ISSN 2229-5518

Evaluation of Data Encryption Algorithms

Neha Ramdeo

Abstract— This paper tries to present a comparison between the most common and used algorithms in the data encryption field. 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. This paper provides a performance comparison between four of the most common encryption algorithms: DES, 3DES, Blowfish and AES. The comparison has been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithm's encryption/decryption speed. Simulation has been conducted using C# language.

Index Terms— Encryption Algorithms, Cryptography, AES, DES, Blowfish, TripleDES

1 Introduction

The increased importance of exchanged data over the internet has led to the research for the best solution to offer the necessary protection against the data thieves' attacks along with speed and efficiency. Encryption is a process of converting plain data "unhidden" to cryptic data "hidden" to save it against data thieves'. This process has another part where cryptic text needs to be decrypted on the other hand to be understood. Fig. 1 shows the simple flow of commonly used Encryption - Decryption Flow encryption algorithms.

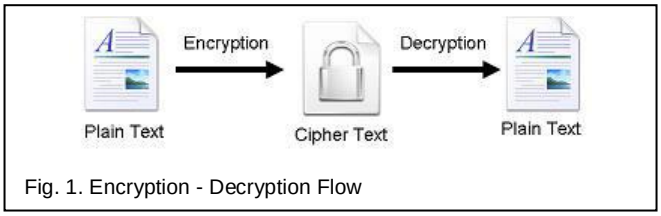

Fig. 1. Encryption - Decryption Flow

2 Encryption Goals

This section explains the five main goals behind using Cryptography [Aamer2005].

Authentication: This means that before sending and receiving data using the system, the receiver and sender identity should be verified.

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.

• *Neha Ramdeo is currently pursuing bachelors of technology program in computer science in Jaypee Institute of Information Technology, India. E-mail: neha.ramdeo@gmail.com*

3 Data Encryption Algorithms

This section intends to give the readers 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 weaknesses of DES, which made it an insecure block cipher.

3DES: As an enhancement of DES, the3DES (TripleDES) 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. But it is a known fact that 3DES is slower than other block cipher methods.

AES: (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. It was originally called Rijndael (pronounced Rain Doll). It was selected in 1997 after a competition to select the best encryption standard. It has variable key length of 128, 192, or 256 bits; default 256. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices 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: It is one of the most common public domain encryption algorithms provided by Bruce Schneier –one of the world's leading cryptologists, and the president of Counterpane Systems, a consulting firm specializing in cryptography and computer security. It takes a variable length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all uses.

4 Simulation Setup

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). Blowfish implementation used here is the one provided by Markus Hahn [BlowFish.NET] under the name Blowfish.NET. This implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm. These settings are used to compare the results with the initial results obtained from [Priya2002].

TABLE 1
ALGORITHM SETTINGS

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

5 Simulation Procedure

Here, our goal is to measure the Encryption and Decryption speed of each algorithm for different packet sizes. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased, the power consumption of this encryption technique is decreased.

By considering 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 that the results will be relatively fair and accurate.

The Simulation program (shown in Fig. 2) accepts three inputs: Algorithm, Cipher Mode and data block size. After a successful execution, the data generated, encrypted and decrypted are shown. 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.

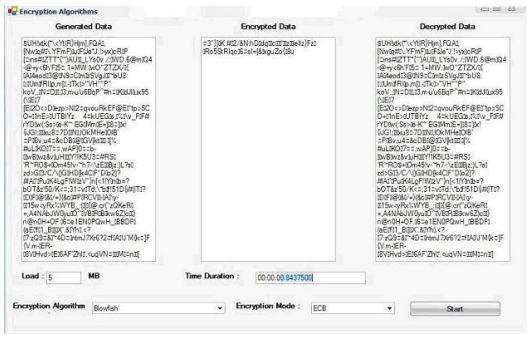

Fig. 2. GUI of Simulation Program

6 Simulation Results

Simulation results for this compassion point are shown Fig. 3 at encryption stage. The results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time. It can also be noticed here; that 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics [IJCSC2011].

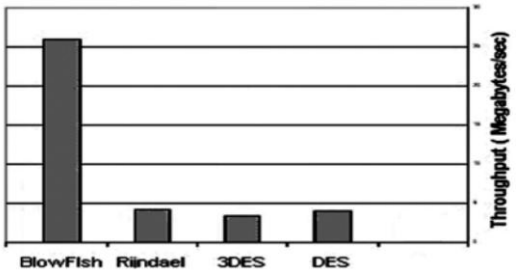

Fig. 3. Throughput of each encryption algorithm (Megabyte/Sec)

Simulation results for this compassion point are shown Fig. 4 decryption stage. We can find in decryption that Blowfish is the better than other algorithms in throughput and power consumption. Finally, Triple DES (3DES) still requires more time than DES.

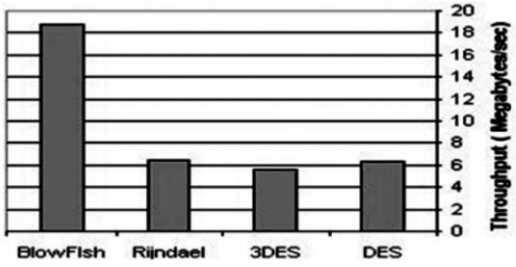

Fig. 4. Throughput of Each Decryption Algorithm (Megabyte/Sec)

This section will 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 [Aamer2005].

6.1 Performance Results with ECB

The first set of experiments were conducted using ECB mode, the results are shown in fig. 5 below. The results show the superiority of Blowfish 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.

Another point can be noticed here that 3DES requires always more time than DES because of its triple phase encryption characteristic. Blowfish, although it has a long key (448 bit), outperformed other encryption algorithms. 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.

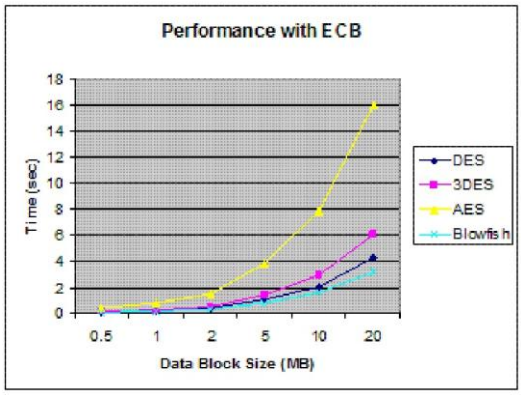

Fig. 5. Performance Results with ECB Mode

6.2 Performance Results with CBC

As expected, CBC requires more processing time than ECB because of its key-chaining nature. The results show in Fig. 6 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.

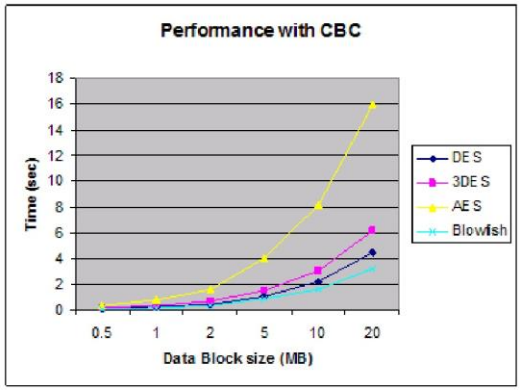

Fig. 6. Performance Results with CBC Mode

7 Conclusion

The presented simulation results showed that Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, this makes it an excellent candidate to be considered as a standard encryption algorithm. AES showed poor performance results compared to other algorithms since it requires more processing power. Using CBC mode has added extra processing time, but overall it was relatively negligible especially for certain application that requires more secure encryption to a relatively large data blocks.

References

[1] [Aamer2005]Aamer Nadeem, *"A Performance Comparison of Data Encryption Algorithm"*, IEEE 2005.

[2] [IJCSC2011]Simar Preet Singh, and Raman Maini, *"Comparisons of Data Encryption Algorithm"* International Journal of Computer Science and Communication, vol. 1, no. 1, pp 125-127, January-June 2011,

[3] [Priya2002]Priya Dhawan., *"Performance Comparison: Security Design Choices,"* Microsoft Developer Network October 2002.