www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-3, Issue-1, Feb- 2015
Review Paper

Int. J. Sci. Res. in Network Security and Communication
ISSN: 2321-3256

Performance Analysis of Data Encryption Algorithms

Sachin sharma[1], Jeevan Singh Bisht[2*]

[1,2*]Dept. of Computer Science and Electronics,
Christian Eminent College Indore, M.P. - INDIA

Received: 10 Dec 2014 Revised: 28 Dec 2014 Accepted: 22 Jan 2015 Published: 28 Feb 2015

Abstract— The two main uniqueness that classify 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. With the emergence of communication techniques as the human beings become advanced day by day these communication techniques also get some advancement or development day by day .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.

Keywords- Encryption Algorithm, AES, DES, Blowfish, TripleDES, Cryptography

I. INTRODUCTION

As the importance and the value of exchanged data over the Internet or other media types are increasing, the search for the best solution to offer the necessary protection against the data thieves' attacks along with providing these services under timely manner is one of the most active subjects in the security related communities. This paper tries to present a fair comparison between the most common and used algorithms in the data encryption field. Since our main concern here is the performance of these algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used.

II. CRYPTOGRAPHY

An overview of the main goals behind using cryptography will be discussed in this section along with the common terms used in this field. 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.

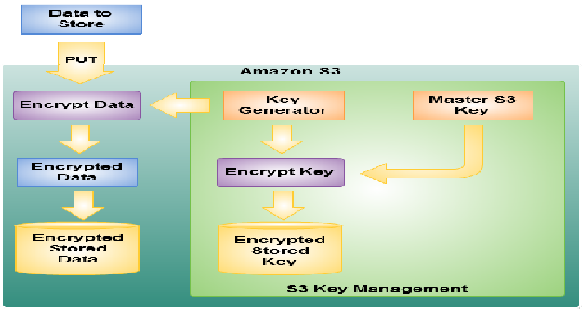


Fig.1 shows the simple flow of commonly used encryption algorithms.

Cryptography Goals:

1) Confidentially or Privacy: -

Keeping information secret from all, but those who are authorized to see it. Confidentially is the protection of transmitted data from passive attacks. With respect to the content of data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. The aspect of confidentially is the protection of traffic flow from analysis. This requires that an attacker not be able to observe to source and destination, frequency, length or any other characteristics of the traffic on a communication facility.

2) Data Integrity: -

Ensuring the information has not been altered by unauthorized or unknown means. One must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution

3) Authentication: -

Corroboration of the identify of an entity. Authentication is a service related to identification. This function applies to both entities and information.

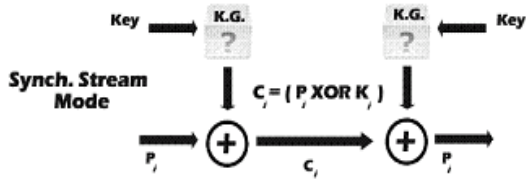
4) Non-repudiation: -

Non-repudiation prevents either sender or receiver from denying a message. Thus, when a message is sent, the receiver can prove that the message was in fact send by the alleged sender. Similarly, when a message is received, the sender can prove the alleged receiver in fact received that message. [http://www.thestudymaterial.com]

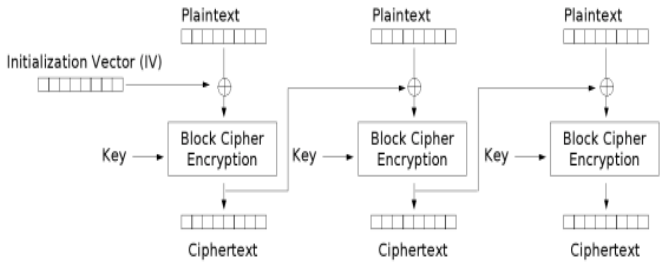
Block Ciphers and Stream Ciphers

An important distinction in symmetric cryptographic algorithms is between stream and block ciphers. [//www.cs.utexas.edu/~byoung/cs361/lecture45.pdf]

Stream ciphers :convert one symbol of plaintext directly into a symbol of cipher text ["http://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption_perf/"].



Block ciphers : encrypt a group of plaintext symbols as one block. ["Wikipedia"]



Cipher Block Chaining (CBC) mode encryption

Simple substitution is an example of a stream cipher. Columnar transposition is a block cipher. Most modern symmetric encryption algorithms are block ciphers. Block sizes vary (64 bits for DES, 128 bits for AES, etc.).

Stream Encryption :

Advantages: Speed of transformation: algorithms are linear in time and constant in space.

Low error propagation: an error in encrypting one symbol likely will not affect subsequent symbols.

Disadvantages:

Low diffusion: all information of a plaintext symbol is contained in a single cipher text symbol. Susceptibility to insertions/ modifications: an active interceptor who breaks the algorithm might insert spurious text that looks authentic.

Block Encryption:

Advantages:

High diffusion: information from one plaintext symbol is diffused into several cipher text symbols.

Immunity to tampering: difficult to insert symbols without detection.

Disadvantages:

Slowness of encryption: an entire block must be accumulated before encryption / decryption can begin.

Error propogation: An error in one symbol may corrupt the entire block .

Mode of Operations:

This section explains the two most common modes of operations in Block Cipher encryption-ECB and CBC- with a quick visit to other modes.

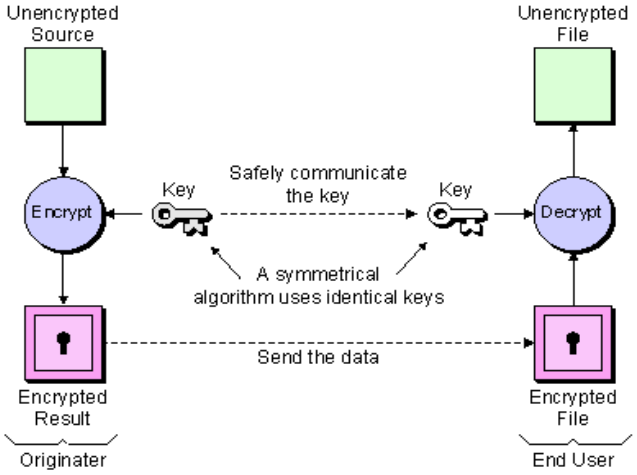
There are many variances of block cipher, where different techniques are used to strengthen the security of the system. The most common methods are: ECB (Electronic Codebook Mode), CBC (Chain Block Chaining Mode), and OFB (Output Feedback Mode). ECB mode is the CBC mode uses the cipher block from the previous step of encryption in the current one, which forms a chain-like encryption process. OFB operates on plain text in away similar to stream cipher that will be described below, where the encryption key used in every step depends on the encryption key from the previous step.

There are many other modes like CTR (counter), CFB (Cipher Feedback), or 3DES specific modes that are not discussed in this paper due to the fact that in this paper the main concentration will be on ECB and CBC modes ["http://www.cs.wustl"].

Symmetric and Asymmetric encryptions

Symmetric Encryption

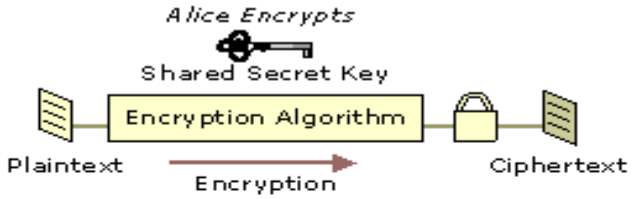
Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.



Asymmetric Encryption

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message ["http://support.microsoft.com/kb/246071"].

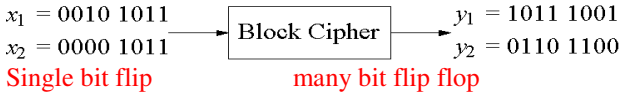


Compared Algorithms:

This section intends to give the readers the necessary background to understand the key differences between the compared algorithms.

DES: Up until recently, the main standard for encrypting data was a symmetric algorithm known as the Data Encryption Standard (DES). However, this has now been replaced by a new standard known as the Advanced Encryption Standard (AES) which we will look at later. DES is a 64 bit block cipher which means that it encrypts data 64 bits at a time. This is contrasted to a stream cipher in which only one bit at a time (or sometimes small groups of bits such as a byte) is encrypted ["http://cs.ucsb.edu/~koc/cs178/docx/w04x-des.pdf"].

Example:



3DES :

Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user-provided key into three sub keys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times, hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key ["http://www.vocal.com /cryptography/tdes/"].

AES:

The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector.

Blowfish: Blowfish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms.

3. Related Work Results:

The performance of the compared algorithms, this section discusses the results obtained from other resources. One of the known cryptography libraries is Crypto++ [Crypto++]. Crypto++ Library is a free C++ class library of cryptographic schemes. Currently the library consists of the following, some of which are other people's code, repackaged into classes.

Table 1 contains the speed benchmarks for some of the most commonly used cryptographic algorithms[1].

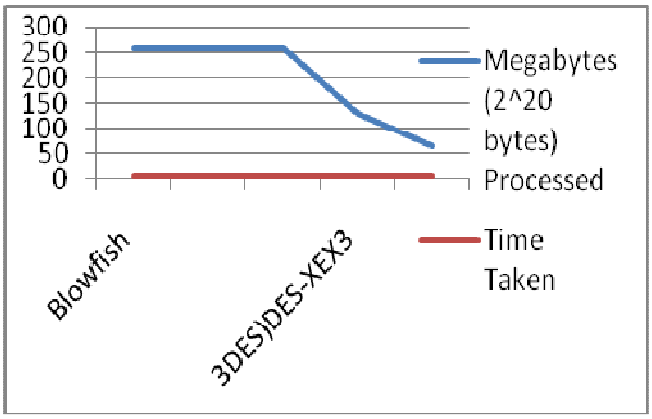
Algorithm	Megabytes (2^20 bytes) Processed	Time Taken
Blowfish	256	3.976
Rijndael (128-bit key)	256	4.196
Rijndael (192-bit key)	256	4.817
3DES)DES-	128	6.159

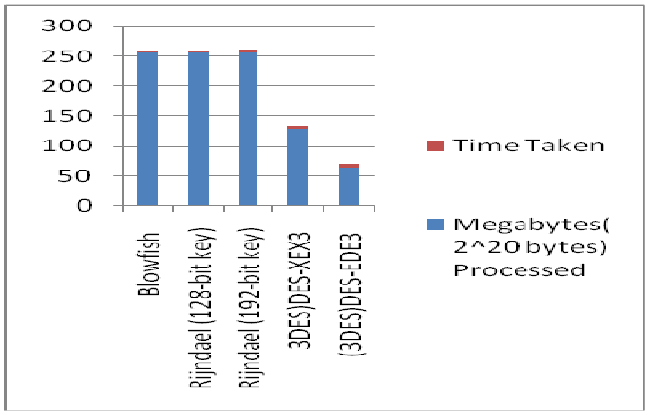
XEX3		
(3DES)DES-EDE3	64	6.499

Table 1 Comparison results using Crypto++

Algorithm	Megabytes (2^20 bytes) Processed	Time Taken
Blowfish	256	3.976
Rijndael (128-bit key)	256	4.196
Rijndael (192-bit key)	256	4.817
3DES)DES-XEX3	128	6.159
(3DES)DES-EDE3	64	6.499

Table 2 Comparison results using Crypto c#



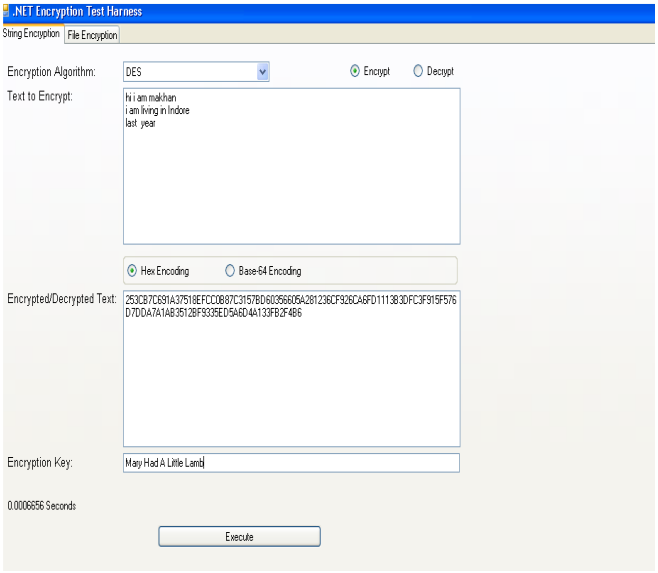


User load Against Request

I have also calculated user load Against request using Simulation application . which is same as Abdel-Karim Al Tamimi[1] .

4. Simulation Setup:

This section describes the simulation environment and the used system components. As mentioned this simulation uses the provided classes in .NETenvironment 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. The implementation uses managed wrappers for DES, 3DES and Rijndael available in System.Security.Cryptography that wraps unmanaged implementations available in Crypto API. These are DESCryptoServiceProvider, TripleDESCryptoServiceProvider and RijndaelManaged respectively. There is only a pure managed implementation of Rijndael available in System.Security.Cryptography,which was used[http //www.cse.wustl.edu].



References:

[1]. Abdel-Karim Al Tamimi " Performance Analysis of Data Encryption Algorithms".

[2]. Daeman and V.Rijmen. AES proposal: Rijndael, National Institute of Standards and Technology.

[3]. R.Chandramouli,"Battery Power aware encryption,"ACM transactions on information and system security (TISSEC), vol 9 no 2 pp.162-180

[4]. J.Daeman and V.Rijmen," Rijndael: The Advance Encryption Standard" Dr. Dobb's Journal pp.137-139.

[5]. D.Coppersmith,"The Data Encryption Standard (DES) and its strength against attacks,"IBM Journal of Research and development pp.243-250.

[6]. A. Nadeem and M.Y.Javed, "A performance comparison of data encryption algorithms," Information and communication technologies2005, pp-84-89.

[7]. "Crypt-Arithmetic Problems via Genetic Algorithm" in 2nd National Conference organized by Christian Eminent College, Indore on March 5, 2013.

[8]. Makhan Kumbhkar at el ,"A Comparative Study of E-Commerce and M-Commerce" , in 2nd National Conference organized by Christian Eminent College, Indore on March 5, 2013.

[9]. Makhan Kumbhkar at el ,"Performance Improvement of Software as a Service and Platform as a Service in Cloud Computing Solution" Vol-1,Issue-6 ISSN: 2320-7639.

