DES VS AES ALGORITHM USING NETWORK SECURITY AND CRYPTOGRAPHY

A thesis submitted in partial fulfillment of the requirements of Varendra University for the degree of BSc Engineering in CSE.

January 2024

Submitted by
Md. Sozibul Islam, ID: 201311122
Md. Foyshal Ahmed Biswas, ID: 201311137
Most. SanjithaMim, ID: 201311193

Department of Computer Science and Engineering
Varendra University
Rajshahi, Bangladesh

Supervised by
Sabina Yasmin
Assistant Professor
Department of Computer Science and Engineering
Varendra University
Rajshahi, Bangladesh

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
VARENDRA UNIVERSITY

CERTIFICATE

This is to certify that this thesis report entitled **"DES VS AES ALGORITHM USING NETWORK SECURITY AND CRYPTOGRAPHY"** submitted by Md. Sozibul Islam (ID: 201311122),Md. Foyshal Ahmed Biswas (ID: 201311137), Most. Sanjitha Mim (ID: 201311193)in partial fulfillment of the requirement for the award of the degree of Bachelor of Science in Computer Science and Engineering of Varendra University, Bangladesh is a record of the candidate own carried out by them under my supervision. This thesis has not been submitted for the award of any other degree.

Supervisor

Sabina Yasmin
Assistant Professor
Department of Computer Science and Engineering
Varendra University
Rajshahi, Bangladesh

Abstract

In today's internet era ,Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. 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 computation time. In this paper two most widely used symmetric encryption techniques data encryption standard (DES) and advanced encryption standard (AES) have been implemented. This paper provides a fair comparison between the most common symmetric key cryptography algorithms: DES, 2DES , AES. Since main concern here is the performance of algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. The comparison is made on the basis of these parameters: speed, block size, and key size. Simulation program is implemented using Java programming. This paper takes a simple literature survey. In which they are one of the significant modules to secure and/or the messages using crypt file keys. In these, DES, 2DES, AES concepts are used to protect the file with the service of encryption and decryption affair. In our paper, we have implemented and analyzed in detail cost and performance of popularly used cryptographic algorithms DES, 2DES, AES. Performance Evaluation: AES, DES Analyzing time based on different file size using Known Plaintext on machine1(Intel Dual core 1.8Ghz Processor with 4 GB RAM).For 104kb file size the run time of DES 0 ,2DES 0 and AES 1.And others runtime description have been describe in methodology.

Acknowledgements

It has been a long and difficult journey, but as a team, we have finally reached our desired outcome, which is a delight.

Predominantly, we would like to thank our supervisor Sabina Yasmin(Assistant Professor, Department of Computer Science and Engineering, Varendra University) for her inspiration, very fruitful collaboration, to do difficult tasks easily, and to be with us generous mind. In a practical sense, the work would have been impossible to complete without her inspiration and guidance. Fortunately, we are not the only ones walking on this trip. We are expressing our sincere gratitude to everyone who has assisted us so far.

We are grateful to Varendra University for providing us with the opportunity to complete our graduation and thesis work in a beautiful environment. We would like to express our respect and gratitude to all the teachers who have helped and encouraged us throughout this thesis work. We would like to thank all the friends who supported us with all their efforts and also thank all the people associated with the thesis work whose work has triggered our thoughts.

Finally, love and respect to parents and family who always wish us success and happiness in all spheres of life. May the peace and mercy of the merciful Allah be upon all.

Contents

List of Figure

List of Table

List of Graph

Chapter 1

Introduction

Cryptography is the science of keeping message secure. The method, in which we disguising a message in such a way so that its substances are kept are encryption and encrypted message, is cipher text[1]. These two industry mainstays of encryption are essential for protecting sensitive data being transferred across networks. Data Encryption Standard (DES) was lodged by NBS/NIS (National Bureau of Standards/ National Institute of Standards) in1977[12], was once the mainstay of cryptography techniques, but a move towards more reliable alternatives has been spurred by DES's vulnerability to contemporary computing power. Presenting AES, a strong heir acknowledged for its effectiveness, durability, and adaptability. The article discusses the differences between the DES and AES algorithms, exploring their complexity as well as how they affect network security in the dynamic world of the internet. As we explore the intricate details of these giants of the use of cryptography this inquiry delivers revelations.

1.1 Data Encryption Standard (DES)

The Data Encryption Standard, or DES, is a block cipher that uses a 56-bit key and a 64-bit block size. The connotation of DES is to confer a standard and confident method to protect the vulnerable information and unclassified data. Each 64 bits of data is ingeminate from 1 to 16 times (which means 16 rounds)[11].

DES is an operations sequence that consists of 16 rounds, with substitution and permutation used in each round. During the process, each of the eight S-boxes—critical lookup tables that are essential to DES—as well as the data and key bits go through shifts, permutations, XOR operations, and other processes. The algorithm's cryptographic strength is increased by these S-boxes, which introduce non-linearity. The decryption is comparable to encryption, however it is carried out in the opposite sequence. DES is a complicated algorithm that provides robust encryption through a well-orchestrated sequence of cryptographic operations. This is demonstrated by the elaborate dance of shifting, permuting, and XORing within DES.

1.2 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) algorithm is one of the block cipher encryption algorithm that was published by National Institute of Standards and technology (NIST) in 2000[11].The Advanced Encryption Standard, or AES, stands for its adaptability, using 10, 12, or 14 rounds based on the chosen key size (128, 192, or 256 bits). The algorithm's durability is determined directly by the number of rounds. With AES, each round consists of multiple steps that have been strategically designed to advance the encryption process.

AES uses four different kinds of transformations in every round—all but the final one—to guarantee security. Key addition, mixing, and substitution-permutation are some of these transformations. The substitution-permutation operation strengthens defenses against cryptographic attacks by introducing non-linearity through byte replacement and permutation. The overall strength of the method is enhanced by mixing procedures, which further boost the diffusion of input data. Key addition adds another level of complexity and security to the encryption process by integrating the secret key utilizing XOR operations.

1.3 Meet-In -The Middle Attack

A cryptographic attack technique known as a "meet-in-the-middle" attack takes advantage of the bidirectional character of some encryption-decryption procedures[16]. When a single key is used for both encryption and decryption, an attacker tries to figure out the secret by using all available keys to encrypt known plaintext and using the same set of keys to decrypt known ciphertext.

After that, the attacker checks the output from both sides in an attempt to find a pair where the decryption and encryption processes "meet in the middle." Finding such a pair exposes the shared key required for the cryptographic procedure. This type of attack works particularly well against algorithms that use keys that are too short or don't have any key strengthening methods.

1.4 Applications of Double DES & AES

There are many potential applications where Double DES and AES algorithm can be useful:

Double DES applications:

- Email encryption: AES has mostly replaced Double DES, a technique once extensively employed for this purpose.
- ATM transactions: To protect financial transactions, some older ATMs continue to use Double DES.
- Smart cards: Data on smart cards, such as identity and payment cards, can be encrypted using double DES.
- Legacy systems: Some legacy systems that are difficult to convert to AES still employ double DES.

Applications of AES:

- Wi-Fi security: Wi-Fi traffic is encrypted using AES to prevent monitoring.
- Virtual private networks (VPNs): To provide safe connection between distant sites, AES is used to encrypt data transferred over VPNs.
- Cloud storage: To prevent unwanted access, data stored in the cloud is encrypted using AES.
- Hard drive encryption: Data on hard drives can be encrypted using AES to prevent loss or theft.
- Data held on mobile devices, such smartphones and tablets, is encrypted using the Advanced Encryption Standard (AES).

1.5 Main objectives of this work

In terms of network security, the main purpose of using cryptographic algorithms such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard) is to ensure the privacy, integrity, and authenticity of the data being transferred across a network. These algorithms are used to protect private communications and data from manipulation. However in the real world, security is not always fully provided. Especially in the case of different social media, in view of that, in our thesis we have been able to complete our work by graphically representing the time according to the different file sizes based on the processor and configuration of the two devices.

Chapter 2

Literature Review

Approaches to compare between Double DES and AES as either Computational time based Approaches or security based. Computational time based techniques often concentrate on obtaining discriminative characteristics directly from the execution time using different configuration computer making any explicit data assumptions. And security based approaches are considered as ensure the better security of the network or data.

2.1. Model-based Approaches:

A model-based approach involves the use of mathematical models to analyze and design cryptographic systems. These models provide a formal framework for understanding the security properties of cryptographic algorithms and protocols[17].

Formal Methods:
Cryptographers often use formal methods to specify and analyze cryptographic algorithms. Formal methods involve mathematical notations and proofs to ensure the correctness and security of cryptographic systems.

Security Models:
Cryptographers define security models to capture the desired security properties of a cryptographic system. Common security models include the indistinguishability model, the semantic security model, and the game-based model.

Proofs of Security:
Model-based approaches often involve providing formal proofs of the security of cryptographic schemes. These proofs demonstrate that the cryptographic system satisfies the security properties specified in the chosen security model.

Protocol Verification:

Model-based approaches are used to verify the security of cryptographic protocols. This involves analyzing the protocol's interactions and ensuring that it achieves its security goals even in the presence of malicious actors.

Computational Complexity:

Model-based approaches often involve analyzing the computational complexity of cryptographic algorithms. This includes assessing the hardness of mathematical problems upon which the security of certain cryptographic schemes relies, such as factoring large numbers or computing discrete logarithms.

Random Oracle Model:

The random oracle model is a common model-based approach used in the analysis of cryptographic protocols. It assumes the existence of an idealized "random oracle" that provides unpredictable and random responses to queries.

2.2. Cryptography Basic Model:

Cryptography involves provoke codes that allow information to be kept secret from the unauthorized user. All the information is kept secure and protected from the third party. For example, if Alice posts some paramount message to Bob, the third person might be read that information without the license of Alice and Bob. So the information might be unsecure. So that cryptography takes the charge to secure the secret. For this cryptography concept is used in many places[13].

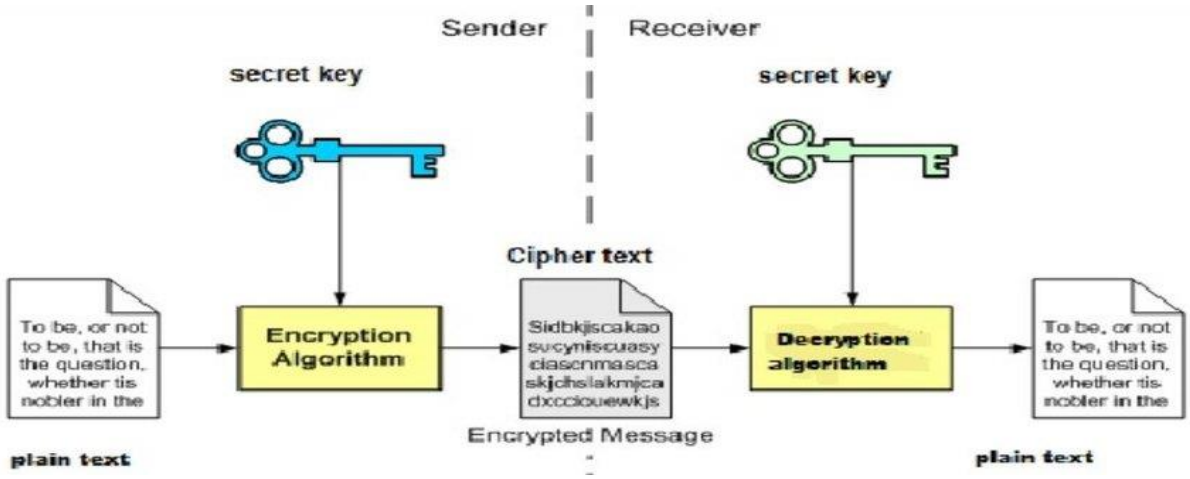

Fig 2.1: Cryptography Basic Function (Model)

2.3. Structure Of Data Encryption Standard (DES):

The Data Encryption Standard (DES) was developed by the National Bureau of Standards (NBS) in 1970s. The connotation of DES is to confer a standard and confident method to protect the vulnerable information and unclassified data.Each 64 bits of data is ingeminatefrom 1 to 16 times (which means 16 rounds). The following illustration is the Data Encryption Standard structure which carries 16 rounds to protect the original text from the unsubscribed user using S-boxes[13].

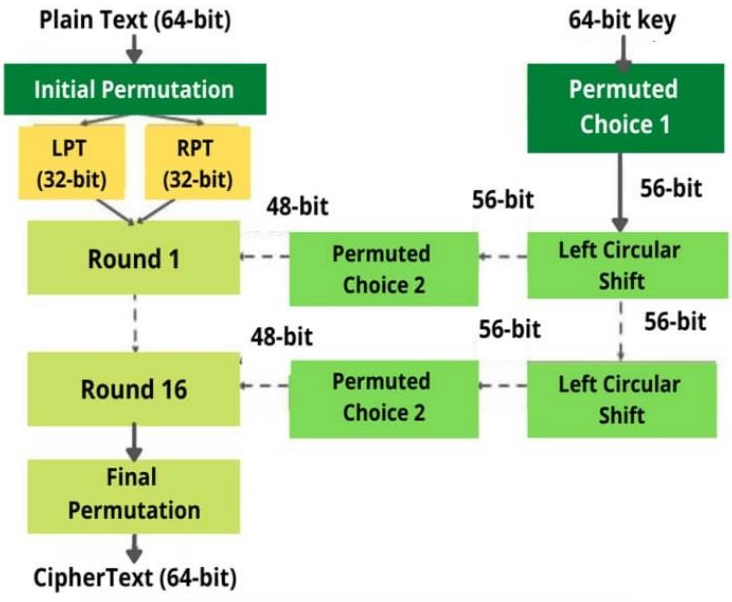

Fig 2.2: Structure of DES

- Solitary / Single Round of DES:

The same procedure is as follows at every round which means every 16 rounds.

Steps:

a) Divide 64-bits into two 32-bit from both sides (left and right).
b) Then the R input is expanding to 48-bits by using Expansion Permutation (E).
c) Expansion Permutation (E) reveals the output in which they perform the XOR operation with key Ki.
d) After the XOR operation,it produces the result which has passed to the S-box which givesas 32-bit output.

e) The Permutation Function (P) permuting the resultant value once again for the clarification.

f) Simultaneously 56-bit key will also be divided into two halves as 28-bits which give the performance using Left Circular Shift and Permutation, after thisit will reduce the size of the key and which spread the result into every round[12].

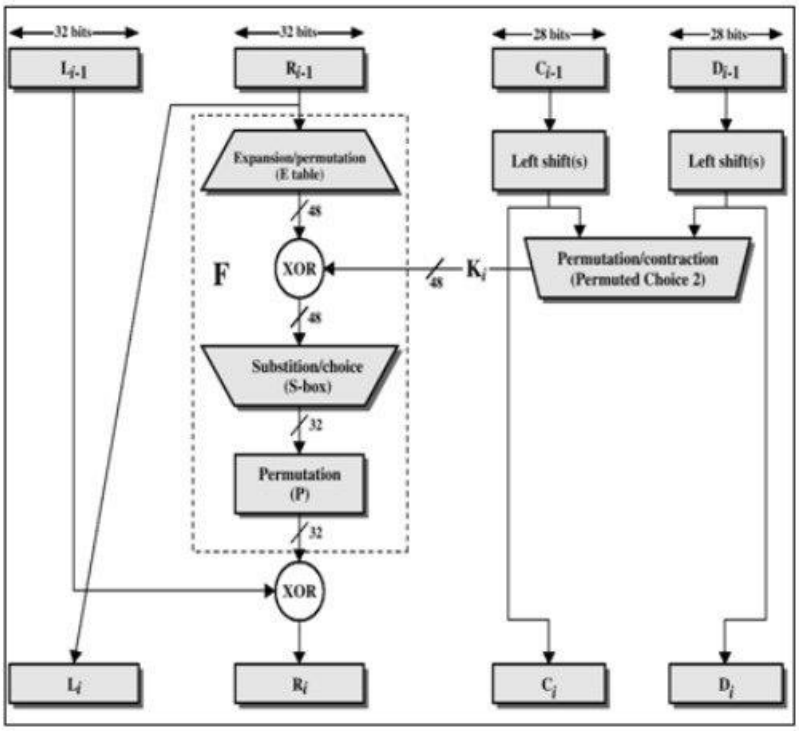

Fig 2.3: Single Round of DES

- Strength of DES:

Some of the important strengths in DES are[12],

a) Data Encryption Standard has a strong avalanche effect.

b) Using this DES, Brute-force attack is not possible.

c) Timing attack is also difficult.

2.4 STRUCTURE OF DATA ENCRYPTION STANDARD (2DES)

Double DES (Data Encryption Standard) or 2DES refers to a cryptographic algorithm that uses the DES encryption algorithm twice in succession to provide an extra layer of security. DES itself is a symmetric key block cipher that operates on fixed-size blocks of data (64 bits) using a key length of 56 bits. However, due to advances in computing power and the discovery of vulnerabilities, DES has become relatively insecure[16].

Mathematically, if the three keys are represented as K1, K2, and K3, and the plaintext is denoted as P, the double DES encryption process can be expressed as:

Ciphertext = E(K3, D(K2, E(K1, Plaintext)))

The encryption process is made of two permutations (P-boxes), which we call initial and final permutations, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm.

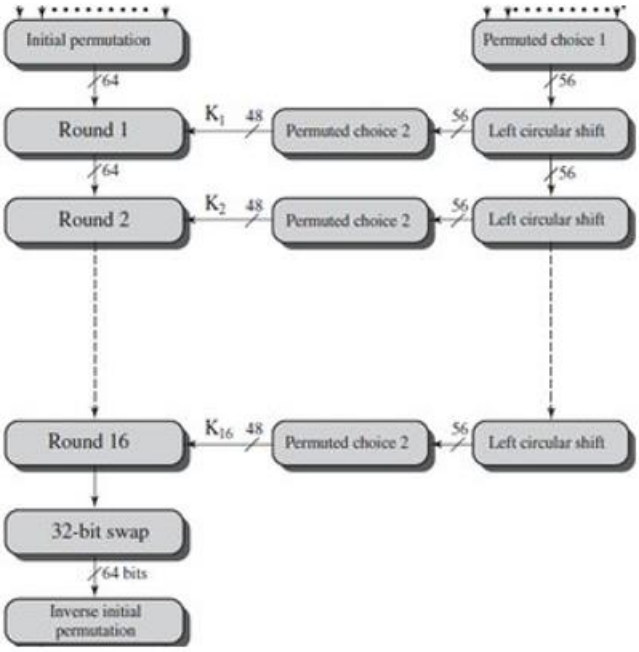

Fig 2.4: Structure of 2DES

- Solitary / Single Round of 2DES

Double-DES (2DES) is a symmetric-key encryption algorithm that uses two rounds of the Data Encryption Standard (DES) algorithm in succession.

Steps:

a.Key Generation:

- Two 56-bit keys, K1 and K2, are generated independently.

b.Initial Permutation (IP):

- The 64-bit plaintext block is subjected to an initial permutation (IP) to rearrange its bits according to a fixed permutation table.

c.Feistel Network:

- The 64-bit block is divided into two 32-bit halves, left (L0) and right (R0).
- The right half (R0) is expanded to 48 bits using an expansion permutation.
- The expanded right half is then XORed with the first 48 bits of the key (K1) to produce a result.
- The result is passed through the S-boxes, where each 6-bit block is substituted with a 4-bit block.
- The output from the S-boxes is then subjected to a permutation (P-box).
- The result of the P-box permutation is XORed with the left half (L0).
- The left half becomes the new right half, and the XOR result becomes the new left half.

d.Swap:

- After the Feistel network, the left and right halves are swapped.

e.Second Round:

- The swapped right half becomes the new left half, and the original right half is subjected to the Feistel network again using a new subkey (K2).
- This process is similar to the first round, with the expanded right half XORed with the second 48 bits of the key (K2).

f.Inverse Initial Permutation (IP^(-1)):

- After the second round, the left and right halves are concatenated, and the result is subjected to the inverse initial permutation (IP^(-1)), which is the reverse of the initial permutation.

g.Output:

- The final 64-bit block is the ciphertext.

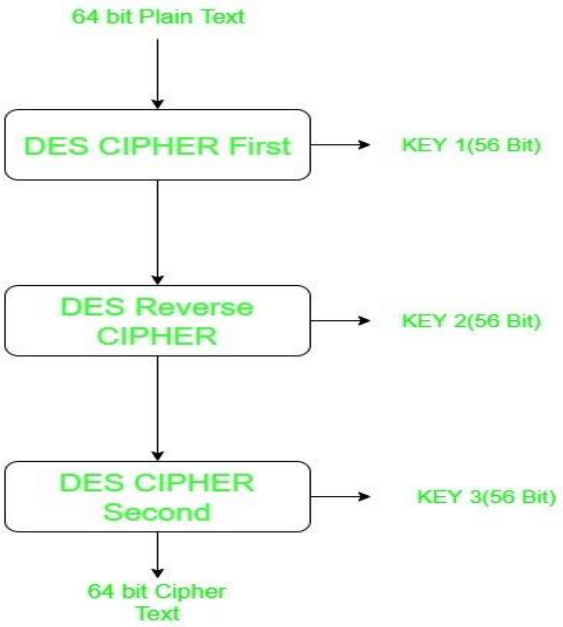

Fig 2.5: Single Round of 2DES

- Strength of 2DES:

Compatibility:

- 2DES is designed as an extension of the original DES algorithm, making it compatible with existing DES implementations.

Familiarity:

- Because it builds upon DES, which was widely used and studied, 2DES was initially considered an incremental step that retained a sense of familiarity.

- Weaknesses:

Meet-in-the-Middle Attack:

- The primary weakness of 2DES is the meet-in-the-middle attack, which significantly reduces its effective key strength. This attack takes advantage of the fact that 2DES encrypts with one key and then decrypts with another key. By precomputing the encryption with all possible keys and the corresponding decryption, an attacker can perform a more efficient search for the correct keys.

Inadequate Key Length:

- Despite using two 56-bit keys, the effective key length of 2DES is not 112 bits due to the meet-in-the-middle attack. Instead, it is effectively reduced to 2^(56+56), resulting in a lower effective key strength than one might expect from using two keys.

Vulnerability to Exhaustive Search:

- The effective security level of 2DES is not sufficient against modern computational capabilities. It is vulnerable to exhaustive search attacks, where an attacker systematically tries all possible key combinations.

Not Recommended for High-Security Applications:

- Due to its weaknesses and the availability of more secure alternatives, 2DES is not recommended for high-security applications. Advanced Encryption Standard (AES) and Triple-DES (3DES) are considered more secure choices.

2.5. OVERVIEW OF ADVANCED ENCRYPTION STANDARD (AES)

[23]AES is a symmetric block cipher also called as private, which uses the same key for the process of encryption and decryption. Advanced Encryption Standard (AES) was suggested by Rijndael. AES will encrypt and decrypt the block size of 128 bits using diverse cipher keys of 128,192, and 256 bits. Generally AES accommodates four alternate transformations such as Sub-Bytes, Shift Rows, Mix-Columns, and Add Round Key. In this paper focuses the concept around the cryptographic function in which how they are officiate in the network area. At first AES will monitor the block and key size of the text, then it will pertain the data into the AES algorithm. Which means it first evaluate the volume to insert the data. Data Encryption Standard (DES) involves six rounds to change from the plain text to cipher text, whereas, Advanced Encryption Standard (AES) involves 10 rounds to change from the plaintext to cipher text. This is the dissimilarity between these two systems. Each round is quite similar to convert the text. AES works under the encryption and decryption manner by the rule of Expand key. For encrypting, the algorithm will work from round 1 to 10. For decrypting, the algorithm will work in a reverse manner[1].Not only encrypted plain text128-bit key is also © 2019 JETIR March 2019, Volume 6, Issue 3 www.jetir.org (ISSN-2349-5162) JETIR1903380 Journal of Emerging Technologies and Innovative Research (JETIR) www.jetir.org 577 constituted as square matrices of bytes. In this section the key is represented as words W0 to W43. Therefore 44 words, each word contains 4-bytes.Finally the key matrix is stored as words (Expanded Key).

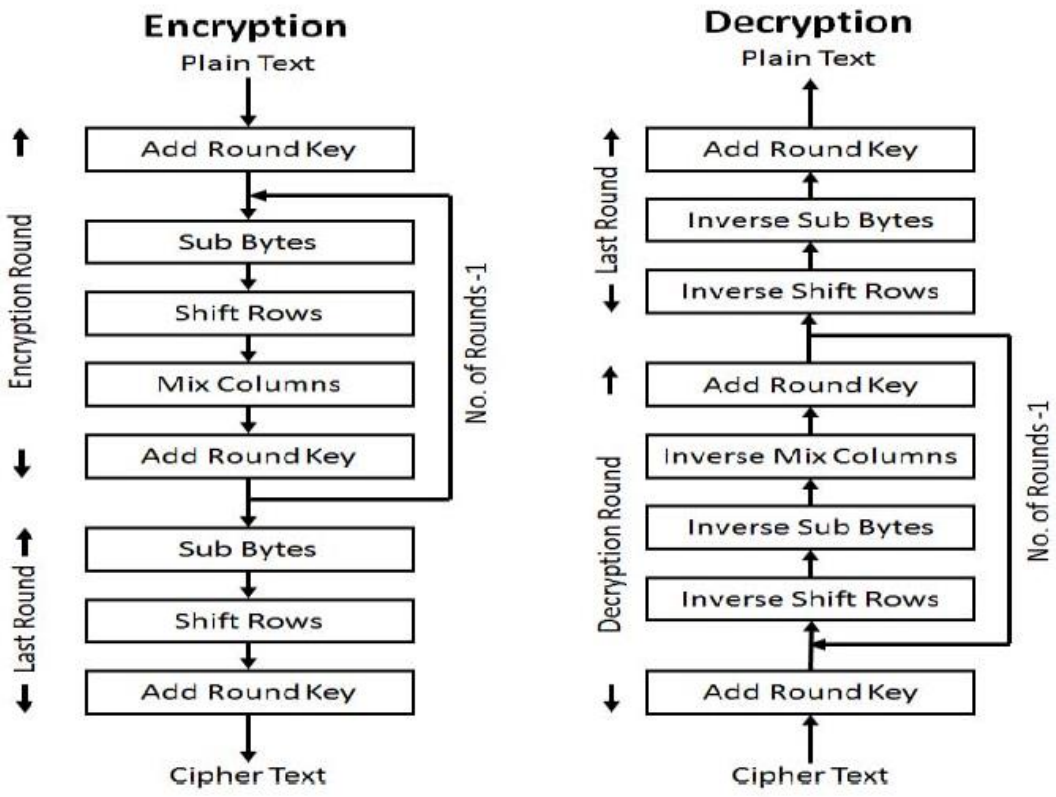

Fig 2.6: Block Diagram for AES Encryption and Decryption

The above figure (4) suppresses few blocks or steps to do the encryption. AES takes 128-bit blocks as an input for encrypting the data or plaintext, which can be represented by square matrix. The particular matrix is copied into state array which perform some modification at each level of encryption. Which means the state array is replicated from an input matrix. After this process, the final result is sent to the out matrix. And also out matrix is a depot to save the output or the result[12].

- Add Round Key:

Add round key performs bitwise XOR operation between the state array and the resulting round key that is the output of the key expansion algorithm.

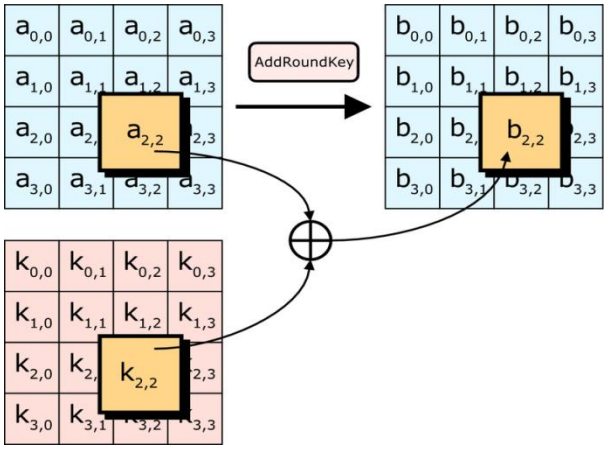

Fig 2.7: AES – Add Round Key

- Substitute Bytes:

Substitute Byte is also called as a Sub Bytes transformation which is one of the transformation technique which is a nonlinear byte substitution and also a simple table lookup technique. The implementation of this transformation is simple. Sub Bytes transformation is an S-Box which consist of 16*16 matrix in which the S-Box is used for both forward and inverse transformation[12].

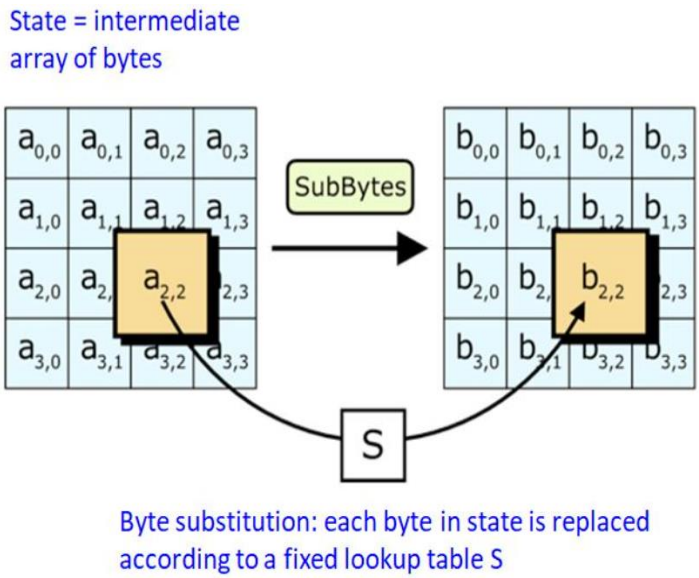

Fig 2.8: AES – Sub Bytes

- AES ADVANTAGES AND DISADVANTAGES

Advantages:

1. When comparing to other method the process of AES has more speed.
2. S-Box is used to abolish the symmetric.
3. Comprehensibility of description.

4. More fastened, so no one cannot hack or attack the personal information[12].

Drawbacks:

1. It uses an excessively potty algebraic structure.
2. Implementing with software is much complicated[12].

2.6. Related Work

There are various research studies that compare between the performance of the common encryption algorithms. This section discusses the results of some of these studies have analyzed and implemented encryption and decryption algorithms DES, 2DES, AES, are symmetric key cryptographic algorithms[5].The study developed an SMS encryption for mobile communication on android message application because of its insecurity during transmission. The study further implemented three of block cipher symmetric cryptography algorithms (i.e. AES algorithm, DES, and 2-DES) and compared three of them in terms of encryption and decryption delay time in order to know the most suitable cryptography algorithm for mobile communication on android message application[3]. In this paper evaluate the performance of the algorithms such as AES, DES to encrypt text files under three parameters like computation time, memory usage, and output bytes. Encryption time was computed to convert plaintext to cipher text then comparing the algorithm to find which algorithm takes more time to encrypt text file[13].

Chapter 3

Methodology

The steps of the methodology proposed In this thesis, including the comparison between Double DES and AES algorithm], and Meet-in-the-middle-attack is graphically illustrated in Figure (4.1) of the study.

3.1 Double DES Encryption and Decryption Method:

Double DES is an encryption approach which uses two example of DES on same plain text. In both examples it provides different keys to encode the plain text. Double DES is easily to learn. Double DES uses two keys, such as k1and k2. It can implement DES on the original plain text using k1 to get the encrypted text. It can implement DES on the encrypted text, but this time with the different key k2. The final output is the encryption of encrypted text as shown in the figure.

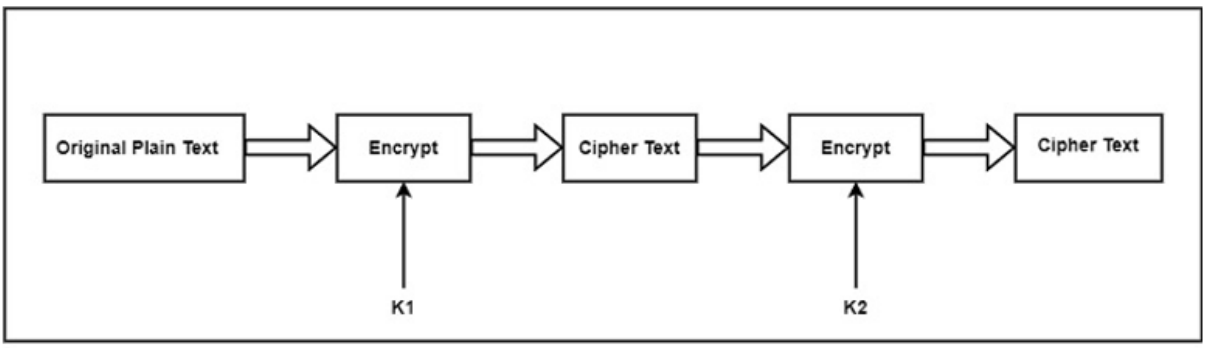

Fig 3.1: Double DES Encryption

The double encrypted cipher-text block is first decrypted using the key K2 to make the singly encrypted cipher text. This ciphertext block is then decrypted using the key K1 to acquire the original plaintext block.

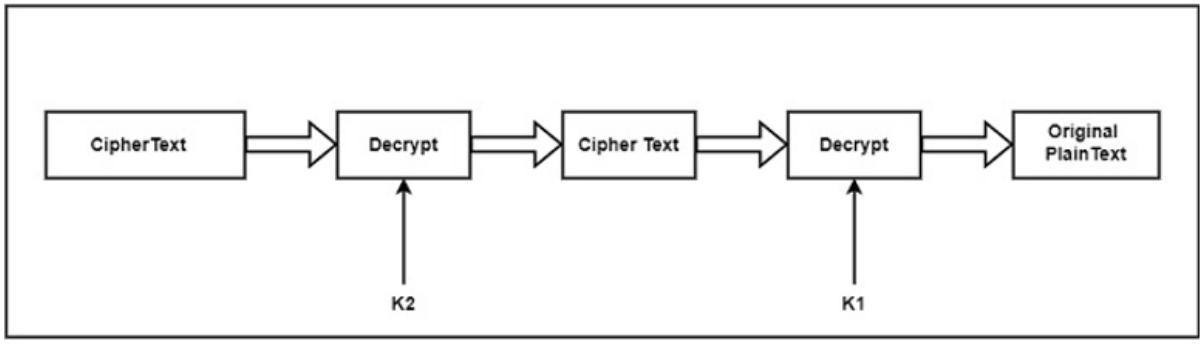

Fig 3.2: Double DES Decryption

If it can use a key of only 1 bit, there are two possible keys including 0 and 1. If it can use a 2 bit key, there are four possible key values such as (00, 01, 10 and 11).

In general, if it can use an n-bit key, the cryptanalyst has to implement 2^n operations to try out all the possible keys. If it can use two different keys, each including n bits, the cryptanalyst would require 2^{2n} attempt to crack the key.

3.1.2 The meet-in-the-middle attack working process:

The meet-in-the-middle attack is a type of cryptanalytic attack commonly used against encryption algorithms that use symmetric keys. Furthermore, the attack takes advantage of the fact that the encryption and decryption processes are inverse operations of each other. Therefore, an attacker follows a brute-force approach to find the secret key we use in the encryption process.

The attack works by dividing the key space into two parts. First, it encrypts the plaintext using all possible keys from one-half of the key space. Additionally, an attacker decrypts the resulting ciphertext using all possible keys from the other half of the key space. Finally, the attacker checks for a match between intermediate values obtained from the encryption and decryption steps.

If a match is found, the key used in the encryption and decryption is in the middle of the key space. By repeating the process with smaller key spaces on either side of the matched key, the attacker can eventually find the secret key used in the encryption. The meet-in-the-middle attack is particularly effective against encryption algorithms with a relatively small key space and vulnerable to exhaustive key search.

Using a known-plaintext attack called meet-in-the-middle attack

assume two adjacent block ciphers (e.g. double DES)

C = EK2(EK1 (p))

But

X= EK1(p) = DK2 (C)

so given a known pair, [p, C]encrypt p with 256 keys & decrypt C with 256 keys

compare to find match; double check

if OK, then you have the two keys

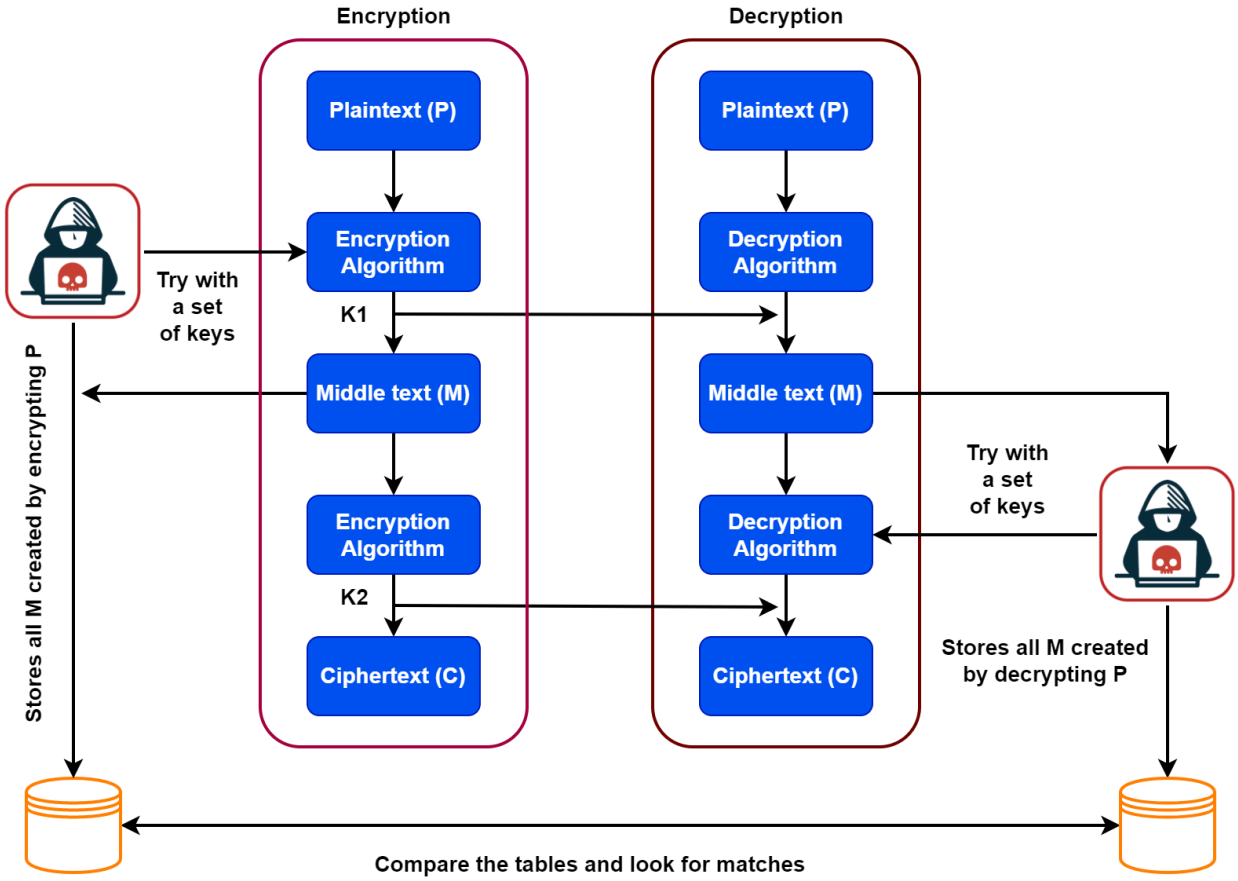

Fig 3.3: Process of Meet-in-the-middle-attack

An attacker typically follows five steps in order to implement or launch the meet-in-the-middle attack:

3.1.3 AES Encryption and Decryption Method:

Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −

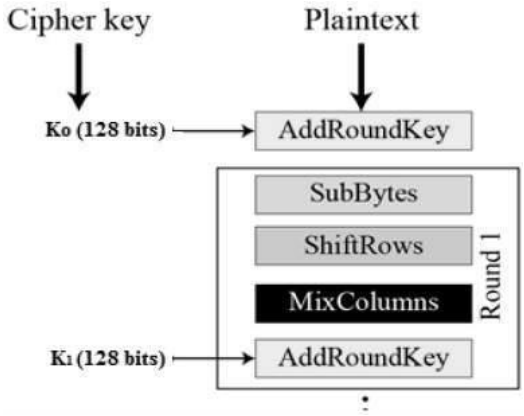

Fig 3.4: AES Encryption Process

Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shiftrows.

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns:

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey:

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

3.2 Security Assessment:

Table: 3.1 Comparison Between DES ,2DES and AES

FACTORS	DES	Double DES	AES
Key Length	56 bits	112bits	128,192 or 256 bits
Block Size	64 bits	64 bits	128,192 or 256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Developed	1977	1977	2000
Security	Proven inadequate	Proven inadequate	Considered secure
Cryptanalysis Resistance	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Strong against differential, truncated differential, linear, interpolation and square attacks
Usage in Modern Applications	Obsolete; replaced by AES	Not recommended due to security weaknesses	Widely adopted; standard encryption algorithm for modern applications
Possible Keys	2^56	2^112	2^128, 2^192 and 2^256

In summary, AES is considered a more secure and modern encryption algorithm compared to Double DES. It offers better key strength, resistance to attacks, and is suitable for a wide range of applications. Double DES, on the other hand, is considered obsolete due to its vulnerability to meet-in-the-middle attacks and the availability of stronger encryption alternatives like AES.

3.3 Performance Evaluation:

a) AES, DES Analyzing time based on different file size using Known Plaintext on machine1(Intel Dual core 1.8Ghz Processor with 4 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 1.8Ghz Processor with 4 GB RAM configuration.

The result that was obtained is shown below in the graph.

File Size	DES(Time In second)	Double DES (Time in Sec)	AES (Time in Sec)
94Kb	0	0	1
104Kb	0	0	1
115.5Kb	0	0	1
124.2kb	1	0	1
136Kb	1	0	2

Table 3.2:Analyzing time based on known plaintext

Graph:

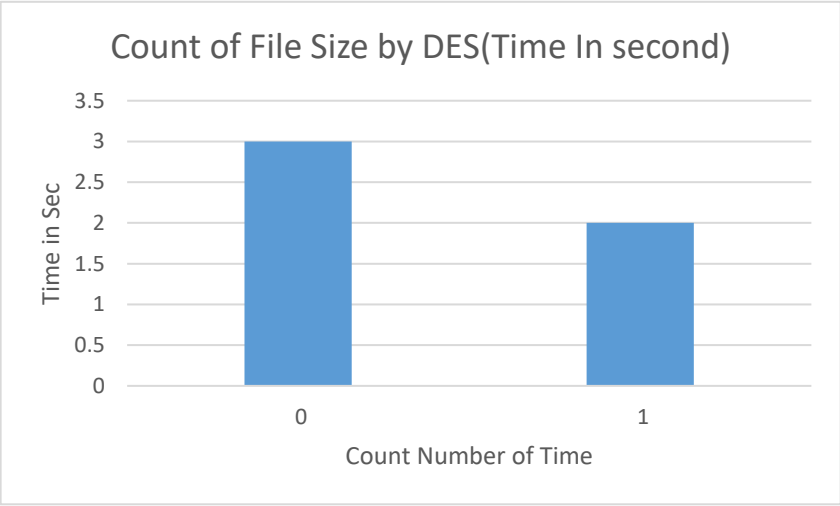

Fig 3.5: Count of file size by DES

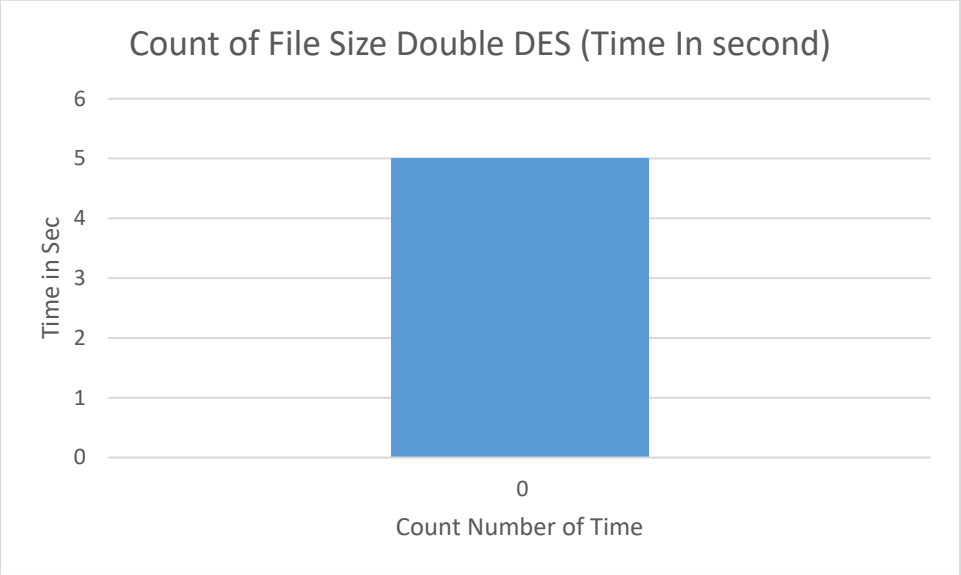

Fig 3.6: Count of file size by Double DES

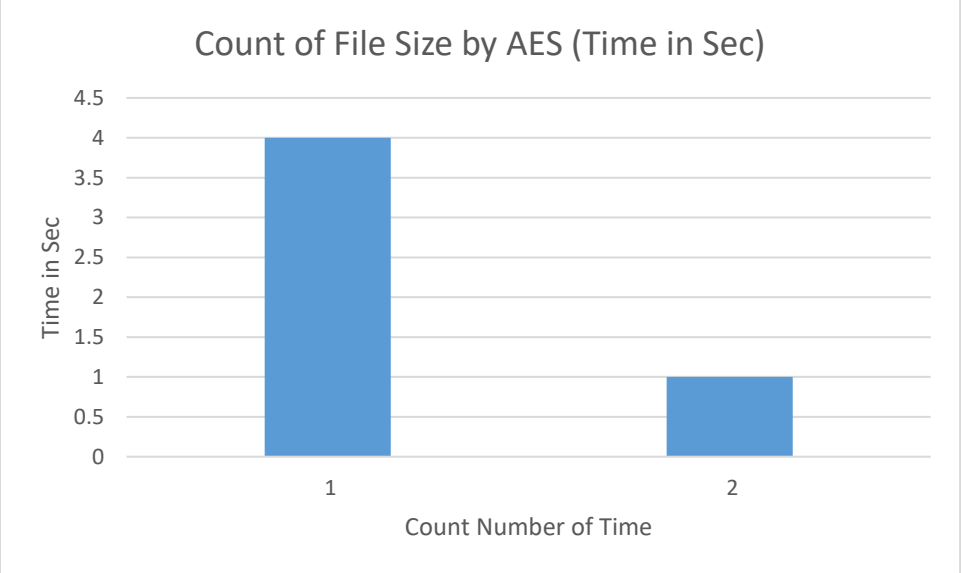

Fig 3.7: Count of file size by AES

b) AES ,Des and 2DES Analyzing time based on different file size using Known Plaintext on machine2(Intel core i5 processor with 8 GB RAM)
This graph has shown the time being utilized by AES, DES and 2DES security algorithms on a machine2 using known plaintext. With the help of graph and table the comparison of AES, DES and 2DES security algorithms is shown.

File Size	DES(Time In second)	Double DES (Time in Min)	AES (Time in Sec)
94Kb	0	0	0
93.5Kb	0	0	3
93.8Kb	0	0	3
94.2kb	0	0	0
99.4Kb	0	0	0

Table 3.3:Analyzing time based on known plaintext

Graph:

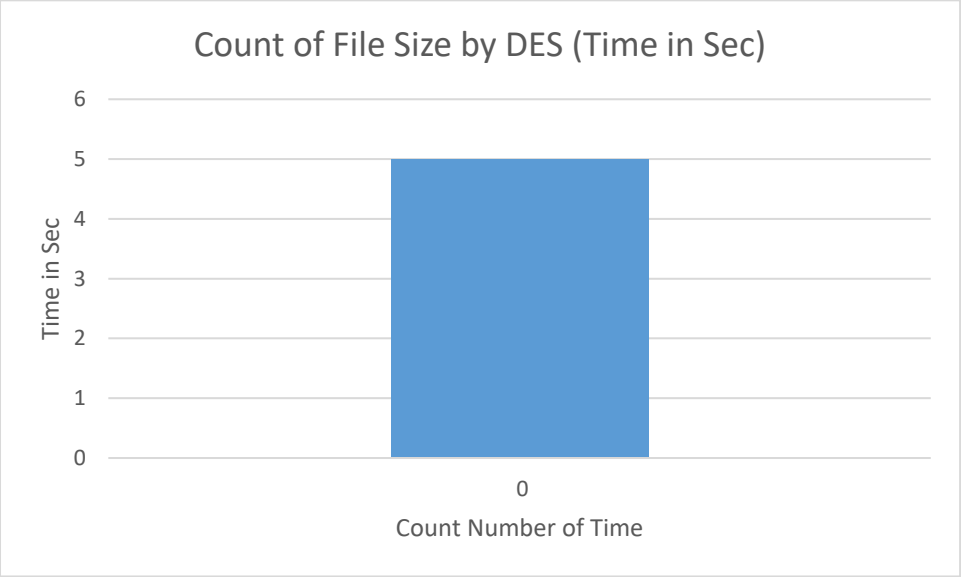

Fig 3.8: Count of file size by DES for Computer 2

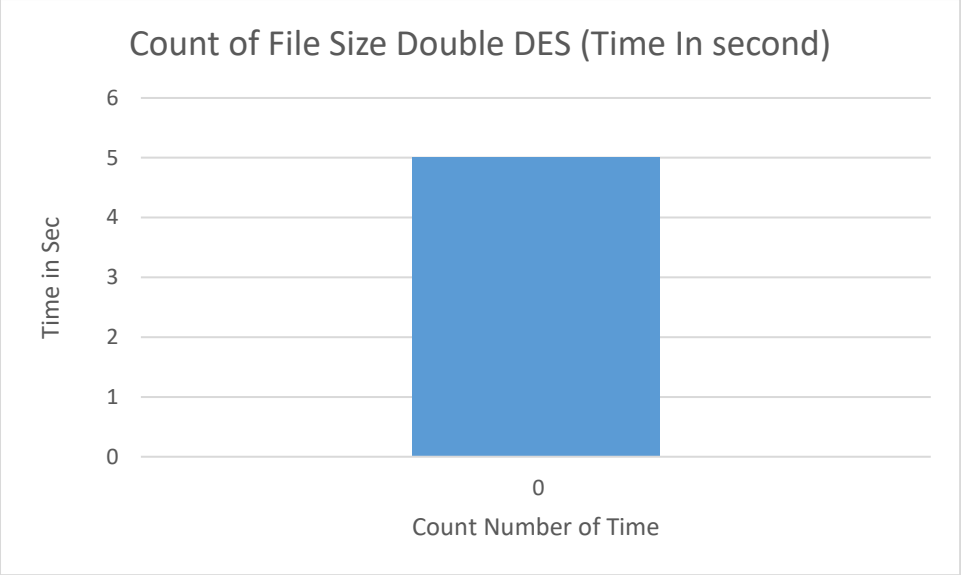

Fig 3.9: Count of file size by Double DES for Computer 2

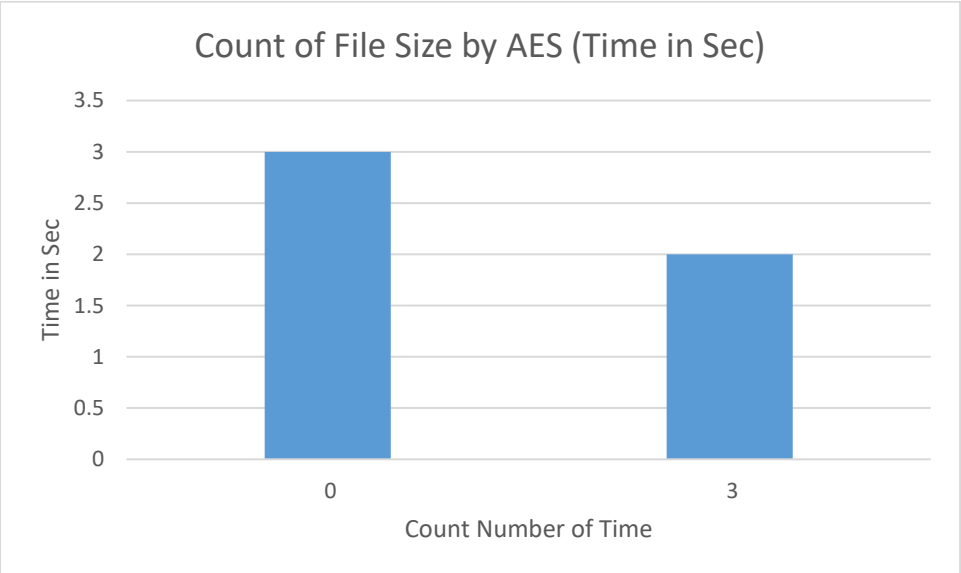

Fig 3.10: Count of file size by AES for Computer 2

The DES algorithm takes 0–1 seconds to process files of different sizes, as Figure (3.5) illustrates. Figure (3.6) illustrates that Double DES takes only 0 seconds to run, but Figure (3.7) demonstrates that AES, takes 1-2 seconds longer than the other algorithm and is executed by computer1's 4GB of RAM.

The DES method takes 0 seconds to process files of different sizes, as Figure (3.8) illustrates. Figure (3.10) shows that AES takes more time (0-3) seconds to perform than the other method, however figure (3.9) shows that Double DES takes just 0 seconds to process and is executed by computer2's 8GB of RAM.

Chapter 4

Results and Discussion

4.1 Environment Setup

Hardware requirements for this test include an i5 processor, 4 and 8 GB of RAM, and a 2 GB Nvidia graphics card. For classification, javax.crypto.Cipher,javax.crypto.KeyGenerator, library were used. For 2DES and AES comparison, a number of java libraries were also used. These library algorithms were performed with NetBeans code editor and we use java language for implement this algorithms.

4.2 Experimental Result of Comparison among DES, 2DES and AES Algorithm

DES (Data Encryption Standard):

Key Length: 56 bits.

Security Concerns: DES is considered insecure against modern cryptographic attacks due to its small key size. Brute-force attacks and other more sophisticated techniques can break DES encryption.

Usage: DES was widely used in the past but is now considered obsolete for secure applications.

Security: It provides inadequate security.

2DES (Double DES):

Key Length: 112 bits (two 56-bit keys used consecutively).

Security Concerns: 2DES provides only a limited increase in security over DES because it is vulnerable to a meet-in-the-middle attack. This vulnerability makes it less secure than the increase in key size might suggest.

Usage: Due to its security weaknesses, 2DES is not recommended for secure cryptographic applications.

Security: It also provides inadequate security.

AES (Advanced Encryption Standard):
Key Length: AES supports key lengths of 128, 192, or 256 bits.
Security: AES is widely considered secure and is used in a variety of applications, including securing sensitive data, communications, and more. Its security is based on the choice of a strong key and the underlying structure of the algorithm.
Usage: AES is the standard encryption algorithm used in many modern applications and systems. It has replaced DES and 3DES in most scenarios.

Security: It provides Higher level of security.

4.3 Experimental Result of DES,2DES and AES

In this thesis, we compare the execution time of the DES, Double DES and AES algorithm. We execute this algorithm into two different computer. And this two computer have different kind of configuration. Computer1 has a 4GB of RAM with intel core i5 8^{th} generation processor . And the Computer2 has a 8GB of RAM with intel core i5 10^{th} generation processor.

Computer1 of 4GB RAM:

	DES(Time In second)	Double DES (Time in Sec)	AES (Time in Sec)
94Kb	0	0	1
104Kb	0	0	1
115.5Kb	0	0	1
124.2kb	1	0	1
136Kb	1	0	2

Table4.2: Output of the Machine1 4GB of RAM

In table (5.3.1), demonstrates that DES algorithm need time from 0-1 second for executing different size of file. Where Double DES need only 0 second for execution and AES needs more time (1-2)second than the other algorithm.

Computer2 of 8GB RAM:

File Size	DES(Time In second)	Double DES (Time in Min)	AES (Time in Sec)
94Kb	0	0	0
93.5Kb	0	0	3
93.8Kb	0	0	3
94.2kb	0	0	0
99.4Kb	0	0	0

Table4.3: Output of the Machine2 8GB of RAM

In table (5.3.2), demonstrates that DES algorithm need time from 0 second for executing different size of file. Where Double DES need only 0 second for execution and AES needs more time (0-3)second than the other algorithm.

So we can see that the AES algorithm needs more time for executing the program than the DES and 2DES algorithm. But AES provide the better security than rest of the other algorithm.

Chapter 5

Conclusions and Future Work

5.1 Conclusions

Based on the research above, it can be said that security is a major concern right now. Several approaches are offered for security-related purposes. We refer to this system as cryptography. We employ two types of keys in cryptography: public and private. These keys enable us to encrypt and decrypt data in order to make it secure. The term "ciphertext" refers to encrypted data, while "decrypted data" is termed plaintext. There are two varieties of cryptography: symmetric and asymmetric. This study compares the AES and Double DES symmetric key security methods. Algorithms with symmetric keys use the same key for both encryption and decryption. The work mentioned above also demonstrates how well both algorithms perform. It is shown that at different machines, both algorithms need varying amounts of time. The same algorithm performed on different devices using the same data packet takes varying times. It is evident from the discussion above that every algorithm has a different speed. AES cannot be broken by using this attacking technique, even though meet in the middle attacks can break Double DES.
Especially compared to Double DES, AES is more secure.

5.2 Future Work

In the future, this thesis will involve further work with more variations in occlusion conditions for occlusion reduction. Some possible directions for future research include:

1. Post-Quantum Cryptography: Both DES and AES are vulnerable to potential threats from quantum computers. Research on quantum-resistant cryptography algorithms needs continued pursuit to ensure long-term data security.
2. Blockchain integration: Investigating the use of encryption algorithms within blockchain technology for secure data storage, transactions, and smart contracts.
3. Key Management: Secure key generation, storage, and distribution remain critical challenges in cloud security. Exploring decentralized and hardware-based solutions for key management can enhance security and reduce reliance on vulnerable central servers. Additionally, advancements in quantum-resistant key exchange protocols will be crucial for post-quantum security.

References

[1] Bawna Bhat, Abdul Wahid Ali and Apurva Gupta, "DES and AES performance evaluation", *Proceedings of IEEE International Computing Communication & Automation (ICCCA) Conference*, pp. 887-890, 2015.

[2] Aamer Nadeem and M. Younus Javed, "A performance comparison of data encryption algorithms", *Proceedings of IEEE First international In Information and communication technologies conference*, pp. 84-89, 2005.

[3] K.B. Logunleko1, O.D. Adeniji , A.M. Logunleko," A Comparative Study of Symmetric Cryptography Mechanism on DES, AES and EB64 for Information Security" International Journal of Scientific Research in Computer Science and Engineering, Vol.8, Issue.1, pp.45-51, February (2020).

[4] Mahmoud Alfadel, El-Sayed M. El-Alfy and Khaleque Md Aashiq Kamal, "Evaluating time and throughput at different modes of operation in AES algorithm", *Proceedings of IEEE 8th International Information Technology (ICIT) Conference*, pp. 795-801, 2017.

[5] Shaza D. Rihan, Ahmed Khalid, Saife Eldin F. Osman," A Performance Comparison of Encryption Algorithms AES and DES" International Journal of Engineering Research & Technology (IJERT), Vol. 4 Issue 12, December-2015.

[6] Buchmann Johannes, Introduction to cryptography, Springer Science & Business Media, 2013.

[7] M. Kannan, D. C. Priya and S. VaishnaviSree, *A COMPARATIVE ANALYSIS OF DES AES AND RSA CRYPT ALGORITHMS FOR NETWORK SECURITY IN CLOUD COMPUTING*, vol. 6, no. 3, pp. 10, 2019.

[8] C. Paar and J. Pelzl, "The Advanced Encryption Standard (AES)" in Understanding Cryptography, Berlin, Heidelberg:Springer, 2010.

[9] 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.

[10] P. Karthigaikumar and Soumiya Rasheed, "Simulation of Image Encryption using AES Algorithm", *IJCA Special Issue on "Computational Science-New Dimensions & Perspectives" NCCSE 2011*.

[11] Nirmaljeet Kaur, Sukhman Sodhi, Data Encryption Standard Algorithm (DES) for Secure Data Transmission, International Conference on Advances in Emerging Technology, 2016.

[12] M.Kannan , Dr.C.Priya , S.VaishnaviSree" A COMPARATIVE ANALYSIS OF DES, AES AND RSA CRYPT ALGORITHMS FOR NETWORK SECURITY IN CLOUD COMPUTING" Journal of Emerging Technologies and Innovative Research (JETIR), 2019 JETIR March 2019, Volume 6, Issue 3.

[13] Ako Muhamad Abdullah," Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data" Department of Applied Mathematics & Computer Science Eastern Mediterranean University – Cyprus, June 16, 2017.

[14] Akash Kumar Mandal; Chandra Parakash; Archana Tiwari," Performance evaluation of cryptographic algorithms: DES and AES" 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science.

[15] Jawahar Thakur , Nagesh Kumar," DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" International Journal of Emerging Technology and Advanced Engineering ,(ISSN 2250-2459, Volume 1, Issue 2, December 2011).

[16] Sandy Tri Kurnia; Yeni Farida; Santi Indarjani ; "Comparison of Meet-in-the-middle Attacks on 2-DES and 2-AES with Four Scenarios" 2023 IEEE International Conference on Cryptography, Informatics 2023•ieeexplore.ieee.org

[17] J Botella, F Bouquet, JF Capuron ;Model-based testing of cryptographic components--lessons learned from experience- 2013 IEEE Sixth 2013 - ieeexplore.ieee.org