International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 11, November 2014

# Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System

**Karthik .S[1], Muruganandam .A[2]**

[1]Research Scholar, Periyar University, Salem, Tamilnadu, India
[2]Research Scholar, Bharathiar University, Coimbatore, Tamilnadu, India

**Abstract:** ***This paper contains a technique for secret communication using cryptography. It is a technique which is used to protect the important data. The secret message is encrypted by a block cipher based on two cryptographic algorithms, the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA) which may be used by Federal organizations to protect sensitive data. This algorithm uniquely defines the mathematical steps required to transform data into a cryptographic cipher and also to transforms the cipher back to the original form with block length of 128 bits and key length of 256 bits. This paper provides a performance comparison between the most common encryption algorithms: DES, 3DES, AES and Blowfish.***

**Keywords:** DES, Triple DES, AES, Cryptography

## 1. Introduction

Data Encryption Standard (DES) is the block cipher which takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. It is a symmetric encryption technique which means both sender and receiver use a shared key to encrypt and/or decrypt the data as shown in the below Figure 1.1: The problem of this technique is that if the key is known to others the entire conversation is compromised. The 3DES block size is 64 bits and also uses a key to customize the transformation, so that decryption can only be performed by those who know the particular key used to encrypt. The key basically consists of 64 bits however, only 56-bits of these are actually used by the algorithm. Eight bits are used solely for checking parity, and thereafter discarded. Hence the "*effective key length is 56-bits*" and it is always quoted. Every 8th bit of the selected key is discarded i.e., positions 8, 16, 24, 32, 40, 48, 56, 64 are removed from the 64-bit key leaving behind only the 56-bit key.

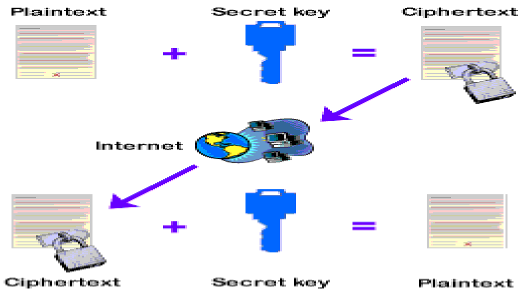


**Figure 1.1:** Conversion of Secret key

### 1.1 History of DES

DES algorithm used for encryption of the electronic data. It was developed in the early 1970s at IBM and based on an earlier design by *Horst Feistel*, the algorithm submitted to the National Bureau of Standards (NBS) to propose a candidate for the protection of sensitive unclassified electronic government data. It is now taken as unsecured cause of its small size and a brute force attack is possible in it. In January 1999 distributed .net and the Electronic Frontier Foundation (EFF) collaborated to publicly break a DES key in 22 hours and 15 minutes. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES).

### 1.2 Cryptography

Cryptography means data secure, it helps to ensure data privacy, maintain data integrity, authenticate communicating parties, and prevent repudiation.

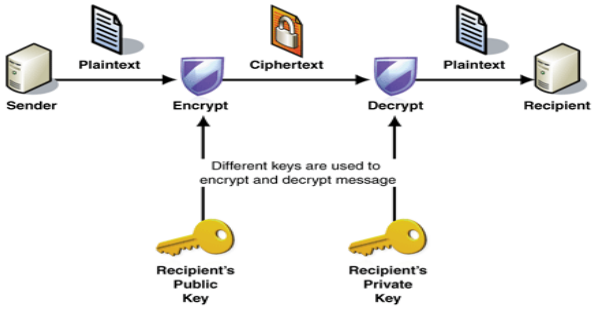


**Figure 1.2:** Key schedules for Encryption and Decryption

The above Figure 1.2: as shown in key schedule for encryption and decryption algorithm which generates the sub keys. Initially, 56 bits of the key are selected from the initial 64 by Permuted Choice 1 (PC-1) and the remaining eight bits are either discarded or used as parity check bits. The 56 bits are divided into two 28 bit halves; each half is treated separately. In successive rounds, both halves are rotated left by one and two bits (specified for each round), and then 48 sub key bits are selected by Permuted Choice 2 (PC-2) i.e. 24 bits from the left half and 24 from the right. The rotations (denoted by "<<<") mean that a different set of bits is used in each sub key, each bit is used in approximately 14 out of the 16 sub keys.

### 1.2.1 Cryptography Goals

This section explains the five main goals behind using Cryptography. Every security system must provide a bundle of security functions that can assure the secrecy of the system.

These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories:

- **Authentication:** Authentication means before sending and receiving data using the system, the receiver and sender identity should be verified.
- **Secrecy or Confidentiality:** In this function is how most people identify a secure system. It means only the authenticated people are able to interpret the message or content and no one else.
- **Integrity:** Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets.
- **Non-Repudiation:** In this function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.
- **Service Reliability and Availability:** Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users.

### 1.2.2 Advantages

i. DES has been around a long time (since 1977), even no real weaknesses have been found: the most efficient attack is still brute force.
ii. DES is an official United States Government standard; the Government is required to re-certify, DES every five years and ask it be replaced if necessary. DES has been re-certified in 1983, 1987, and 1992.
iii. DES is also an ANSI and ISO standard. Since DES was designed to run on 1977 hardware, it is fast in hardware and relatively fast in software.

### 1.2.3 Disadvantages

i. The 56 bit key size is the biggest defect of DES and the chips to perform one million of DES encrypt or decrypt operations a second are available (in 1993).
ii. Hardware implementations of DES are very fast.
iii. DES was not designed for software and hence runs relatively slowly.
iv. In a new technology it is improving a lot of possibility to break the encrypted code, so AES is preferred than DES.

### 1.2.4 Objectives

i. Provide functionality to store a file in an encrypted format which can only be accessed by providing the correct password.
ii. Modify the system to make the directories password protected.
iii. To review a short history of DES and define the basic structures.
iv. To describe the building block elements of DES
v. To describe the round keys generation process and to analyze data encryption standard.

### 1.2.5 Motivation

**(a) Security**
Secures data from being accessed by any malicious user.

**(b) Privacy**
Ensure that private data is not accessed by other users.

**(c) Reliability**
Only responsible users are provided to access these data.

(**d) Resource sharing**
Many users can use the same system and still can work independently

### 1.3 AES (Advanced Encryption Standard)

AES is a new cryptographic algorithm that can be used to protect electronic data. Specifically, AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes). A Public-key ciphers, can use a pair of keys, symmetric key ciphers use the same key to encrypt and decrypt data. The new AES will certainly become the de facto standard for encrypting all forms of electronic information, replacing DES. AES-encrypted data is unbreakable in the sense that known cryptanalysis attack can decrypt the AES cipher text without using a brute-force search through all possible 256 bit keys. Security is no longer an afterthought in anyone's software design and development process. It will greatly increase the reliability and safety of your software systems. DES is a block cipher, as shown in below Figure 1.3.

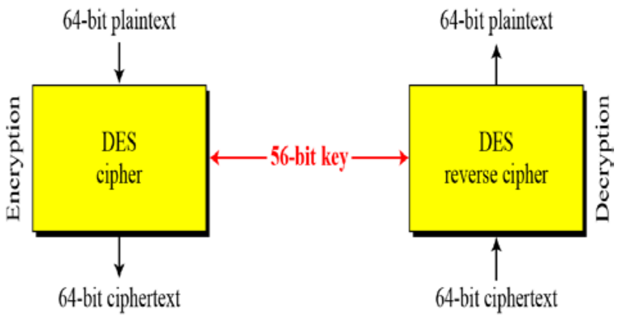


**Figure 1.3:** Encryption and decryption with DES

## 2. Overview of Encryption and Decryption

Encryption is a process of coding information which could either be a file or mail message into cipher text a form unreadable without a decoding key in order to prevent anyone except the intended recipient from reading that data. Decryption is the reverse process of converting encoded data to its original un-encoded form, plaintext. A key in cryptography is a long sequence of bits used by encryption / decryption algorithms. The following example to represents a hypothetical 40-bit key:

**10101001 10011110 00011100 01010101**

### 2.1 Types of Encryption

Depending on the type of encryption, information can be displayed as various numbers, letters, or symbols. Those who work in cryptography fields make it their job, to encrypt information or to break codes to receive encrypted information.

### 2.1.1 Manual Encryption

Manual encryption is a type that involves the use of encryption software. These are computer programs that encrypt various bits of information digitally. Manual encryption involves the user's participation completely. The files wants to encrypt are chosen, and then an encryption type is chosen from a list that the security system provides.

### 2.1.2 Transparent Encryption

Transparent encryption is another type of computer software encryption. It can be downloaded onto a computer to encrypt everything automatically. One of the most important secure types of encryption available because it doesn't leave anything that might be forgotten when using manual encryption. Every executable application and file created in the computer has an encrypted copy that can withstand power surges and protects information in case a computer is stolen.

### 2.1.3 Symmetric Encryption

All encryption is done via a computer software program. You can easily encrypt information by yourself. One of the simplest ways to do this is through symmetric encryption. Here, a letter or number coincides with another letter or number in the encryption code. You can take any written text and substitute letters and numbers for their coded counterpart, thus encrypting the text.

### 2.1.4 Asymmetric Encryption

Asymmetric encryption is a secure and easy way that can be used to encrypt data that you will be receiving. It is generally done electronically. A public key is given out to whomever you want or posted somewhere for the public to see. They can encrypt information using the key and send it to you. This is often done when writing emails. This means encrypt the data with the public key, it can only be read again by whomever the private key has.

### 2.2 Types of Decryption

### 2.2.1 Symmetric Decryption

In symmetric encryption, the same mathematical equation both encrypts and decrypts the data. The following example, a simple letter substitution cipher, such as A=B, B=C, etc., is symmetrical because you simply reverse the process to decrypt the message. If you send a message using a symmetric encryption method, the recipients must also have the key to decrypt the document.

### 2.2.2 Asymmetric Decryption

Asymmetric decryption methods, also known as public-key decryption, use a system involving a pair of linked keys. In this system, anything encoded with one key requires the other key to decrypt, and so on. When you encode a message using someone's public key, you know that only a recipient possessing the corresponding private key can read it.

### 2.2.3 Hashing

Hashing is a form of encryption that uses a specialized one-way encryption key. If you hash a given volume of data, it will produce a unique output string to that data, but it is impossible to reconstruct the data from the output string. You can re-encode the original data and compare it to the result string to verify it. This can serve as a type of error correction in encoding. Hashing a message and providing that value to your correspondents ensures that they can hash the message themselves and compare the values. As long as the two output strings match, recipients know the message is complete and unaltered.

## 3. Cryptographic

### 3.1 Symmetric Key Cryptography

The DES most widely used symmetric key cryptographic method is the Data Encryption Standard (DES) as shown in below Figure 3.1: It uses a fixed length, 56-bit key and an efficient algorithm to quickly encrypt and decrypt messages. It can be easily implemented in the encryption and decryption process even faster. In general, increasing the key size makes the system more secure. A variation of DES, called Triple-DES or DES - EDE (Encrypt-Decrypt-Encrypt), uses three applications of DES and two independent DES keys to produce an effective key length of 168 bits.

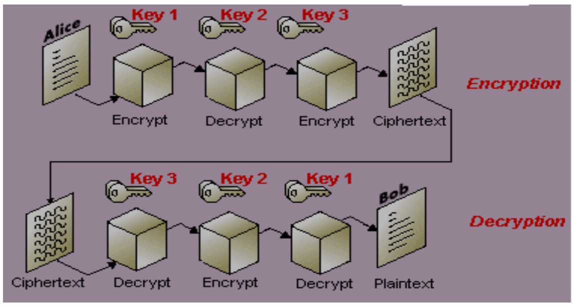


**Figure 3.1**: Symmetric Key – Triple DES

Despite the efficiency of symmetric key cryptography, it has a fundamental weak spot-key The International Data Encryption Algorithm (IDEA) was invented by James Massey 1991. IDEA uses a fixed length, 128-bit key (larger than DES but smaller than Triple-DES). It is also faster than Triple-DES. In the early 1990s, Don Rivest of RSA Data Security, Inc., invented the algorithms RC2 and RC4. These use variable length keys and are claimed to be even faster than IDEA.

### 3.2 Implementation of Triple DES (3DES)

In 1998 a standard ANS X9.52 and named Triple Data Encryption Algorithm (TDEA).

a. Block cipher with symmetric secret key
b. Block length = 64 bits
c. Key length = 56, 112 or 168 bits

3DES was created because DES algorithm, invented in the early 1970s using 56-bit key. The effective security 3DES provides is only 112 bits due to meet-in-the-middle attacks. Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. In DES, data is encrypted and decrypted in 64 -bit chunks. The input key for DES is 64 bits long; the actual key used by DES is only 56 bits in length.

The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

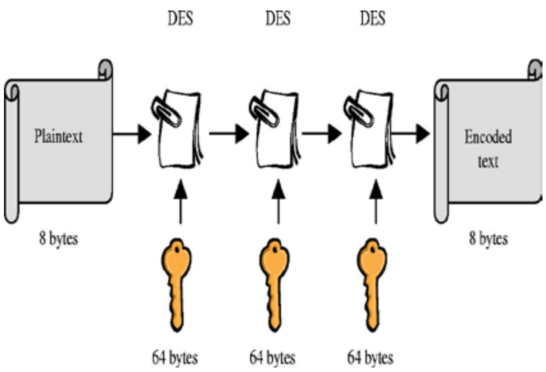


**Figure 3.2:** Triple DES Using 64 bytes

The above Figure 3.2 as shown in Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three keying options in data encryption standards:

a. All keys being independent
b. Key 1 and key 2 being independent keys
c. All three keys being identical

Key option 3 as shown in Figure 3.3: triples DES. The triple DES key length contains 168 bits but the key security falls to 112 bits.

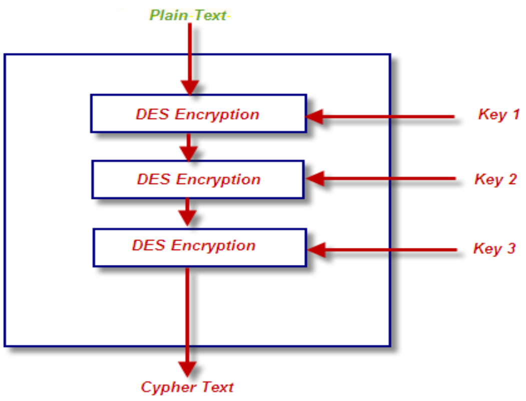


**Figure 3.3:** Working of Triple DES

**(i) Algorithm:**
Run DES three times:

ECB mode:
If $K_2 = K_3$, this is DES
Backwards compatibility
Known not to be just DES with $K_4$
Has 112 bits of security, not 3 56 = 168

Triple DES algorithm uses three iterations of common DES cipher. It receives a secret 168-bit key, which is divided into three 56-bit keys.

- Encryption using the first secret key
- Decryption using the second secret key
- Encryption using the third secret key

**Encryption:**
c = E3 (D2 (E1 (m)))

**Decryption:**
m = D1 (E2 (D3(c)))

Using decryption in the second step during encryption provides backward compatibility with common DES algorithm. In these case first and second secret keys or second and third secret keys are the same whichever key.

c = E3 (D1 (E1 (m))) = E3 (m)
c = E3 (D3 (E1 (m))) = E1 (m)

It is possible to use 3DES cipher with a secret 112-bit key. In this case first and third secret keys are the same.

$c = E_1 (D_2 (E_1 (m)))$

Triple DES is advantageous because it has a significantly sized key length, which is longer than most key lengths affiliated with other encryption modes. DES algorithm was replaced by the Advanced Encryption Standard and Triple DES is now considered to be obsolete. It derives from single DES but the technique is used in triplicate and involves three sub keys and key padding when necessary. Keys must be increased to 64 bits in length Known for its compatibility and flexibility can easily be converted for Triple DES inclusion. The following Figure 3.4 and Figure 3.5 is the block diagram of 3DES as shown in below.

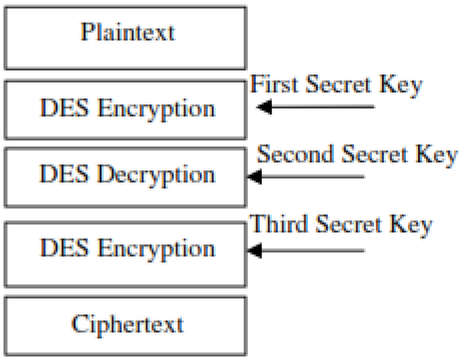


**Figure 3.4:** Block Diagrams: 3DES Encryption

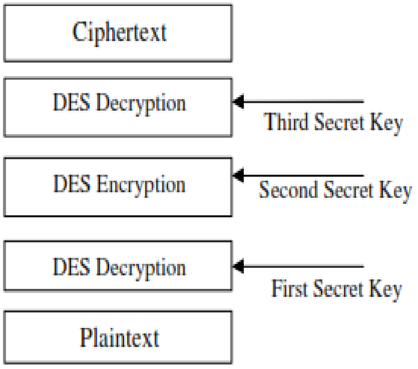


**Figure 3.5:** Block Diagrams: 3DES Decryption

## 4. Performance Analysis of Data Encryption Algorithms

In this area intends to give the readers for the necessary background to understand the key differences between the compared algorithms.

1) **DES:** (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974. Since that time, many attacks and methods recorded that exploit the weaknesses of DES, which made it an insecure block cipher.
2) **3DES:** An enhancement of DES, the 3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level.
3) **AES:** (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Rijndael (pronounced Rain Doll) algorithm was selected in 1997, after a competition to select the best encryption standard. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers.
4) **Blowfish:** Blowfish is a variable length key, 64-bit block cipher. The Blowfish algorithm was first introduced in 1993. This algorithm can be optimized in hardware applications though it's mostly used in software applications. It suffers from weak keys problem, no attack is known to be successful against.

### 4.1 Related Work and Comparative Results

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources. The below Table 4.1 contains the speed benchmarks for some of the most commonly used cryptographic algorithms. These results are good to have an indication about what the presented comparison results. It is shown that Blowfish and AES have the best performance among others. And both of them are known to have better encryption (i.e. stronger against data attacks) than the other two.

**Table 4.1:** Comparison results using Crypto++

| *Algorithm* | *Megabytes(2^20 bytes) Processed* | *Time Taken* | *MB/ Second* |
|---|---|---|---|
| Blowfish | 256 | 3.976 | 64.386 |
| Rijndael (128-bit key) | 256 | 4.196 | 61.01 |
| Rijndael (192-bit key) | 256 | 4.817 | 53.145 |
| Rijndael (256-bit key) | 256 | 5.308 | 48.229 |
| DES | 128 | 5.998 | 21.34 |
| (3DES)DES-XEX3 | 128 | 6.159 | 20.783 |
| (3DES)DES-EDE3 | 64 | 6.499 | 9.848 |

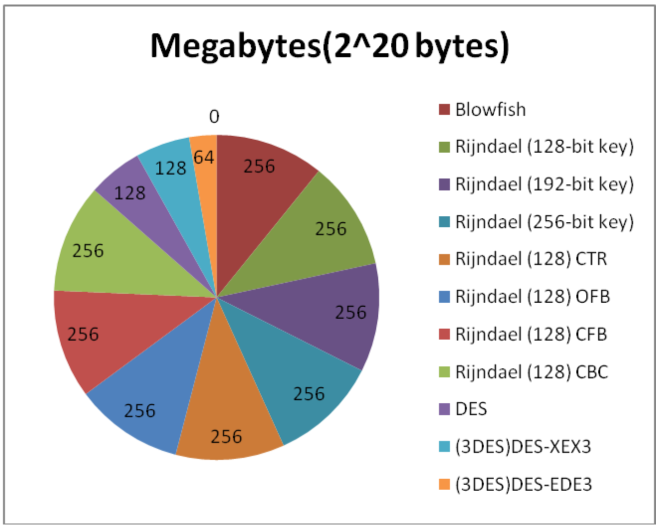


**Figure 4.2:** Comparison results using Crypto++ - Graph

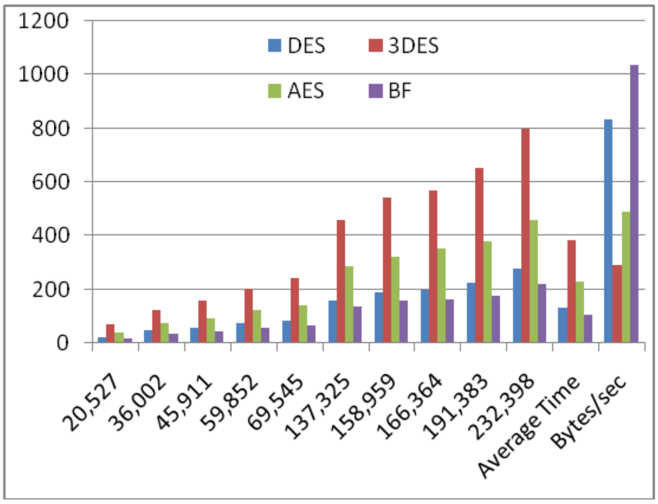


**Figure 4.3:** Comparative Execution time in Encryption Algorithm System 1

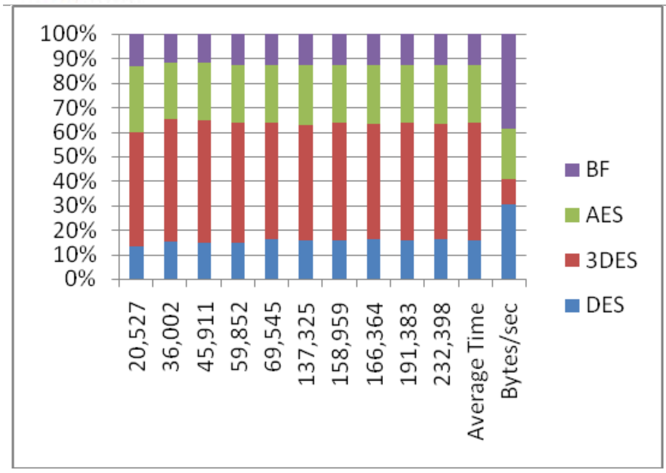


**Figure 4.4:** Comparative Execution time in Encryption Algorithm System 2

The result is easy to observe that Blowfish has an advantage over other algorithms in terms of throughput and also comparison between the algorithms in stream mode using Chain Block Chaining (CBC).

The results showed that Blowfish has a very good performance compared to other algorithms. Also it showed that AES has a better performance than 3DES and DES. Amazingly it shows also that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data.

The above experiments for comparing the performance of the different encryption algorithms implemented inside .NET framework. Their results are close to the ones shown in Figure 4.3.

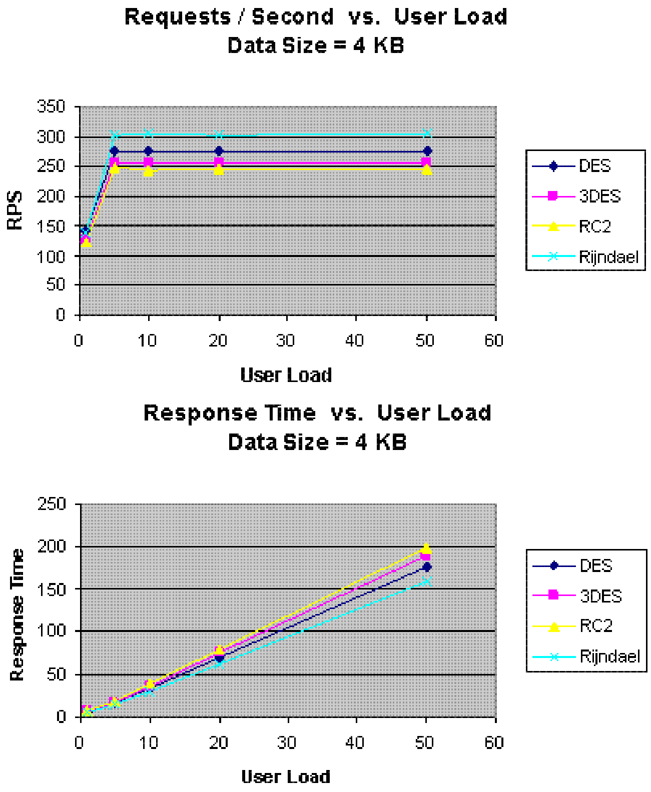


**Figure 4.5**: Comparison results using .NET implementations.

The comparison was performed on the following algorithms: DES, Triple DES (3DES), RC2 and AES (Rijndael). The results shows that AES outperformed other algorithms in both the number of requests processes per second in different user loads, and in the response time in different user-load situations.

## 5. Simulation Environment and Discussion

This simulation uses the provided classes in .NET environment to simulate the performance of DES, 3DES and AES (Rijndael). In this Triple Data Encryption Standard implementation used here under the name Cryptograph.NET. This implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm. The implementation uses managed wrappers for DES, 3DES and Rijndael available in System.Security.Cryptography that wraps unmanaged implementations available in CryptoAPI. TDESCryptoServiceProvider, TripleDESCryptoServiceProvr and Rijndael Managed respectively. There is only a pure managed implementation of Rijndael available in System.Security.Cryptography, which was used in the tests.

### 5.1 Performance Evaluation Methodology

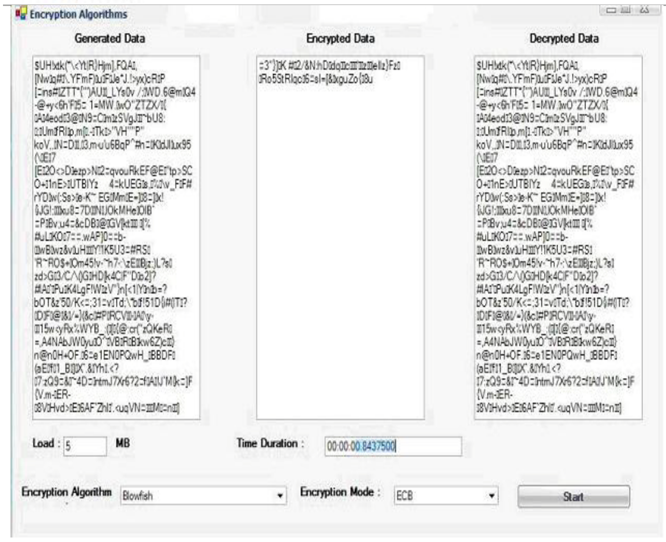
This section describes the techniques and simulation choices made to evaluate the performance of the compared algorithms. In addition to that, we will discuss the methodology related parameters like: system parameters, experiment factor(s), and experiment initial settings.

### 5.1.1 Simulation Procedure

Consider the different sizes of data blocks (0.5MB to 20MB) the algorithms were evaluated in terms of the time required to encrypt and decrypt the data block. All the implementations were exact to make sure the accurate results The Simulation program accepts three inputs:

a. Algorithm,
b. Cipher Mode and
c. Data block size.

After a successful execution, the data generated, encrypted, and decrypted are shown in the Figure 5.1. Note: Most of the characters cannot appear since they do not have character representation. Another comparison is made after the successful encryption/decryption process to make sure that all the data are processed in the right way by comparing the generated data (the original data blocks) and the decrypted data block generated from the process.



Load : 5 MB

Time Duration : 00:00:00.8437500

Encryption Algorithm Blowfish

Encryption Mode : ECB

Start

**Figure 5.1:** GUI Environment Simulation Program

### 5.1.2 Simulation Results

This section show the results obtained from running the simulation program using different data loads. The results show the impact of changing data load on each algorithm and the impact of Cipher Mode (Encryption Mode) used.

### 5.1.3 Performance Results with ECB

The first set of experiments were conducted using ECB mode, the results are shown below in Figure 5.2. The results show the superiority of DES algorithm over other algorithms in terms of the processing time. It shows also that AES consumes more resources when the data block size is relatively big. The results shown here are different from the results, since the data block sizes used here are much larger than the ones used in their experiment. Note: here 3DES requires always more time than DES because of its triple phase encryption characteristic. DES and 3DES are known to have worm holes in their security mechanism, Blowfish and AES, on the other hand, do not have any so far. These results have nothing to do with the other loads on the computer since each single experiment was conducted multiple times resulting in almost the same expected result. DES, 3DES and AES implementation in .NET is to be best.

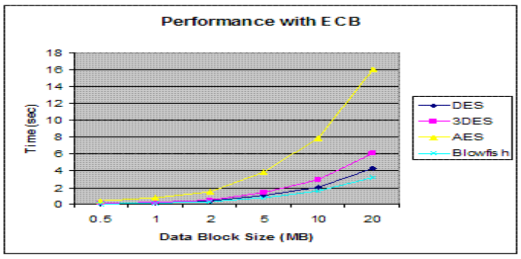


**Figure 5.2:** Performance Results with ECB Mode

### 5.1.4 Performance Results with CBC

In CBC requires more processing time than ECB because of its key-chaining nature. The results show in Figure 5.3 indicates also that the extra time added is not significant for many applications, knowing that CBC is much better than ECB in terms of protection. The difference between the two modes is hard then the results showed that the average difference between ECB and CBC is 0.059896 seconds, which is relatively small.

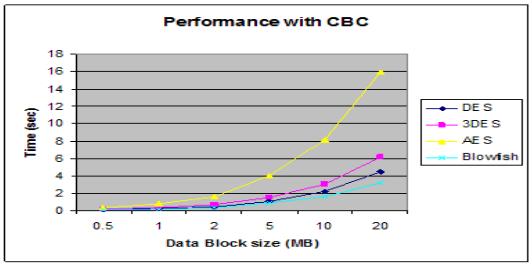


**Figure 5.3:** Performance Results with CBC Mode

This section showed the simulation results obtained by running the four compared encryption algorithms using different Cipher Modes. Different load have been used to determine the processing power and performance of the compared algorithm.

## 6. Conclusion and Future work

The presented simulation results showed that 3DES has a better performance result with ECB and CBC than other common encryption algorithms used. In this paper we present a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, 3DES, Blowfish, RC2, and RC4. In case of changing key size, it can be seen that higher key size leads to clear change in the battery and time consumption. In future the work may be extensive by including the schemes and techniques over different types of data such as image, sound and video and rising a stronger encryption algorithm with high speed and minimum energy consumption.

## Acknowledgement

My sincere gratitude to The Management, and I am grateful thank to our department staff members of computer science, Don Bosco College, Dharmapuri, Tamil Nadu, India, for their Support and motivation.

## References

[1] Aamer Nadeem, "A Performance Comparison of Data Encryption Algorithm," IEEE 2005.

[2] Abdul kader, Diaasalama and Mohiv Hadhoud, "Studying the Effect of Most Common Encryption Algorithms," International Arab Journal of e-technology, Vol.2. No.1.

[3] Aman Kumar, Sudesh Jakhar, Sunil Maakar, "Distinction between Secret key and Public key Cryptography with existing Glitches", Volume: 1, 2012.

[4] Data Encryption Standard (DES), FIPS PUB 46-3 - 1999.

[5] Feistel, Cryptography and Computer Privacy, Scientific American, Volume: 28, No.5, 1973.

[6] Grabbe J, Data Encryption Standard: The Triple DES algorithm illustrated Laissez faire city time, Volume: 2, No. 28, and 2003.

[7] Jian L and Ligan S, Study on Chaotic Cryptosystem for Digital Image Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52 - 1998.

[8] Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52 - 1998.

## Author Profile

**Mr. S. Karthik** received the M.C.A, in Sacred Heart College, Tirupattur, and pursuing M.Phil., degree at Don Bosco College, Sogathur, Dharmapuri, Tamilnadu, India. He is a Research Scholar in the field of Network Security. He is very much enthusiastic in NETWORKING area.

**Mr. A. Muruganandam** received the M.Sc., in Thanthai Hans Roever College, Perambalur, and M.Phil., degree at Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, in 1999 and 2004 respectively. He is an Assistant Professor cum Head in the Research Department of Computer Science, Don Bosco College, Sogathur, Dharmapuri, Tamilnadu, India. Presently pursuing Doctorate Degree [Ph.D.] in Computer Science at Bharathiar University, Coimbatore. He is a Research Scholar in the field of Wireless Sensor Networks. He is very much interested in Networking area.. His ongoing research focused on Selective Jamming Attacks in Wireless Sensor Network