ISSN 2250-3153

Comparative Analysis of AES and DES security Algorithms

Sumitra

Lecturer (Computer science)
Advanced Institute of Technology & Management, Palwal

Abstract - In recent years network security has become an important issue. Cryptography has been used to secure data and control access by sharing a private cryptographic key over different devices. Cryptography renders the message unintelligible to outsider by various transformations Data Cryptography is the scrambling of the content of data like text, image, audio and video to make it unreadable or unintelligible during transmission. Its main goal is to keep the data secure from unauthorized access.

Index Terms: AES, DES, Cryptography, Symmetric key, Asymmetric key, Encryption, Decryption

I. INTRODUCTION

The goal of cryptography is to make it possible for two people to exchange a message in such a way that other people cannot understand the message. There is no end to the number of ways this can be done, but here we will be concerned with methods of altering the text in such a way that the recipient can undo the alteration and discover the original text. The original text is usually called "clear text" and the encoded or altered text is called "cipher text". The conversion from clear text to cipher text is called "encoding" or "enciphering", and the opposite operation is called "decoding" or "deciphering". Information is an asset that has a value like any other asset. As an asset, information needs to be secured from attacks. Now-a-days security becomes an essential feature in almost all area of communication. While sending a message to a person over an insecure channel such as internet we must provide confidentiality, integrity, authenticity and non-repudiation [1]. These are the four major security aspects [2] or goals.

There are a number of encryption algorithms those can be broadly classified into two categories: *Symmetric/Private key encipherment* and *Asymmetric/Public key encipherment* [3, 4]. The difference between these two is that to communicate with *n* people *private key cryptography* requires (*n*£(*n*¡1))=2 number of keys as shown in the Figure 1.1 whereas; *public key cryptography* requires only *n* number of key pairs (one private and one public key) .

Public key cryptography discovered nearly two decades ago has revolutionized the way for the people to communicate securely and in an authenticated way [1]. Any message (text, binary ¯les, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

II. Basics

Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right[5,6]. Cryptography has often been used to protect the wrong things, or used to protect them in the wrong way. We'll see plenty more examples when we start looking in detail at real applications. Unfortunately, the computer security and cryptology communities have drifted apart over the last 20 years. Security people don't always understand the available crypto tools, and crypto people don't always understand the real-world problems. There are a number of reasons for this, such as different professional

backgrounds (computer science versus mathematics) and different research funding (governments have tried to promote computer security research while suppressing cryptography).

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process[9,10]. It is a science of protecting information by encoding it into an unreadable format. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, *cryptanalysis* is the science[7]. Of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called *attackers*. *Cryptology* embraces both cryptography and cryptanalysis.

III. Types of Cryptosystems

There are three types of cryptosystems: Symmetric key, Asymmetric key and Hash Functions. Symmetric key encryption uses one key to encrypt and decrypt. Asymmetric key encryption uses two keys; when one key is used to encrypt, the other is used to decrypt. Hash functions create a message digest via an algorithm and use no key.

(a) *Symmetric key Encryption*

Symmetric key (also called private key or secret key) cryptography uses the same key to encrypt and decrypt. The name "private key" derives from the need to keep the key private. A major challenge associated with symmetric key cryptosystems is the secure distribution of keys. Common symmetric key encryption algorithms include DES (the Data Encryption Standard) and AES (the Advanced Encryption Standard).

(b) *Asymmetric Key Encryption*

Asymmetric key encryption (also called public key encryption) uses two keys: a public and a private key. Data encrypted with one key can be decrypted only with the other key. Whitfield Diffie and Martin Hellman first publicly described this approach in November 1976in *New Directions in Cryptography*, where they announced: "We stand today on the brink of a evolution in cryptography."

IV. Comparison of AES, DES

a) *AES, DES analyzing time based on different file size using Entropy on machine1(Intel Dual core 2.4 Ghz Processor with 1 GB RAM)*

The time taken by AES, DES security algorithm on machine1 using entropy is shown below in the graph.This comparison is done on machine1 with *Intel Dual core 2.4 Ghz Processor with 1 GB RAM* configuration.

File Size	AES(Time in sec)	DES(Time in sec.)
512Kb	49.03	66.09
1Mb	44.84	67.94
1.5Mb	47.8	57.47
2.0Mb	51.14	66.29
2.5Mb	51.28	59.42

Table 5.1 Comparison based on entropy

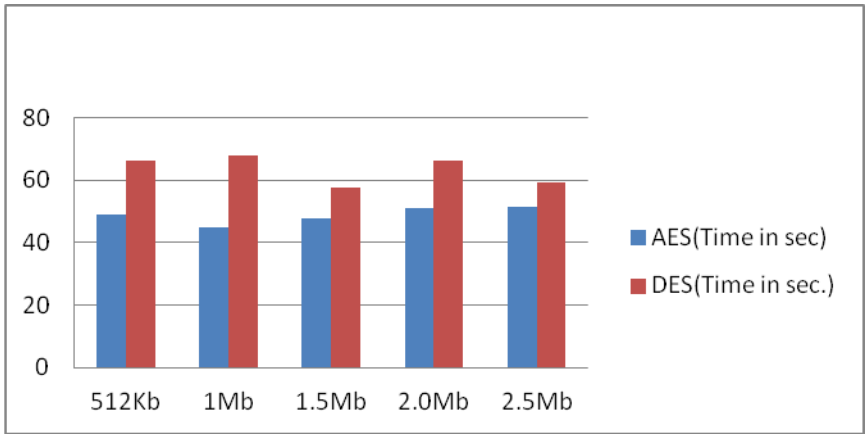

Fig. 5.1: Analyzing time based on entropy

b) AES, DES Analyzing time based on different file size using Known Plaintext on machine1(Intel Dual core 2.4 Ghz Processor with 1 GB RAM)

A simulation test was carried out over various files of different size on machine1. This comparison is done on machine1 with *Intel Dual core 2.4 Ghz Processor with 1 GB RAM* configuration.The result that was obtained is shown below in the graph.

File Size	AES(Time in sec.)	DES(Time in sec)
512Kb	24.68	34.64
1Mb	28.98	28.56
1.5Mb	23.38	30.47
2Mb	26.71	28.45
2.5Mb	25.31	34.67

Table 5.2: Comparison based on known plaintext

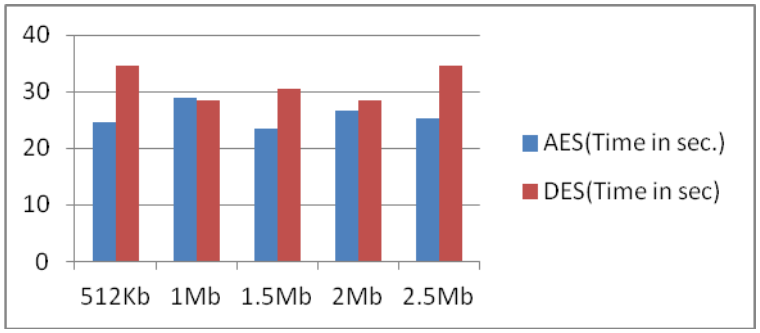

Fig.5.2: Analyzing time based on known plaintext

C) AES, Analyzing time based on different file size using Entrophy on machine2(Intel core i3 processor with 2 GB RAM)

Here a machine with different configuration is used to carry out the time analysis between these algorithms. A number of files with different sizes were fed into the simulation test. The result obtained after simulation are represented in the form of graph below.

File Size	AES(Time in sec.)	DES(Time in sec)
512Kb	36.81	35.28

1Mb	32.81	45.45
1.5Mb	30.75	35.59
2.0Mb	31.15	37.7
2.5Mb	45.53	37.89

Table 5.3. Comparison based on entropy

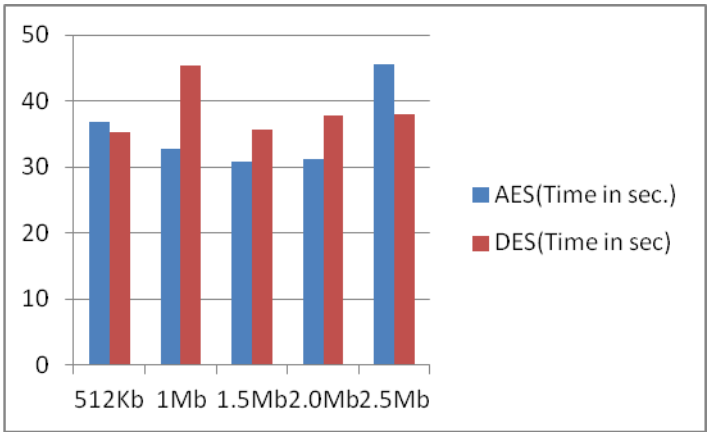

Fig.5.3. Analyzing time based on entropy

d) AES,Des and SDES Analyzing time based on different file size using Known Plaintext on machine2(Intel core i3 processor with 2 GB RAM)

This graph has shown the time being utilized by AES, DES and SDES security algorithms on a machine2 using known plaintext. With the help of graph and table the comparison of AES, DES and SDES security algorithms is shown.

File Size	AES	DES
512Kb	18.5	21.02
1Mb	19	22.7
1.5Mb	20.52	21.35
2.0Mb	19.08	22.77
2.5Mb	18.92	23.01

Table 5.4: Comparison based on known plaintext

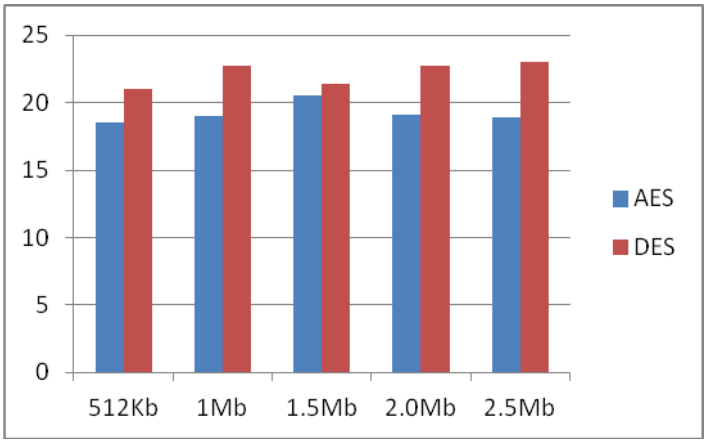

Fig.5.4: Analyzing time based on known plaintext

IV. CONCLUSION AND FUTURE SCOPE

From above work it is concluded that security is an important issue at present time .There are a no. of schemes are available for security purpose This scheme is called cryptography. In cryptography we use key called public key and private key.With the help of these keys we encrypt and decrypt the data fro make secure. Encrypted data is called ciphertext and decrypted data s called plaintext. Cryptography is of two types : a) Symmetric b) asymmetric. In this paper two symmetric key security algorithms AES and DES are compared .Symmetric key algorithms are those algorithms which have same key for encryption and decryption. All Also above work shows the performance of both algorithms .It is shown that both algorithms consume different times at different machines. Different machines take different times for same algorithm over same data packet. From above explanation it is shown that all algorithms have different speed. AES is more secure as compare to DES.

REFERENCES

[1] Yuliang Zheng. Digital signcryption or how to achieve cost(signature encryption) cost(signature) + cost(encryption). In CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, pages 165{ 179, London, UK, 1997. Springer-Verlag.

[2] William Stallings. Cryptography and Network security: Principles and Practices. Prentice Hall Inc., second edition, 1999.

[3] Paul C. van Oorschot Alfred J. Menezes and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.

[4] Behrouz A. Forouzan. Cryptography and Network Security. Tata McGraw-Hill, 2007.

[5] William J Caelli, Edward P Dawson, and Scott A Rea. Pki, elliptic curve cryptog-raphy, and digital signatures. Computers and Security, 18(1):47 { 66, 1999.}

[6] Lawrence C. Washington. ,Elliptic Curves: Number Theory and Cryptography.CRC Press, 2003.

[7] Surya A. E®endi R. Sutikno, S. An implementation of elgamal elliptic curves cryptosystems. pages 483 {486, Nov 1998.}

[8] G. JULIUS CAESAR , JOHN F. KENNEDY “Security Engineering: A Guide to Building Dependable Distributed Systems ,”pages 73.

[9] \ CISSP All-in-One Certification Exam Guide,” 200075_ch08_HarrisX 11/30/01 10:22 AM Page 495”

[10] Phil Zimmermann ,An Introduction to Cryptography” The Basics of Cryptography”.

AUTHOR

Sumitra , M.Tech (CSE.),A.I.T.M. Palwal. Sumitra.gupta1@gmail.com