ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Data Encryption and Decryption Using By Triple DES Performance Efficiency Analysis of Cryptosystem

Praveen Kumar B[1], Rajaanadan N.S[2]

Research Scholar, Dept. of Computer Science, KMG College of Arts and Science, Gudiyattam, Tamilnadu, India[1]

Asst. Professor, Dept. of Computer Science, KMG College of Arts and Science, Gudiyattam, Tamilnadu, India[2]

ABSTRACT: Cryptography plays very important role in security of data. Cryptography means to transfer sensitive information across insecure networks like internet so that it cannot be read by anyone except the person whom we want to send it. It basically hides the information. The federal organization used the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA) which may be used to protect sensitive data. Cryptography algorithms are divided into Symmetric and Asymmetric key cryptography. Symmetric Cryptography is further divided into Block Ciphers and Stream ciphers. This paper discusses Performance Analysis of different block cipher algorithms (DES, 3DES, BLOWFISH) of Symmetric Key Cryptography. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. Simulation results are given to demonstrate the effectiveness of each algorithm. Simulation has been conducted by using .Net frame work and C# language.

General Terms
Information Security, Encryption, Network Security
KEYWORDS: Encryption, DES, 3DES

I. INTRODUCTION

In recent years, a lot of applications based on internet are emerged such as on-line shopping, stock trading, internet banking and electronic bill payment etc. Such transactions, over wire or wireless public networks demand end-to-end secure connections, should be confidential, to ensure data authentication, accountability and confidentiality, integrity and availability, also known as *CIA triad* [1]. 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. The only problem with 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 supposedly 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 are 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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

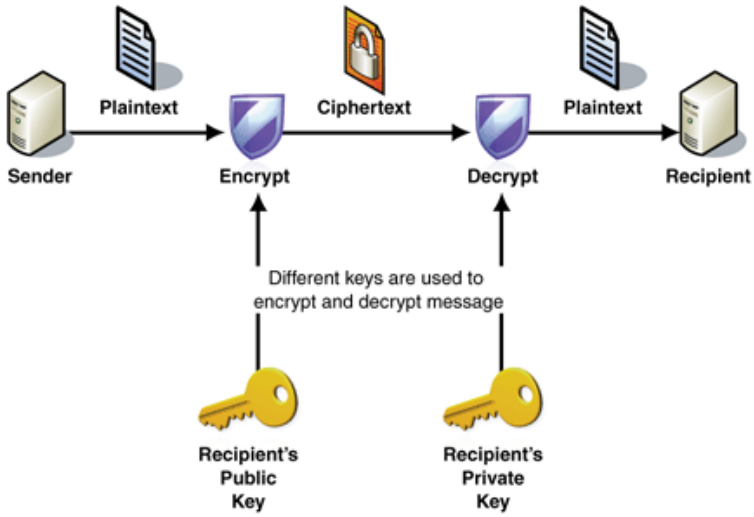

Figure.1 Key schedule for Encryption and Decryption

II. RELATED WORK

An overview of the main goals behind using cryptography will be discussed in this section along with the common terms used in this field. The cryptographic algorithm is a block cipher with a block length of 128 bits and key length of 256 bits. The secret message is encrypted by this block cipher. Two cipher text bits are to be embedded in each pixel of the image. Each pixel is 8 bits. The embedding locations in a pixel are: 6th and 7th bit locations or 7th and 6th bit locations or 7th and 8th bit locations or 8th and 7th bit locations depending upon the cipher text bits. The 8th bit means the Least Significant Bit (LSB). The technique is experimented and results are discussed. In this technique is a unique and stronger approach of doing Steganography with images. It provides two levels of security, one at the cryptography level and other at the Steganography level. The cryptography algorithm is a block cipher with 256 bit key, thus a stronger one. The Steganography follows a cipher text dependent embedding. After the cipher text is embedded, the degradation in image quality is not noticeable by human visual system. The amount of message that can be embedded is also very good. The technique is not susceptible to histogram based attacks.

Cryptography is usually referred to as "the study of secret", while nowadays is most attached to the definition of encryption. Encryption is the process of converting plain text "unhidden" to a cryptic text "hidden" to secure it against data thieves. This process has another part where cryptic text needs to be decrypted on the other end to be understood. Figure.1 shows the simple flow of commonly used encryption algorithms.

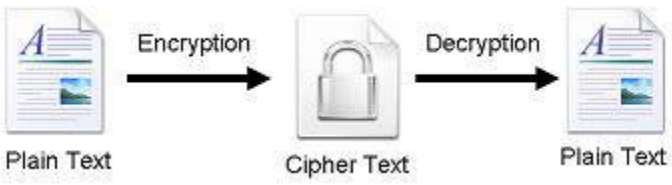

Figure.1 Encryption-Decryption Flow

As defined, cryptographic system is "a set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context." This definition defines the whole mechanism that provides the necessary level of security comprised of network protocols and data encryption algorithms.

A.Goals of Cryptosystem

This section explains the five main goals behind using Cryptography.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Authentication: This means that before sending and receiving data using the system, the receiver and sender identity should be verified.
Secrecy or Confidentiality: Usually this function (feature) is how most people identify a secure system. It means that only the authenticated people are able to interpret the message (date) 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: 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. Such systems should provide a way to grant their users the quality of service they expect.
B. Advantages of DES over other algorithms:

- DES has been around a long time (since 1978) and has been studied to death. Even now no real weaknesses have been found: the most efficient attack is still brute force
- DES is an official US Government standard; the US Government is required to re-certified the DES every five years and ask it be replaced if necessary. DES has been re-certified in 1983, 1987and 1992.
- Anybody can learn the details and implement it because DES is also an ANSI and ISO standard.
- Since DES was designed to run on long time hardware, it is so fast in hardware and to relatively fast in software.

C. Disadvantages of DES:

- The 56-bit key size is the biggest defect of DES. Chips to perform one million of DES encrypt or decrypt operations a second are available (in 1993). A $1 million DES cracking machine can search the entire key space in about 7 hours.
- Hardware implementations of DES are very fast; DES was not designed for software and hence runs relatively slowly.

III. PROPOSED ALGORITHM

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.

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.

A. Implementation of Triple DES (3DES)

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

- ✓ Block cipher with symmetric secret key
- ✓ Block length = 64 bits
- ✓ Key length = 56, 112 or 168 bits

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

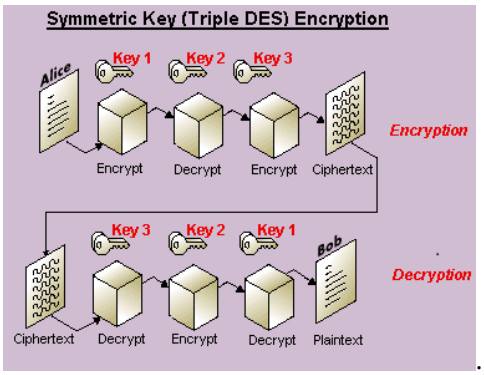

Figure 2.1 Triple DES Encryption and Decryption

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.

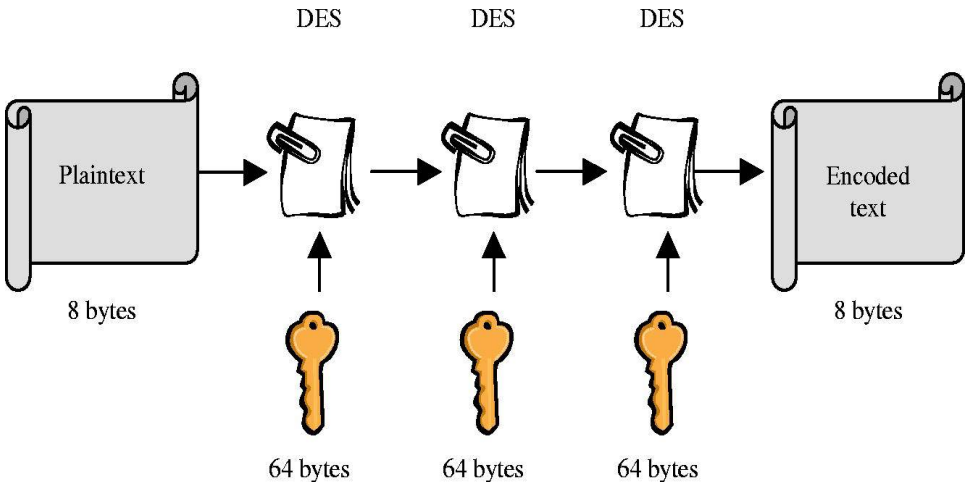

Figure 2.1 Triple DES using 64 bytes

The above Figure 2.1 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:

- ✓ All keys being independent
- ✓ Key 1 and key 2 being independent keys
- ✓ All three keys being identical

Key options 3 as shown in Figure 2.2 triple DES. The triple DES key length contains 168 bits but the key security falls to 112 bits**.**

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

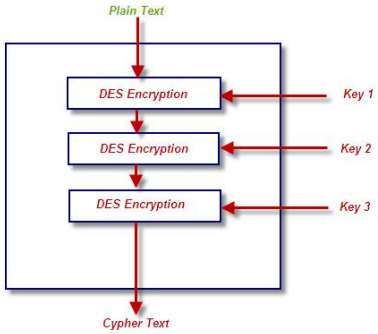

Figure 2.2 Working of Triple DES

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 (1992)

Has 112 bits of security, not 3 56 = 168

Triple DES algorithm uses three iterations of common DES cipher. In its strongest version, 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. It is stronger than simply DES encrypting used twice (with two 56-bit keys) because it protects against meet-in-the-middle attacks.

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

IV. 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.

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.

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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

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.

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.

A. 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 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 1: Comparison results using Crypto++

Algorithm	Megabytes(2^20 bytes) Processed	Time Taken	MB/Second
Blowfish	256	3.975	64.402
Rijndael (128-bit key)	256	4.197	61.995
Rijndael (192-bit key)	256	4.818	53.134
Rijndael (256-bit key)	256	5.307	48.238
Rijndael (128) CTR	256	4.435	57.722
Rijndael (128) OFB	256	4.835	52.947
Rijndael (128) CFB	256	5.379	47.592
Rijndael (128) CBC	256	4.618	55.435
DES	128	5.997	21.344
(3DES)DES-XEX3	128	6.160	19.364
(3DES)DES-EDE3	64	6.498	9.849

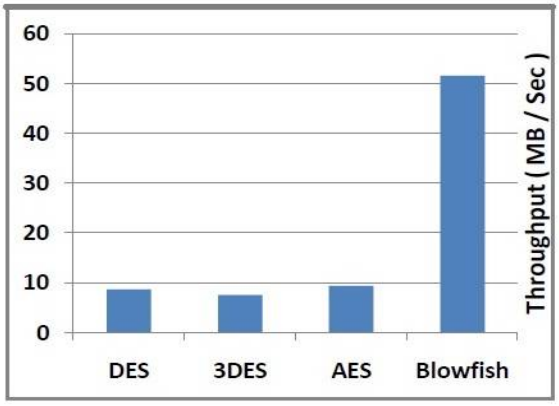

Figure 1.2 Throughput of encryption algorithms

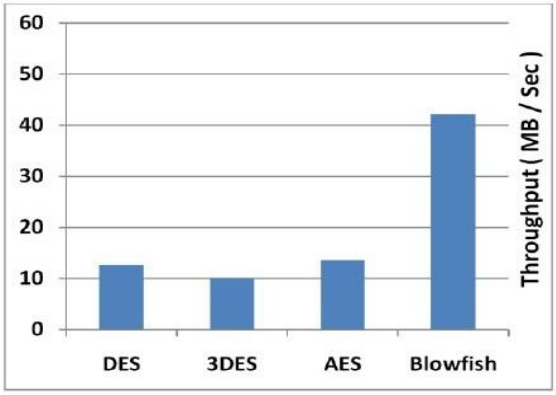

Figure 1.3. Throughput of decryption algorithms

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

The above figure 1.2 &1.3 shows evaluate the performance of the suggested system, a performance test was conducted for a method with an DES encryption algorithm, which has been applied in the existing systems, and for a method with the scrambling encryption technique.

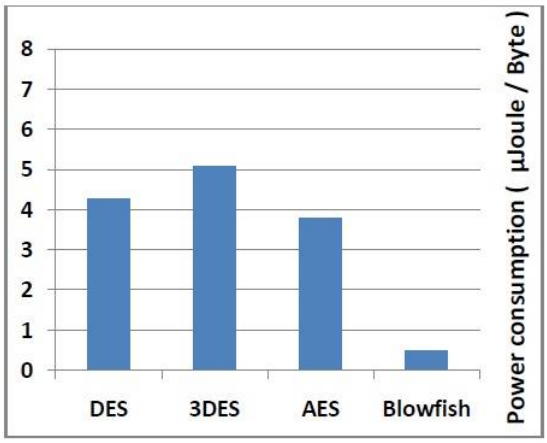

Figure 1.4. Power consumption (µJule / Byte)

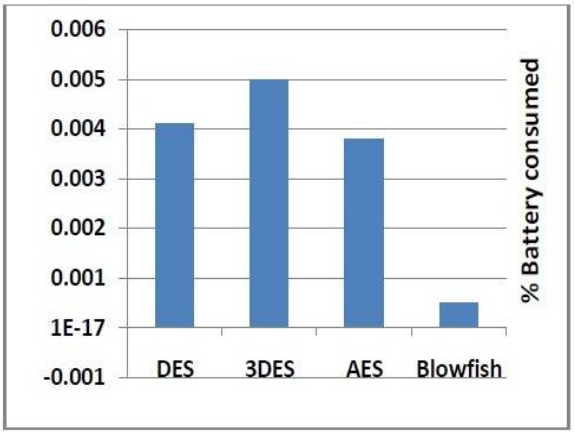

Figure 1.5. Power consumption (% battery con)

Figure 1.4 & 1.5 shows the battery consumption for the derived algorithms.

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.

The limitation of the new improver algorithm is Memory Used in New method is higher than the old method. This is because of the algorithms which we have used is providing a very high security. As we have used “3DES” a bundle of three algorithms which is providing very high security as compared to the previous algorithm which is “DES”. So from these results we can conclude that we have reduced the time complexity and enhanced the security level for the Data Transmission.

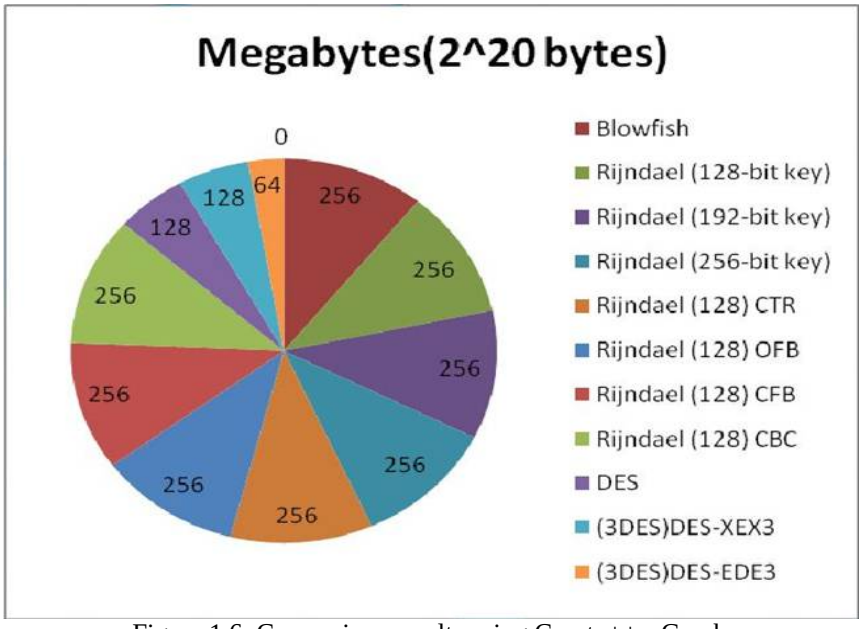

Figure 1.6: Comparison results using Crypto++ - Graph

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

V. SIMULATION ENVIRONMENT AND DISCUSSION

In this section describes the simulation environment and the used system components. This simulation uses the provided classes in .NET environment to simulate the performance of DES, 3DES and AES (Rijndael). In this thesis 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. These are DESCryptoServiceProvider, TripleDESCryptoServiceProvider and Rijndael Managed respectively. There is only a pure managed implementation of Rijndael available in System.Security.Cryptography, which was used in the tests.

Table 1
Algorithm Settings
Shows the algorithms settings used in this experiment. These settings are used to compare the results.

Algorithm	Key Size (Bits)	Block Size (Bits)
DES	64	64
3DES	192	64
Rijndael	256	128
Blowfish	448	64

3DES and AES support other settings, but these settings represent the maximum security settings they can offer. Longer key lengths mean more effort must be put forward to break the encrypted data security.

Since the evaluation test and the results using block cipher, due to the memory constraints on the test machine (1 GB) the test will break the load data blocks into smaller sizes. The load data are divided into the data blocks and they are created using the Random Number Generator class available in System.Security.Cryptography.

A. 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.

B. System Parameters

The experiments are conducted using 3500+ AMD 64bit processor with 1GB of RAM. The simulation program is compiled using the default settings in .NET 2010 visual studio for C# windows applications. The experiments will be performed couple of times to assure that the results are consistent and are valid to compare the different algorithms.

C. Experiment Factors

To evaluate the performance of the compared algorithms, the parameters that the algorithms must be tested for must be determined. The security features of each algorithm as their strength against cryptographic attacks is already known and discussed. The experiment factor to determine the speed performance of algorithms and to encrypt/decrypt data blocks of various sizes.

D. 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 as shown below in Figure 5.1 accepts three inputs:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

- ✓ Algorithm,
- ✓ Cipher Mode and
- ✓ Data block size.

After a successful execution, the data generated, encrypted, and decrypted are shown in the Figure 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.

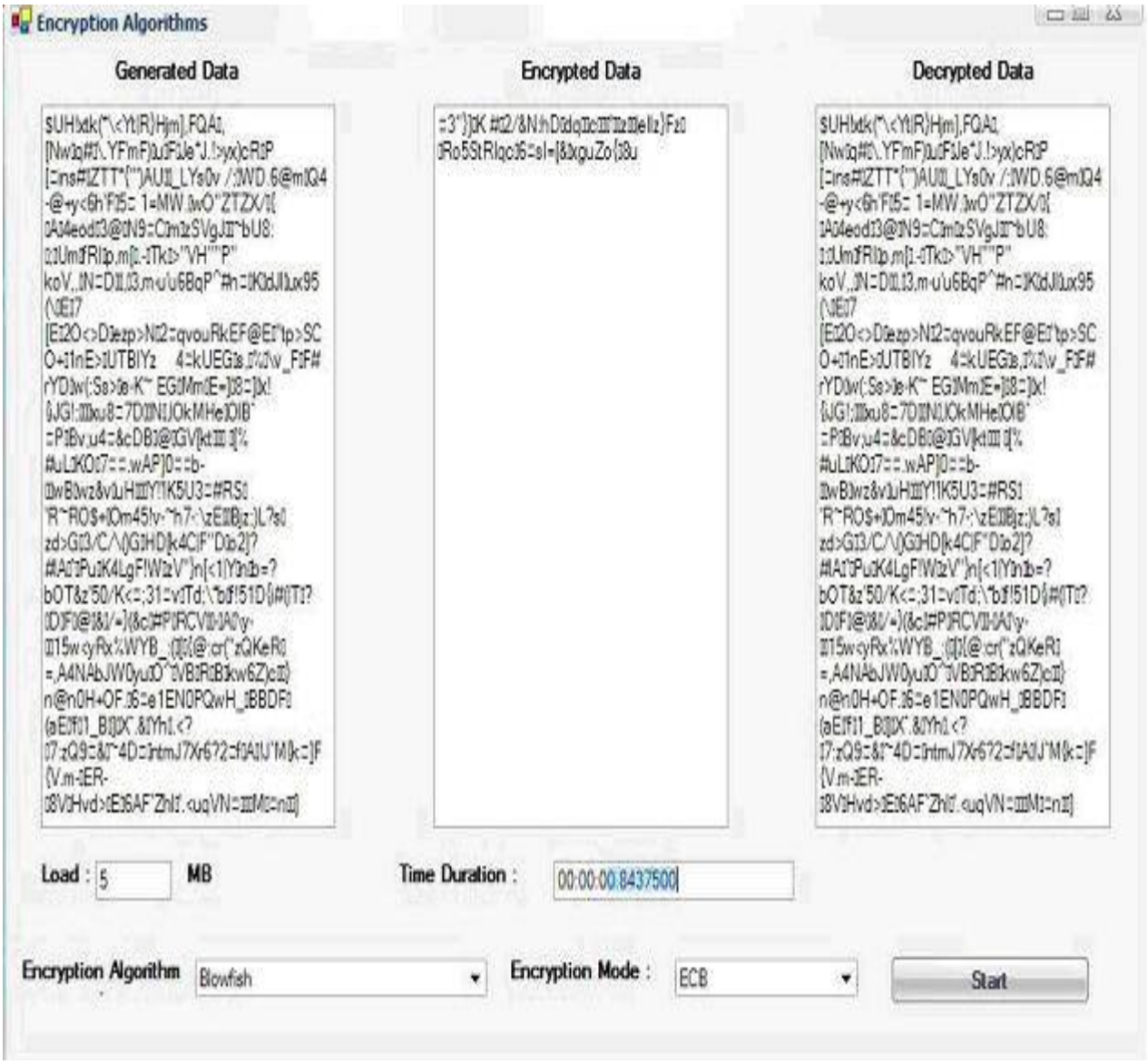

Figure 1 GUI Environment Simulation Program

Simulation Results

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

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.

Performance Results with ECB

The first set of experiments were conducted using ECB mode, the results are shown below in Figure 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.

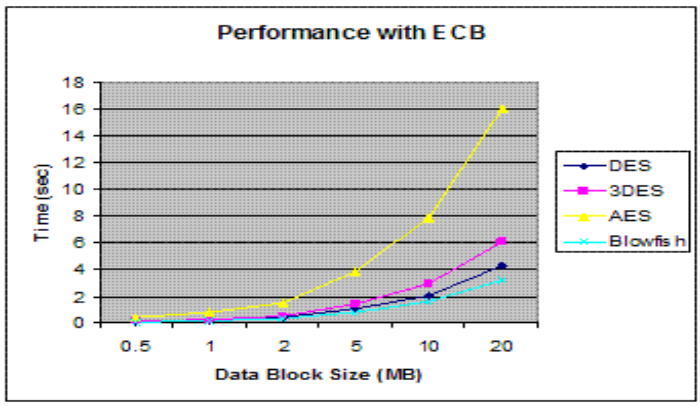

Figure 2 Performance Results with ECB Mode

Performance Results with CBC

In CBC requires more processing time than ECB because of its key-chaining nature. The results show in Figure 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 second, which is relatively small.

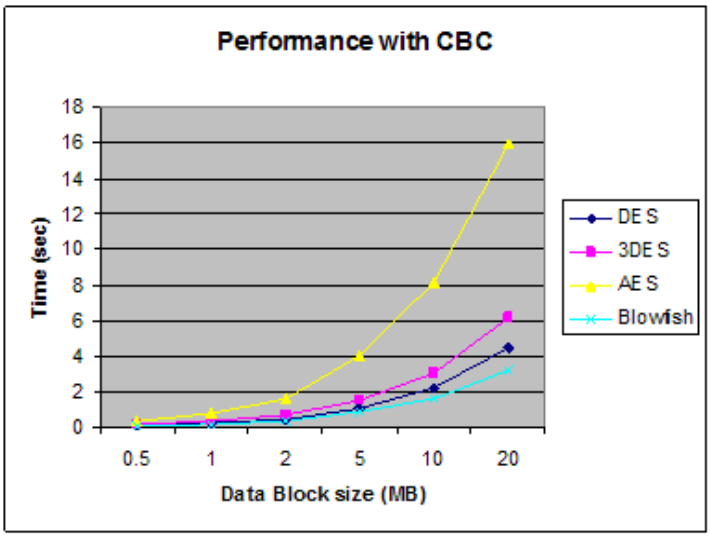

Figure 3 Performance Results with CBC Mode

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

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.

VI. CONCLUSION AND SCOPE OF FUTURE WORK

The internet usage and network system is growing rapidly. So there are some additional requirements to secure the data transmitted over different networks using different services. To afford the security to the network and data different encryption methods are used. In this paper, a survey on the existing works on the Encryption techniques has been done. To sum up, all the techniques are useful for real-time Encryption. Each technique is unique in its own way, which might be suitable for different applications and has its own pro's and con's. According to research done and literature survey it can be found that 3DES algorithm is most efficient in terms of speed, time, and throughput effect. The Security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. Our future work will explore this concept and a combination of algorithms will be applied either sequentially or parallel, to setup a more secure environment for data storage and retrieval. It is a flexible solution for any cryptographic system and security layers of wireless protocol. Measurement results and comparisons between the proposed and previous hardware implementations are presented that shows quite encouraging results. 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. Our future work will explore this concept and a combination of algorithms will be applied either sequentially or parallel, to setup a more secure environment for data storage and retrieval.

REFERENCES

1. Aamer Nadeem, "A Performance Comparison of Data Encryption Algorithm," IEEE 2005.
2. Abdul D S, Elminaam, Kader H M A and Hadhoud MM (2008), "Performance Evaluation of Symmetric Encryption Algorithms," IJCSNS International Journal of Computer Science and Network Security, Vol.8 No.12, December.
3. Abdul kader, Diaasalama and Mohiv Hadhoud, "Studying the Effect of Most Common Encryption Algorithms," International Arab Journal of e-technology, Vol.2. No.1.
4. Abhishek Pandey, Tripathi R C, "A Survey on Wireless Sensor Networks Security" International Journal of Computer Applications (0975 – 8887), Volume 3 – No.2, June 2010.
5. Akkaya K, Demirbas M and Aygun R.S. "The Impact of Data Aggregation on the performance of Wireless Sensor Networks", Wiley Wireless Communication Mobile Computing (WCMC), Vol.3, 171-193, 2008.
6. Al-Karaki J, Ul-Mustafa R, Kamal A (2004), Data aggregation in wireless sensor networks exact and approximate algorithms in proceedings of the workshop on high performance switching and routing (pp. 241–245).
7. Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Maakar, "Distinction between Secret key and Public key Cryptography with existing Glitches", IJEIM - 0067, vol.1, 2012.
8. Anjum F, Subhadrabandhu D and Sarkar S (2004), "Signature based Intrusion Detection for Wireless Ad-Hoc Networks, A Comparative study of various routing protocols", in IEEE 58th Vehicular Technology Conference.

BIOGRAPHY

Praveen Kumar B is a Research Scholar in the Department of Computer Science, KMG College of Arts and Science, Gudiyattam, Vellore District, Tamil Nadu, India. He received Master of Computer Application (MCA) degree in 2009 from Sacred Heart College, Tirupattur, Vellore District, Tamil Nadu, and India. His research interests are Network Security, Crypto System, Algorithms, and RDBMS etc.