Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Comparative Analysis of Private Key Cryptography Algorithms: DES, AES and Triple DES

Sakshi Duggal[*], Vandana Mohindru
Department of CSE, Shoolini
University, Solan (H.P),
India

Pankaj Vadiya , Sachin Sharma
Department of CSE, Shoolini
University, Solan (H.P),
India

Abstract—Today's internet world is very competitive and to survive in such a competitive world there must be a secure environment to communicate. Internet and network applications are growing fast day by day. For this purpose there is a requirement of efficient and strong algorithm which will provide strong encryption and all these algorithms and encryption are part of cryptography. Cryptography is the field of network security which provides methods or algorithms to secure the information by hiding its meaning. It means that cryptography can convert the information from its readable form to unreadable form. If anyone tries to change or read information illegally than he cannot do so because the information is not readable until it is reconverted to readable form which is only possible by the mechanism of cryptography. And encryption is the process of converting plain text "unhidden" to "cryptic" text "hidden" to secure it against data thieves. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attack and its speed and efficiency is doing so. This paper provides a fair comparison analysis between three most common private key algorithms: DES, AES and Triple DES on the basis of execution time and data block size. Since main concern here is the performance of algorithms under different settings, the presented comparisons takes into consideration the behaviour and the performance of algorithm when different data loads are used. 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, Private key Cryptography, Public Key Cryptography, DES, AES, Triple DES, ECB, CBC, OFB, CFB.

I NTRODUCTION

With more than 188 million Americans connected with the internet [1], information security has turned into a top necessity. Numerous applications — electronic mail, electronic banking, medical databases, and electronic business — oblige the require of private information. For example, when taking part in electronic commerce, customers give visa numbers when purchasing items. In the event that the association is not secure, an attacker can without much of a stretch acquire this delicate information. With a specific end goal to execute a far reaching security plan for an offered system to surety the security of an association, the accompanying services must be given [2], [3], [4] those are confidentiality, authentication, data integrity and non-repudiation. There is a need of methods which provides all these functionalities together. Although it is very difficult to find out such methods, but cryptography can assure some/all of these features of a security algorithms. —cryptography is the field of network security which provides methods or algorithms to secure the information by hiding its meaning. It means that cryptography can convert the information from its readable form to unreadable form. If anyone tries to change or read information illegally than he cannot do so because the information is not readable until it is reconverted to readable form which is only possible by the mechanism of cryptography. 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.

In section 2 will give a brief overview of cryptography. Section 3 will discuss the comparisons of three algorithms. Section 4 will give the results of the research and provide discussion about the same. Finally, section 5 concludes this paper by summarizing the key points and other related considerations.

II OVERVIEW OF CRYPTOGRAPHY

The art and science of keeping messages secure is cryptography and it is practiced by cryptographers. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking cipher text; that is, seeing through the disguise. The branch of mathematics encompassing both cryptography and cryptanalysis is cryptology and its practitioners are cryptologists. The goals of cryptography are:

- **Confidentiality**: Keeping messages secret.
- **Authentication**: verifying the message's source.
- **Integrity**: assuring that a message has not been modified.
- **Key management**: distributing the secret "keys" for cryptographic algorithms

Cryptographic algorithms used to ensure confidentiality fall within one of two categories:

- **Private-key Cryptography**(also known as Symmetric-key Cryptography)
- **Public-key Cryptography**(also known as Asymmetric-key Cryptography)

A. *Private key Cryptography*

Private key encryption is a form of cryptosystem in which encryption and decryption are performed using the same key.[5] This is also known as conventional encryption, single key, secret key, shared key, one-key and Symmetric key. Private Key transforms plaintext into cipher text using a secret key and encryption algorithm. Using the same key and decryption algorithm, the plaintext recovered from the cipher text.

There are two types of private key encryption algorithms: stream cipher and block ciphers which provide bit-by-bit and block encryption respectively. Following are the some most common symmetric/secret key cryptographic algorithms:

- DES: Data Encryption Standard
- Triple DES: Triple Data Encryption Standard
- AES: Advanced Encryption Standard/ rijndael
- IDEA: International Data Encryption Algorithm
- RC4: Rivest Cipher4
- BLOWFISH

With this form of cryptography, it is evident that the key must be known to both the sender and the receiver; that, actually, is the secret. The greatest trouble with this approach, obviously, is the distribution of the key.

B. *Public key Cryptography*

Public key encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys – one a public key and one a private key. [5] It is also known as asymmetric key. The approach called asymmetric key cryptography evolved to address the security issues posed by symmetric key cryptography. This method tackles the issue of secret key cryptography by utilizing two keys rather than a single key. Asymmetric cryptography [7] utilizes a pair of keys. In this process, one key is utilized for encryption, and the other key is utilized for decryption. This process is known as asymmetric cryptography because the keys are required to finish the process. These two keys are collectively known as the key pair. In asymmetric cryptography, one of the keys is openly distributed. This key is known as public key and is utilized for encryption. Subsequently, this method for encryption is additionally called public key encryption. The second key is the secret or private key and is utilized for decryption. The private key is not distributable. This key, in the same way as its name recommends, is private for each communicating entity.

In the public key cryptography, the information that is encrypted with public key must be decrypted with the corresponding private key. Alternately, data encrypted with the private key must be decrypted with the relating public key. Because of this asymmetry, public key cryptography is known as asymmetric cryptography.

Many public key algorithms were developed on the basis of the concept of public key cryptography. The most widely used public key algorithms include:

- RSA (Rivest, Shammir, and Adleman)
- Diffie-Hellman
- ElGamal
- Digital Signature Standard
- Elliptic Curve Cryptography.

C. *Private and Public key Comparison*

Private Key encryption it is also called as symmetric key or 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. Public key encryption it is also called as asymmetric 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 mean. IN other words, data encrypted by one public key can be encrypted only by its corresponding private key. The private or symmetric key encryption is a cryptography technique that uses a shared secret key to encrypt and decrypt the data. Symmetric encryption algorithms are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms. Public key encryption techniques are about 1000 times slower than Symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique [8]. As shown in figure 1 Private Key cryptography scheme are generally categorized as being either stream cipher or block cipher. Stream ciphers work on a single bit (byte or computer word) at a time and implements some type of feedback mechanism with the goal that the key is always showing signs of change. Stream ciphers [6] come in a few flavours yet two are worth mentioning here. Self-Synchronizing stream ciphers calculate every bit in the key-stream as a function of the past n bits in the key-stream. It is termed "self-synchronizing" on the grounds because the decryption procedure can stay synchronized with the encryption transform only by knowing how far into the n-bit key-stream it is. One issue is error propagation; a confused bit in transmission will bring about n garbled bits at the receiving side.

Synchronous stream ciphers generate the key-stream in a manner autonomous of the message stream however by utilizing the same key-stream generation function at sender and receiver. While stream ciphers don't propagate transmission errors, they are, by their nature, periodic so that the key-stream will eventually repeat.

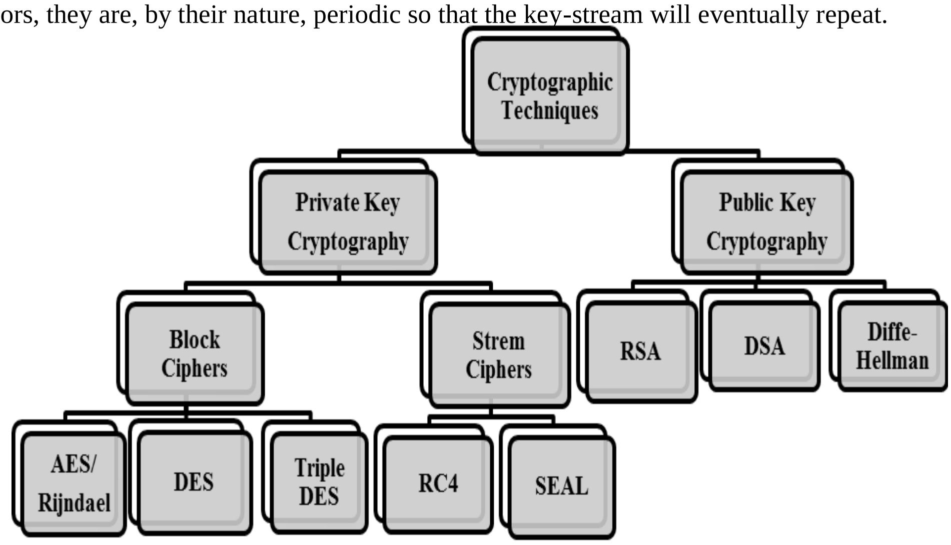

Figure 1: The classification of major encryption techniques is shown in.

A block cipher is alleged on the grounds that the scheme encrypts one block of data at once utilizing the same key on each block. By and large, the same plaintext block will dependably encrypt to the same cipher content when utilizing the same key as a part of a block cipher in as much as the same plaintext will encode to distinctive ciphertext in a stream cipher. Block ciphers can operate in one of several modes. The following are the four most important modes:

- ECB: Electronic Codebook
- CBC: Electronic Codebook
- CFB: Cipher Feedback
- OFB: Output Feedback

D. *Modes of Operations*

Block ciphers [10] can operate in one of several modes; the following four are the most important:

- **Electronic Codebook (ECB) mode** is the simplest, most important application: the secret key is used to encrypt the plaintext block to form a cipher text block. Two identical plaintext blocks are used and they always generate the same cipher text block. Although this is the most basic mode of block ciphers, it is susceptible to a variety of brute-force attacks.
- **Cipher Block Chaining (CBC) modes** add a feedback mechanism to the encryption scheme. In CBC, the plaintext is exclusively-ORed (XORed) with the previous cipher text block to increase encryption. In this mode, two identical blocks of plaintext never encrypt to the same ciphertext.
- **Cipher Feedback (CFB) mode** is a block cipher implementation as a self-synchronizing stream cipher. CFB mode allows data to be encrypted in units which are smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input. If we were using 1-byte CFB mode, for example, each incoming character is placed into a shift register the same size as the block, encrypted, and the block transmitted. At the receiving side, the ciphertext is decrypted and the extra bits which are present in the block are discarded.
- **Output Feedback (OFB) mode** is a block cipher implementation whose concept is similar to a synchronous stream cipher. OFB protects the same plaintext block from generating the same ciphertext block by using an internal feedback mechanism which is independent of both the plaintext and cipher text bit-streams.

E. *Applications of Cryptography*

By now, various cryptography techniques and their advantages and disadvantages are discussed above. Now it is time to take a look at the implementation of cryptography to provide basic security features, which are, confidentiality, integrity, authentication, and non-repudiation.

All these security features can be provided by using any one of the following methods:

- Message encryption
- Message Authentication Code (MAC)
- Hash functions

III . COMPARED ALGORITHMS

A. *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.

B. *Triple DES*:

As an enhancement of DES, the3DES (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 leve1. But it is a known fact that Triple DES is slower than other block cipher methods. Triple DES was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56), beyond the reach of brute-force techniques such as those used by the EFF DES Cracker. Triple DES has always been regarded with some suspicion, since the original algorithm was never designed to be used in this way, but no serious flaws have been uncovered in its design, and it is today available cryptosystem used in a number of Internet protocols.

C. *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.

IV RESULTS AND ANALYSIS

With the end goal of dissection and correlation of the algorithms the algorithms are simulated (designed) in JAVA programming language. Simulation utilizes the gave classes within java environment to simulate the execution of DES, AES and Triple DES. The execution utilization oversaw wrappers for DES, AES and Triple DES accessible in java.cypto and java.security [11] that wraps unmanaged executions accessible in JCE (Java Cryptography Extension) & JCA (Java Cryptography Architecture).the Cipher class gives the usefulness of a cryptographic Ciphers utilized for encryption and decryption. It structures the center of the JCE framework.

This section will examine the results which are acquired by running the simulation program utilizing diverse data loads. The results indicate the effect of changing data load on every algorithm and the effect of Cipher Mode utilized. The results are gotten for the diverse data loads given by the user. The execution times for these distinctive data loads are computed inside the simulation program and showed. At that point the results are changed over to the graphs in Microsoft Excel and the analysis is carried out. The assessment is intended to assess the results by utilizing block ciphers. Henceforth, the load data (plaintext) is separated into smaller block size measure according to algorithm settings.

A. *Performance Result with ECB Mode*

The first set of experiments were conducted using ECB mode, the results are shown in figure 2 below.

The results show that there is less contrast between the execution times of the three algorithms however as we expanding the data loads the execution time likewise expanding in the equivalent ratio for each of the three algorithms.

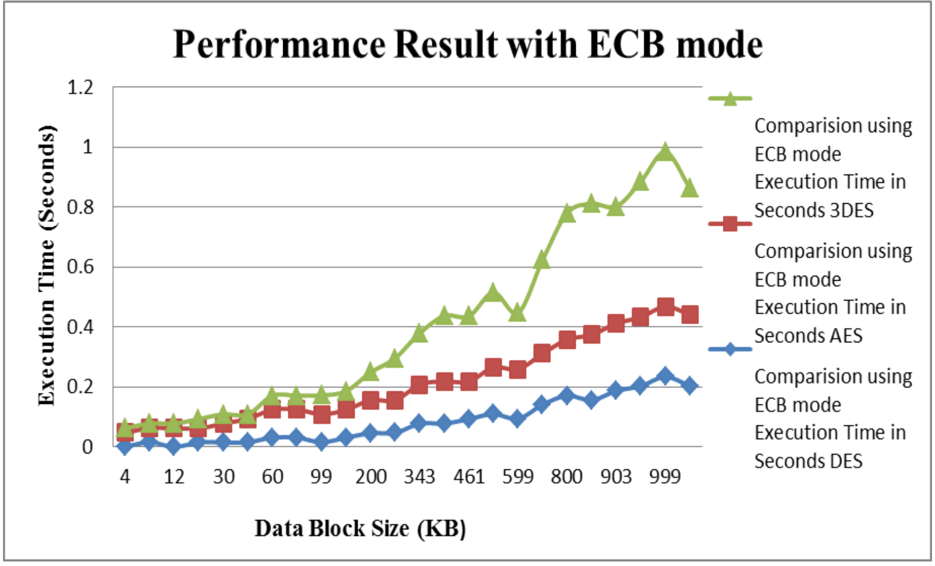

Figure 2: Performance Results with ECB mode

At starting moment that the data block size is less that is between 4 KB to 99 KB there is very little contrast in executing time as the block size builds from 150 KB or more than their is variety in the execution time of these three algorithms. In the wake of acquiring the data in the table the graph of the data is structured by utilizing the Microsoft Excel graph establishment. DES algorithm is great over other two algorithms that are AES and Triple DES regarding the processing time and speed is acquired. Furthermore AES devours more assets and additionally preparing time when the information data size is moderately greater than DES however AES is most secure algorithm out of all.

B. Performance Results with CBC:

The second set of experiments were conducted using CBC mode, the results are shown in figure 3 below.

It could be seen from the data acquired that again there is less distinction between the execution times of the three algorithms the expanding data loads brings about expanding execution time. It can likewise be seen that utilizing the CBC mode of Operation additional time is added to the execution of the three algorithms.

At starting moment that the data block size is less that is between 4 KB to 150 KB there is very little contrast in execution time. As the block size builds yet it is small to the point that it could be seen barely be bare eyes. As the block size expands from 200 KB or more than there is variation in the execution time of these three algorithms. At the same time as the CBC is more secure than ECB, it is favoured over ECB. Additionally, CBC is useful for little provisions and in addition for medium size of requisitions. As the data loads builds the speed of algorithm by utilizing this mode diminishes. In the wake of acquiring the information in the table the graph of the data is structured by utilizing the Microsoft Excel chart establishment. DES algorithm is great over AES and Triple DES algorithm as far as the processing time and speed is acquired. What's more AES devours more assets and additionally processing time when the data block size is moderately enormous however AES is most secure algorithm out of all.

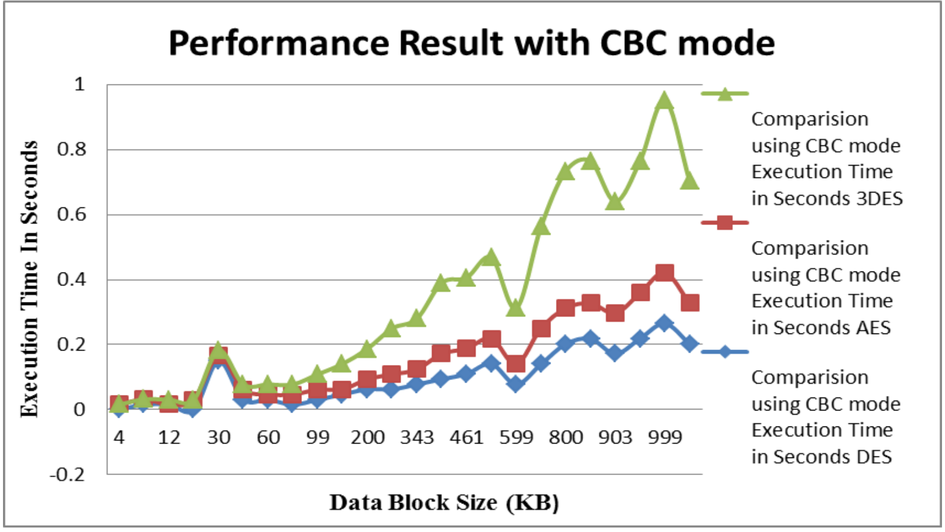

Figure 3: Performance Results with CBC mode

C. Performance Result with OFB mode:

The third set of experiments were conducted using OFB mode, the results are shown in figure 4 below. The results acquired are such a great amount of indistinguishable to the past modes clarified. Yet as OFB mode is a block cipher execution thoughtfully like a synchronous stream cipher, OFB keeps the same plaintext obstruct from creating the same cipher text block by utilizing an inside input component that is free of both the plaintext and cipher text bit-streams. Thus, it is included some additional normal time of execution for every algorithm.

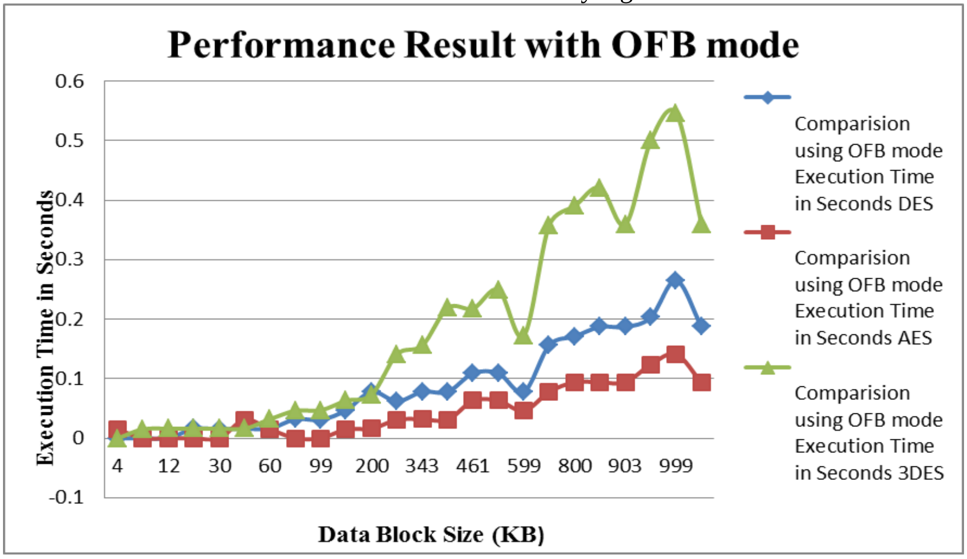

Figure 4: Performance Results with OFB mode

In the wake of getting the data in the table the graph of the information is framed by utilizing the Microsoft Excel graph shaping. AES algorithm is great over DES and Triple DES algorithms as far as the processing time and speed is acquired. Also AES expends less resources and less processing time when the data block size is moderately enormous and AES is most secure algorithm out of all

D. Performance Result with CFB mode:

The fourth set of experiments were conducted using CFB mode, the results are shown in figure 5 below.

The results acquired are much indistinguishable to the past modes clarified. At the same time as CFB mode is a block cipher usage as a synchronizing toward oneself stream cipher. CFB mode permits data to be encrypted in units littler than the block size, which may be valuable in a few provisions, for example, encryption intelligent terminal info. The table underneath shows the processing time needed to process different data loads. At initial point when the data block size is less that is between 4 KB to 150 KB there is not much difference in execution time as the block size increases from 200 KB and above than there is large variation in the execution time of these three algorithms. In the wake of getting the data in the table the graph of the data is shaped by utilizing the Microsoft Excel graph structuring. DES algorithm is great over AES and Triple DES algorithms regarding the processing time and speed is gotten. What's more AES devours more resources and additionally processing time as contrast with DES when the data block size is generally enormous yet AES is most secure algorithm out of all.

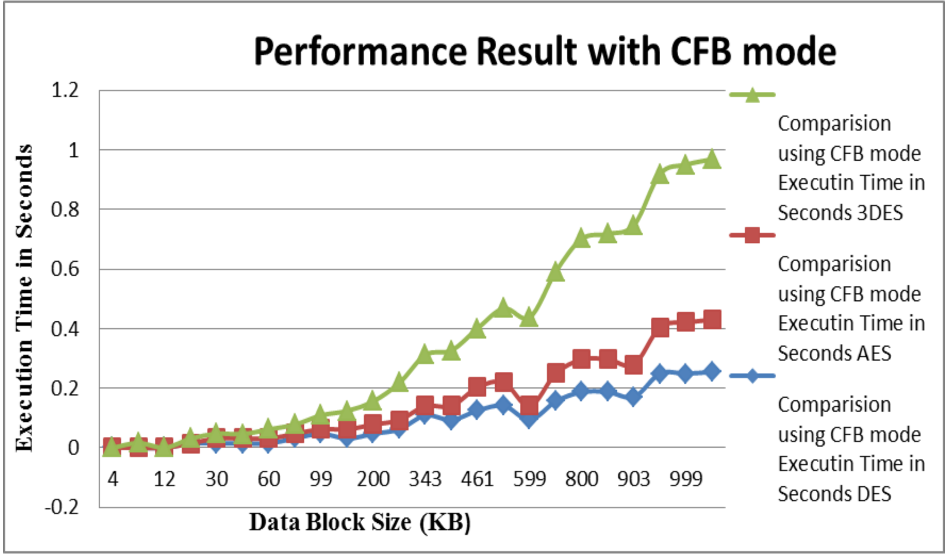

Figure 5: Performance Results with CFB mode

V CONCLUSION AND FUTURE SCOPE

The simulation of three private key algorithms i.e. DES, AES Triple DES based on two fundamental attributes key size and block size which shows that DES algorithm is great over AES and Triple DES algorithms regarding the processing time and speed is gotten. AES consumes more resources and additionally processing time as contrast with DES when the data block size is generally enormous yet AES is most secure algorithm out of all. In future we can also perform analysis between the private key cryptography algorithms on the premise of block ciphers and stream ciphers. Also work will investigate this idea and blend of algorithms will be examined and could be executed in better simulator to show signs of improvement comes about by utilizing diverse modes of operations. This examination is possible in an alternate simulator by thinking seriously about networking to show which algorithm performs better in system.

REFERENCES

[1] P. Gil. How big is the Internet? World Wide Web —http://netforbeginners.about.com/cs/technoglossary/f/FAQ3.htm, 2005.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, Boca Raton, Florida, USA, 1997.

[3] B. Schneier. Applied Cryptography. John Wiley & Sons Inc., New York, USA, 2nd edition, 1996.

[4] W. Stallings. Network and Internetwork Security – Principles R. Nicole, "The Last Word on Decision Theory," J. Computer Vision, submitted for publication.

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

[6] 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.

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

[8] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.

[9] A.W.Naji, A.A.Zaidan, B.B.Zaidan, Shihab A, Othman O. Khalifa, " Novel Approach of Hidden Data in the (Unused Area 2 within EXE File) Using Computation Between Cryptography and Steganography International Journal of Computer Science and Network Security (IJCSNS) , Vol.9, No.5 , ISSN : 1738-7906, pp. 294-300.

[10] 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.

[11] E.E. Reber, R.L. Michell, and C.J. Carter, "Oxygen Absorption in the Earth's Atmosphere," Technical Report TR-0200 (420-46)-3, Aerospace Corp., Los Angeles, Calif., Nov. 1988. (Technical report with report number)

[12] L. Hubert and P. Arabie, "Comparing Partitions," J. Classification, vol. 2, no. 4, pp. 193-218, Apr. 1985. (Journal or magazine citation).

[13] R.J. Vidmar, "On the Use of Atmospheric Plasmas as Electromagnetic Reflectors," IEEE Trans. Plasma Science, vol. 21, no. 3, pp. 876-880, available at http://www.halcyon.com/pub/journals/21ps03-vidmar, Aug. 1992. (URL for Transaction, journal, or magzine).

[14] J.M.P. Martinez, R.B. Llavori, M.J.A. Cabo, and T.B. Pedersen, "Integrating Data Warehouses with Web Data: A Survey," IEEE Trans. Knowledge and Data Eng., preprint, 21 Dec. 2007, doi: 10.1109/TKDE.2007.190746.(PrePrint).