PERFORMANCE ANALYSIS OF SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS: DES, AES and BLOWFISH

Nagesh Kumar[1], Jawahar Thakur[2], Arvind Kalia[3]

[2]Associate Professor, [3]Professor,

Department of Computer Science, Himachal Pradesh University, Shimla

[1]engg.nagesh2@gmail.com, [2]jawahar.hpu@gmail.com, [3]arvkalia@gmail.com

Abstract: - *Security is the most challenging aspects in the internet and network applications. 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. This paper provides a fair comparison between three most common symmetric key cryptography algorithms: DES, AES, and Blowfish. The comparison is made on the basis of these parameters: speed, block size, and key size. Simulation program is implemented using Java programming.*

Keywords: *Cryptography, DES, AES, Blowfish, Encryption, Decryption.*

I. Introduction:

Cryptography is usually referred to as “the study of secret”. Encryption is the process of converting normal text to unreadable form. Decryption is the process of converting encrypted text to normal text in the readable form. Figure 1 below shows the conventional cryptographic process.

Figure 1: Conventional Encryption Model

As defined in RFC 2828 (RFC2828), cryptographic system is "*a set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context.*" The definition gives the whole mechanism that provides the necessary level of security comprised of network protocols and data encryption algorithms.

Cryptography Goals:

There are five main goals of 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 (Earle, 2005):

- Authentication: The process of proving one's identity. This means that before sending and receiving data using the system, the receiver and sender identity should be verified.
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver. Usually this function is how most people identify a secure system. It means that only the authenticated people are able to interpret the message content and no one else.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original. The basic form of integrity is packet check sum in IPv4 packets.
- Non-repudiation: A mechanism to prove that the sender really sent this message. Means 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 provide a way to grant their users the quality of service they expect.

Symmetric and Asymmetric Encryptions:

There are two main categories of cryptography depending on the type of security keys used to encrypt/decrypt the data. These two categories are: Asymmetric and Symmetric encryption techniques.

Symmetric Encryption

It is also called as single key cryptography. It uses a single key. In this encryption process the receiver and the sender has to agree upon a single secret (shared) key. Given a message (called plaintext) and the key, encryption produces unintelligible data, which is about the same length as the plaintext was. Decryption is the reverse of encryption, and uses the same key as encryption.

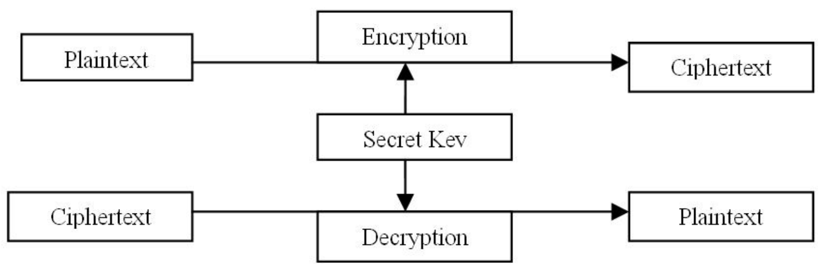

Figure 2: Symmetric Key Cryptography Process

Asymmetric Encryption

It is also called as public key cryptography. It uses two keys: public key,which is known to the public, used for encryption and private key, which is known only to the user of that key, used for decryption. The public and the private keys are related to each other by any mathematical means. In other words, data encrypted by one public key can be encrypted only by its corresponding private key. Encryption and decryption procedure as shown below in figure 3:

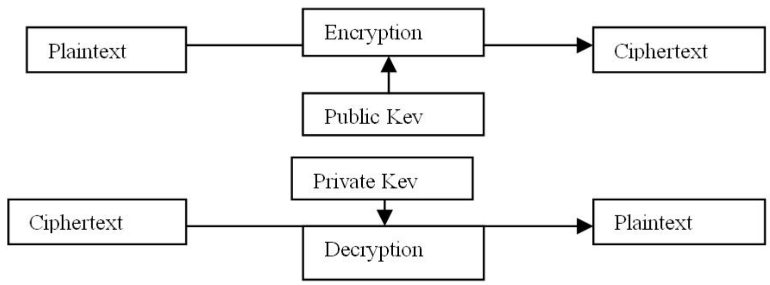

Figure 3: Public Key Cryptography Process

Section 2 will give a brief review of all the concerned research papers. It will provide a brief discussion of the other contributors and their conclusions. Section 3 will discuss the main objective of research. Section 4 will discuss the methodology used in the work with simulation settings. Section 5 will give the results of the research and provide discussion about the same. Finally, section 6 concludes this paper by summarizing the key points and other related considerations.

II. BACKGROUND STUDY:

Compared Algorithms:

DES: (Data Encryption Standard), was the first encryption standard to be published by NIST (National Institute of Standards and Technology). It was designed by IBM based on their Lucifer cipher. DES became a standard in 1974 (www.tropsoft.com). DES uses a 56 bit key, and maps 64 bit input block into a 64 bit output block. The key actually looks like a 64 bit quantity, but one bit in each of the 8 octets is used for odd parity on each octet. There are many attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher.

AES: (Advanced Encryption Standard), also known as the Rijndael (pronounced as Rain Doll) algorithm, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES was introduced to replace the DES. Brute force attack is the only effective attack known against this algorithm.

Blowfish: Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Though it suffers from weak keys problem, no attack is known to be successful against it (Bruce, 1996) (Nadeem, 2005).

Other Contributions

(Tamimi, 2008) provided a performance comparison between four most common algorithms: DES, 3DES, AES, and Blowfish. The comparison had been conducted by running several different settings to process different sizes of data blocks to evaluate the algorithm's encryption/decryption speed. The simulation setup was in C# programming language. The results of this paper shows that blowfish has a better performance than other common encryption algorithms. AES showed poor performance results compared to other algorithms since it requires more processing power.

(Nadeem, 2005) In this paper, the popular secret key algorithms including DES, 3DES, AES (Rijndael), Blowfish, were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented in Java programming, using their standard specifications, and were tested on two different hardware platforms, to present the comparison. The two different machines are: P-II 266 MHz and P-IV 2.4 GHz.

(Dhawan, 2002) has also done experiments for comparing the performance of the different encryption algorithms implemented inside .NET framework. Their results are close to the ones shown before. 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.

(N. Penchalaiahet.al., 2010) discussed the principal advantages of AES with respect to DES, as well as its limitations. They said that AES can be quite comfortably implemented in high level or low level languages.

(Elminaam et. al., 2010) presented a comparison of AES, DES, 3DES, RC2, Blowfish and RC6. They used 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. They concluded that in case of changing packet size Blowfish showed better performance than other algorithms followed by RC6. AES had better performance than RC2, DES, and 3DES. In case of changing key size – it was concluded that higher key size leads to clear change in the battery and time consumption.

III. OBJECTIVE:

This paper provides a performance comparison between symmetric key cryptography algorithms: DES, AES and Blowfish. The comparison has been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithm's speed for encryption and decryption. The paper also shows the analysis on the basis of two block cipher modes: ECB and CBC. Each algorithm is designed and executed in these two modes.

IV. METHODOLOGY:

Simulation and Settings:

The simulation uses the provided classes in java environment to simulate the performance of DES, AES and Blowfish. The implementation uses managed wrappers for DES, AES and Blowfish available in java.cypto and java.security[CryptoSpec] that wraps unmanaged implementations available in JCE (Java Cryptography Extension) & JCA (Java Cryptography Architecture). The Cipher class provides the functionality of a cryptographic cipher used for encryption and decryption. It forms the core of the JCE framework.

Table 1: Algorithms' Settings

Algorithm	Key Size (Bits)	Block Size (Bits)
DES	64	64
AES	128	128
Blowfish	128	64

The evaluation is meant to evaluate the results by using block ciphers. Hence, the load data (plaintext) is divided into smaller block size as per algorithm settings given in Table 1 above.

System Parameters:

The experiments are conducted using AMD Sempron processor with 2GB of RAM. The simulation program is compiled using the default settings in jdk 1.7 development kit for JAVA. The experiments will be performed couple of times to assure that the results are consistent and are valid to compare the different algorithms.

Experiment Factors:

Since the security features of each algorithm as their strength against cryptographic attacks is already known and discussed. The chosen factor here to determine the performance is the algorithm's speed to encrypt/ decrypt data blocks of various sizes.

V. RESULTS AND ANALYSIS:

This section will show the results which are obtained by 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 used.

A. Performance Results with ECB:

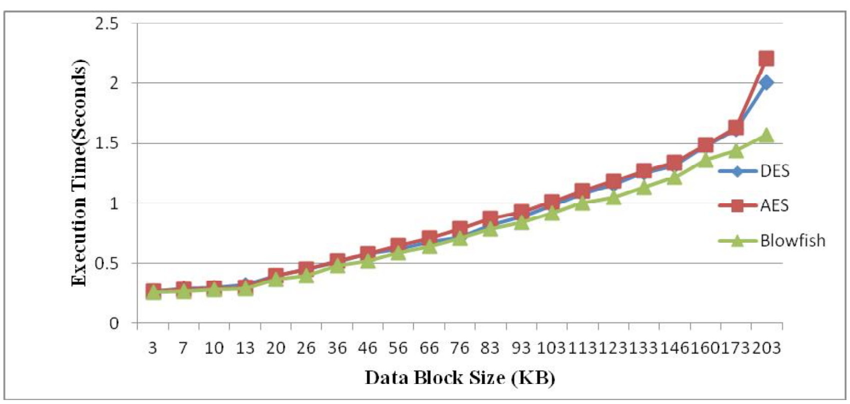

Figure 4: *Performance Results with ECB mode*

The first set of experiments were conducted using ECB mode, the results are shown in figure 4 above. 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.

B. Performance Results with CBC:

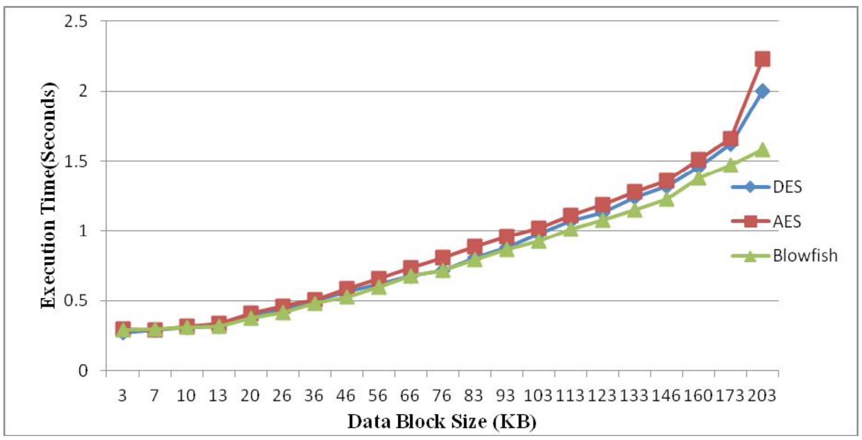

Figure 5: *Performance Results with CBC mode*

The second set of experiments were conducted using CBC mode, the results are shown in figure 5 above. As expected CBC require more processing time than ECB because of its key-chaining nature. The results indicate 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 to see by the naked eye because it is relatively small. Again the results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time.

VI. 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] Singh, S Preet and Maini, Raman. “Comparison of Data Encryption Algorithms”, International Journal of Computer Science and Communication, vol. 2, No. 1, January-June 2011, pp. 125-127.

[2] Elminaam, D S Abd; Kader H M Abdual and Hadhoud, M Mohamed. “Evaluating the Performance of Sysmmetric Encryption Algorithms”, International Journal of Network Security, Vol. 10, No. 3, pp. 216-222, May 2010.

[3] Penchalaiah, N. and Seshadri, R. “Effective Comparison and Evaluation of DES and Rijndael Algorithm (AES)”, International Journal of Computer Science and Engineering, Vol. 02, No. 05, 2010, 1641-1645.

[4] Stallings, W; “Cryptography and Network Security: Principals and Practices”, Prentice Hall, 8th Edition, 2009.

[5] Tamimi, A Al; “Performance Analysis of Data Encryption Algorithms”, Oct 2008.

[6] Results of Comparing Tens of Encryption Algorithms Using Different Settings – Crypto++ Benchmarks, Retrieved Oct. 1, 2008. (http://www.eskimo.com/weidai/benchmarks.html).

[7] Nadeem, Aamer; “A Performance Comparison of Data Encryption Algorithms”, IEEE 2005.

[8] [Hardjono2005],” Security In Wireless LANS And MANS ,”. Artech House Publishers 2005.

[9] Stallings, W;”Cryptography and Network Security”, Prentice Hall, 4th Edition, 2005.

[10] [Edney2003],” Real 802.11 Security: Wi-Fi Protected Access and 802.11i ,”. Addison Wesley 2003.

[11] [RFC2828],"Internet Security Glossary", http://www.faqs.org/rfcs/rfc2828.html.

[12] [TropSoft] "DES Overview", http://www.tropsoft.com/strongenc/des.htm.

[13] Dhawan, Priya; "Performance Comparison: Security Design Choices," Microsoft Developer Network October 2002. http://msdn2.microsoft.com/en-us/library/ms978415.aspx

[14] [Bruce1996] Schneier, Bruce; "Applied Cryptography", John Wiley & Sons, Inc 1996.

[15] http://download.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec

[16] National Institute of Standards and Technology, Data Encryption Standard, FIPS 46-2, 1993.

[17] Kaufman, Charlie; Perlman, Radia and Speciner, Mike. "Network Security Private Communication in a Public World"; Second Edition; Pearson Education; Prentice Hall.

[18] Stallings, William; "Cryptography and Network Security Principles and Practices"; Fourth Edition; Pearson Education; Prentice Hall; 2009.

[19] media.wiley.com/product_data/excerpt/94/.../0764548794.pdf.

[20] Stinson, D.; "Cryptography, Theory and Practice"; CRC Press; Second edition; 2000.

[21] Menezes, A., Oorschot, P. and Vanstone, S. (1996). "Handbook of Applied Cryptography". CRC Press.

[22] Moshopoulos, Nikosand and Chaniotakis, Eleftherios; "A Survey of Cryptography Algorithms – Trends and Products"; National Technical University of Athens, Electrical & Computer Engineering Department, Heroon Polytehneiou 9, 15773 Zographou, Athens, GREECE.

[23] Schneier, B.; Kelsey, J.; Whiting, D.; Wagner, D.; Hall C. and Ferguson N.; "*Performance Comparison of the AES Submissions*"; version 2.0; 1999.

[24] Jorstad, Norman D.; "*Cryptographic Algorithm Metrics* "; Institute for Defense Analyses Science and Technology Division; 1997.