 RSA Algorithm

The first, and still most consistently used asymmetric algorithm RSA is named on the three mathematicians who developed it, Rivest, Shamir, and Adleman. RSA today is used in hundreds of software products and possibly used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a flexible size encryption block and a flexible size key. The key pair is acquired from a very large number, n, that is the product of two prime numbers chosen in accordance to special rules. Since it was introduced in 1977, RSA has been broadly used for establishing secure communication channels and for authentication the identity of service provider over defenseless communication medium. In the authentication scheme, the server implements public key authentication by taking signature of client on a unique message from the client with its private key, thus creating what is called a digital signature. The signature is returned to the client, which verifies it using the server's known public key [9].Encryption algorithms consumes some significant amount of computing resources; such as CPU time, memory, and battery power [2]. This paper examines a method for evaluating the performance of both algorithms. A performance characteristic mainly depends on both the encryption key and the input data. A comparative analysis is performed for those encryption algorithms at different

sizes of data, finally encryption/decryption time. The paper is organized as follows: Section1 covers the introduction part. Section 2 covers literature reviews. In section 3 experimental design of experiments is covered .In section 4 experimental results and analysis is performed. We conclude briefly in section 5.

2 Literature Review

It was concluded in [5] that AES algorithm is faster and more efficient. When the transmission of data is considered there is slight difference in performance of different symmetric key schemes. A study in [8] is conducted for different popular secret key algorithms as AES, DES, and Blowfish. They were implemented, and their performance was compared by encryption of input files of varying contents and sizes.

3 Experimental Design

The different types and sizes of files with extension such as .jpeg, .txt, .doc, and .pdf are used to conduct experiments, where a comparison of two algorithms AES and RSA is performed. Cryptographic tool is used to conduct experiments.

3.1 Evaluation Criterion

Performance of the encryption algorithms is evaluated considering the following criteria.
A. Encryption time
B. Memory usage (encrypted file size)
The encryption time is considered to be the time that an encryption algorithm takes to generate a cipher text from a plain text. Encryption time is calculated by 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 algorithm are performed.

4 Experimental Results and Analysis

Four types of files of different size are used for experimentation of two encryption algorithms AES and RSA. Fifty different files of each type i.e. pdf, jpeg, doc and text are used for testing of algorithm to check memory usage and encryption time. The comparative experimental results of four types of file with small, medium and large size on AES and RSA are shown in Table 1. The AES and RSA algorithms are tested on two parameters memory usage i.e. size of encrypted file and encryption time taken by both algorithms for same file. By analyzing the table 1, we noticed that RSA has more memory usage as compared to AES algorithm. Time taken by RSA algorithm is less as compared to the time taken by AES algorithm. Variation in memory usage is noticed. By analyzing Figure1, shows encryption time taken for encryption on various size of text file by two algorithms i.e. AES and RSA, it is noticed that RSA algorithm takes much less time compared to the time taken by AES algorithm. However memory uses i.e. encrypted file size using RSA is higher as compared to file encrypted using AES algorithm.

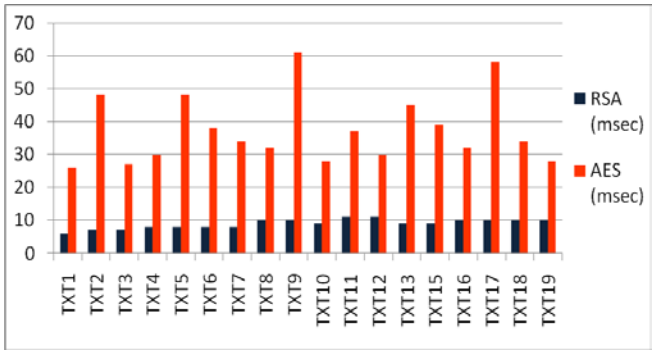

Figure 1: Comparison of encryption time for various sizes of text files

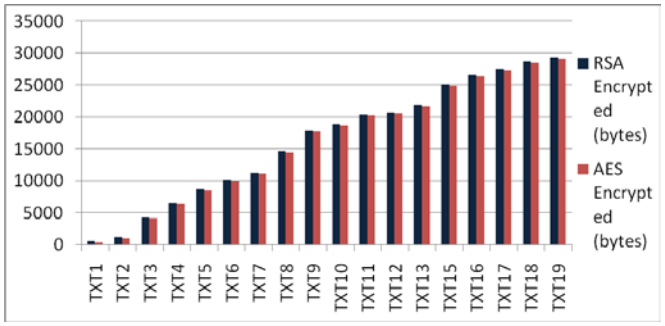

Figure 2: Comparison of memory usage for various sizes of text files

Table 1. Comparative Analysis of RSA and AES

File Type	Data file (Bytes)	Algorithm	Encrypted Size	Time (msec)
JPEG	1.jpg (2513)	RSA	3496	11
		AES	2696	25
	25.jpg (10693)	RSA	10888	10
		AES	10704	38
	50.jpg (1036372)	RSA	1036552	81
		AES	1036384	164
TEXT	1.txt (408)	RSA	584	6
		AES	416	26
	25.txt (42317)	RSA	42504	11
		AES	42320	62
	50.txt (255952)	RSA	256136	31
		AES	255968	61
DOC	1.doc (5180)	RSA	5352	7
		AES	5184	26
	25.doc (105902)	RSA	106088	17
		AES	105904	44
	50.doc (2020915	RSA	2021096	173
		AES	2020928	311
PDF	1.pdf (1245)	RSA	1416	7
		AES	1248	66
	25.pdf (213408)	RSA	213608	31
		AES	213424	64
	50.pdf (12256590)	RSA	12256776	454
		AES	12256592	1298

5 Conclusion

The selected encryption algorithms AES and RSA are used for performance evaluation. For performance evaluation files in different formats like text files, pdf file, word document and images are used and the experimental result based on encrypted file size and encryption time is recorded. From the comparative analysis it is concluded that RSA requires less encryption time as compared to AES, however AES memory usage is less as compared to RSA for all four types of files with extension such as .jpeg, .txt, .doc and .pdf. It is clear from the experimentation that for RSA is performing much better than AES in terms of encryption time. The focus of experimentation is on comparing the performance and effectiveness of both the algorithms (e.g. AES and RSA) providing secure files transmission between these two entities. A combination of asymmetric and symmetric encryption techniques (i.e. RSA and AES encryption methods) depending on the file type is proposed.

References

[1] Nasrin Khanezaei, Zurina Mohd Hanapi, "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", Proceedings of 2014 IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia, pp 58-62.

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

[3] Anoop MS, "Public key Cryptography".

[4] Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", Proceedings of IEEE Computer Society, International Conference on Computer Science and Electronics Engineering, 2012, DOI 10.1109/ICCSEE.2012.193, pp 647-651.

[5] S. Hirani, Energy Consumption of encryption schemes in wireless device thesis, University of Pittsburgh, Apr. 9, 2003, Retrieved Oct.1, 2008.

[6] G. Jai Arul Jose, C. Sajeev, "Implementation of Data Security in Cloud Computing", International Journal of P2P Network Trends and Technology- Volume1Issue1- 2011, pp 18-22.

[7] Parsi Kalpana and Sudha Singaraju,"Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012, pp 143-146.

[8] A.Nadeem, "A performance comparison of data encryption algorithms", IEEE Information and Communication Technologies, pp.84-89, 2006.

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

[10] Diaasalama Abd Elminaam, Hatem Mohamad Abdual Kader, Mohly Mohamed Hadhoud, "Evaluation of the Performance of Symmetric Encryption Algorithms", International Journal of Network Security vol.10, No.3, pp, 216-222, May 2010.

[11] Neetu Settia, "Cryptanalysis of modern Cryptography Algorithms", International Journal of Computer Science and Technology. December 2010.
[12] Du meng,"Data security in cloud computing", Proceedings of the 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka, pp 810-813.

Author Profile

Kalyani P. Karule received the BE. in 2014 and pursuing M.Tech. Degree in Computer Science and Engineering from Yeshwantrao Chavan College of Engineering, Nagpur, India. Working on project research topic Data security in Cloud Computing.

Neha V. Nagrale received the BE. in 2013 and pursuing M.Tech. Degree in Computer Science and Engineering from Yeshwantrao Chavan College of Engineering, Nagpur, India. Working on project research topic Network security.