Security Framework for Distributed Database System

Abstract

This research aims to study various Symmetrical Algorithms, while the main objective of this study is to find out a suitable algorithm for the encryption of any specific size of text file where the experiment of each algorithm is based on encryption of different sizes of the text files, which are in "10 KB to 5 MB", and also to calculate the time duration that each algorithm takes to encrypt or to decrypt the particular size of each text file. There are many types of encryption algorithm, which can be used to encrypt the computerized information in different Organizations, whose all algorithms can encrypt and decrypt any size of text file, but the time duration of each Algorithm during the encryption or decryption process of specific file size is not fixed. Some of the algorithms are suitable for encryption of specific ranges of the file size, or some of algorithms are functional while encryption small size of files, and others algorithms are functional for encryption of big size of text files, based on the time duration disparity among symmetric algorithms during encryption of text files. In this study five symmetrical algorithms are merged in one program using classes and concept of inheritance in the form that if encryption is needed, the program will select the file and it checks the size of the text file. After this process the program automatically will select the suitable encryption algorithm to encrypt the specific text file according to the range of the file size. Knowing that the file size before or after encryption will not change or is stable, in this case of the decryption algorithm will apply the same process of encryption while decrypting files, the program of encryption and decryption code will write using visual Studio 2013. The result will be analyzed with R program (R software), the cipher text will appear in the format of UTF8 which means Unicode Transformation Format, "8" Means "8" bits to represent a character, the size format that will apply in the program will be in format of KB (kilo Byte).

Keywords

Cryptography, Encryption, Decryption, Time Duration, AES, DES, 3DES,

Rijndael, RC2

1. Introduction

Nowadays the requirement for keeping information secure is increasing. The concept of secure communication is not only for the government institutions but also for the private sectors such as organization, education and business projects. The transmissions of information over the network are becoming widely used in many parts of the world which will make the world more connected. To keep communication system secure or to provide a security for the data in computer there are many cryptographic algorithms which can be use to provide a good security, some of them are similar while securing a small size of information and others are good for big size of data.

With the increase in the progress of the technology in the world of communication, Cryptography has become very important for securing the information during transmission, so it protects information against active and passive attack. Cryptography is an algorithm progress which can be used to protect information according to certain key which can be known only between the sender and receiver. In this study I may explain the knowledge of cryptography algorithm and its function in encryption and decryption data.

The essential concept in all communications is that there must be three parts for the communication in order to be effective: First there must be two users or more, a sender and a receiver, they may have something to share between them. The second part of the communication is a medium which is the channel of the communication that is used for transmitting of the data between sender and receiver. The third part is a set of communication rules and protocols.

1.1. Problem of the Study

The following points are the problems of the study:

1) Hackers always attack and destroy the data in system through the security gaps.
2) Lack of finding suitable algorithm for the encryption or decryption of a specific range of the text file size.
3) All algorithms are not suitable for the encryption or decryption any size of the text file.
4) The time durations that each symmetrical algorithm takes to encrypt or decrypt text different files are not similar.

1.2. Important of the Study

The important of this study focus on the following points:

1) The main point of this study is to compare several symmetrical algorithms such as “AES, DES, TDES, RC2, Rijndael” and to find out the best algorithm

according to the time duration that each algorithm takes to encrypt or to decrypt a text file.

2) To adjust all the above mentioned algorithms according to the ability of the time duration that each algorithm takes to encrypt or decrypt a specific size of the text file.
3) To combine all the above mentioned algorithms in one program, so that the program could select a suitable orithm while encrypting or decrypting the text file based on the size of the text file.

1.3. Objectives of the Study

The objectives of this study are as follows:

1) To study different symmetrical algorithms techniques.
2) To find out the time duration that each algorithm takes to encrypt or decrypt different size of the text file so that Programmers need not to reinvent the wheel each time to develop a new application.
3) Create a positive cryptography culture for text file.

2. Related Works

For the more prospective about the performance of the cryptographic algorithms (encryption algorithms), this section explains and describes the previous works applied in the field of data encryption, the concept takes into consideration is a process of speed, throughput power consumption, a valance, data type, and data size. It also explains the findings obtained for several cryptography algorithms.

Shailja Kumari and Jyoti Chawla [1] found that AES (Rijndael) is the most secure symmetric algorithm, it is also better and faster among all the algorithms which have been used in their study, and there is no serious weaknesses in AES (Rijndael) algorithm, there are many gaps of security in symmetric algorithms such as insecure transmission of secret key, weak keys, flexibility, speed, reliability and authentication in IDEA algorithm, it involves large class of weak keys facilitating the cryptanalysis for recovering the key, they also found that the Blowfish exposed to a differential attack against its certain variants, it is also slow in speed but much more faster than (IDEA) International Data Encryption Algorithm. Consistent with my present results, they have used various cryptographic algorithms in order to compare between them and to find the much secure algorithm, with consideration of speed also. Inconsistent with my present findings, Shailaj and Jyoti reported that their comparison was in the role of weak key, flexibility and reliability, they decided that AES (Rijndael) was the best in term of security performance, flexibility, and memory usage.

Mohiuddin Ahmed *et al.* [2] they have talked basically in their paper about "cryptographic technique", under title "Cryptography and State-of-the-art Techniques", they explained that there are constant improvements of data security and information storage systems but still cryptography techniques need to be more strong and agile. They recommended that in the future the cryptogra-

phy should be implemented in image processing and storage systems.

Tannu Bala and Jogesh [3] they have found that security is very important and powerful for the computerized information in the terms of networking and internet, and various communication systems. The paper was under the title "Asymmetric Algorithms and Symmetric Algorithms". The role of their studies was the comparison of different symmetric algorithms (DES and AES), Asymmetric algorithms (RSA and Elgamal), and they recommended that AES algorithm is better while using symmetric algorithms, however Elgamal is powerful while securing the information in asymmetric algorithms. In the future plan they recommended that algorithms will improve to provide more powerful security system.

2.1. The Meaning of Security

William Stallings and Lawrie Brown [4] the security provided to an automated information system in order to achieve the applicable goals of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications). Amandeep Kaur and ShaijaKumari [5] the security of the information has become a public issue in the world of the computerize data, encryption of the information has paramount important in the environment of cryptography.

2.2. Encryption Methods

Villanovaau [6] in practice, asymmetrical and symmetrical encryption often work together for maximum speed and security. Public key encryption starts a session and transfers a shared-secret key used for the remainder of the session. Digital signatures can be used to verify the sender of a message in environments where holders of public and private keys can be trusted. Jan C. A. Van Der Lubbe [7] we can distinguish two types of classical cipher system.

2.3. Transposition System

Jan C. A. Van Der Lubbe [7] transposition cipher is based on changing the sequence of the character of the plaintext, a substitution cipher does not alter the order of the characters of the plaintext, but it replaces the original with others.

3. Materials and Methods

3.1. Cryptography Algorithms

Five symmetrical algorithms techniques have been used in this study, they are as follows: "Rijndael, RC2, AES, DES, and TDES".

3.2. Rijndael Algorithm

MIDNI and Kevin Lee [8] the Rijndael algorithm was built up by John Daemen and Vincent Rijmen, two of them are from Belgium. The Rijndael algorithm was submitted to the National Institute of Standards and Technology (NIST) in 1998.

It was created in order to improve an Advance Encryption Standard algorithm (AES), which was designed to achieve the main three objectives which are speed, code compactness on a wide range of platform, all known attacks and design simplicity. Rijndael is symmetric block cipher algorithm, it support 128 bit block size with key length of 128,192 and 256 bit.

3.3. RC2 Algorithm "Reverts Cipher"

Sheetal Charbathia and Sandeep Sharman [9] Rc2 in the leap of Rc1, RC1 was not published, it was the initiative process which Rivets used to processed a series of designing the symmetric key algorithm, RC was stands for Reverts Cipher algorithm, variants version of RC was design by several researchers in order to create a symmetric key algorithm that can gives well protection for the users data, which can share over network. RC2 also known (ARC2), it stands for Rivest's code, it is a symmetric block cryptography algorithm developed in 1998, RC2 was proposed and considered for the replacement of DES (Data Encryption Standard), if use a variable size in range of 1 - 128 bytes, RC2 is secret key block encryption algorithm, it consists of input and output block size of 64 bit, it was created to be implemented on 16 bit microprocessor. If the key encryption has been performed, then RC2 algorithm runs twice fast than DES on IBM AT. It consists of three further algorithms (Key Expansion, Encryption, and Decryption).

3.4. AES "Advance Encryption Standard"

Shailja Kumari and Jyoti Chwal [10] AES is a block cipher algorithm that uses 128 bit plaintext with 10, 12, 14 or 14 round, it is a symmetric key algorithm base on the festal structure, and variable key length of 128,192,256 bit permuted into 10 sub-keys each of 128,192,256 bit length respectively, it only contains a single X-box and same algorithm also use for decryption. The concept of security on AES deal with its variables nature key size, which can allow up to a key size of 256-bit to provide protection against future attack (potential quantum computing algorithm and collision attack). Priyadarshini Patil *et al.* 2015 AES algorithm stands for (Advance Encryption Standard), it was upgraded by Vincent Rijmen and Joan Daemen in 1998, AES supports any combination of key and data length of 128, 192 and 256. It is a symmetric key block cipher, AES algorithm can let a 128 bit data length that can separate into four basic operational blocks which is known as array of bytes and organized as a matrix of the order of (4×4).

3.5. TDES "Triple Data Encryption Standard"

Vocal [11] TDES stands for Triple Data Encryption Standard, it was developed base on the DES (Data Encryption Standard) covered the same advantages of proven precision and long key length which can ignore unauthorized users and can be used to reduce the time takes to break DES, it also three times slower than DES, but more secure if used properly, TDES takes three 64 bits keys for an

overall key length of 192 bits.

3.6. Cryptography Format: Unicode

Julie D. Allen [12] The Unicode standard is the universal character encoding standard for written characters and text, it introduces accord path of encoding multilingual text that allows the replacement of text data internationally and generates the foundation for global software. The Unicode standards bring the supporting for the world wide web and global environments of today, Unicode standard wanted new internet protocols and implemented in each modern computer languages and operating systems such as C#, Java.

3.7. The Importance of the Unicode

Interproinc [13] the mechanism of Unicode could support more regionally popular encoding system such as ISO-8859, different languages in Europe, shift-JIS in Japan, or BIG-5 in China.

Unicode Standard 2018 The mechanism of Unicode standard specifies codes for the characters used in all the major languages written, scripts include the middle Eastern right to left scripts, European alphabetic scripts and many scripts of Asia, it also include mathematical symbols, punctuation marks, arrows, technical symbols, emoji, etc. Unicode contains code for diacritics. Unicode standard version 9.0 extends codes for more than 135,000 characters from the world's alphabets.

3.8. Logical Order

Unicode Standard [14] The text in Unicode order is stored representation is called logical order, this order almost match to the order in which text is typed in via the keyboard order often match to simple linear progression of characters in one direction such as from left to right or right to left or from top to bottom.

Figure 1 presents the ordering of the text before and after encryption process in UTF format.

3.9. Details of File after Encryption Process

Before encryption or decryption process the program will present to user a message that contains the information of the cryptography process which has shown in Figure 2.

Figure 1. Bidirectional ordering in unicode (Wesley, A. [15]).

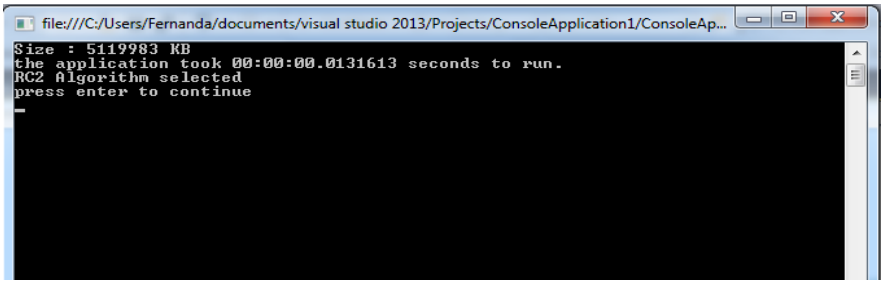

Figure 2. Details of file after encryption process.

4. Results and Discussion

4.1. The Analysis of Results

Different sizes of text files have been encrypted and Decrypted using AES algorithms, the result of the implementation of AES has been compared with various algorithms such as "DES, TDES, RC2 and Rijndael". The concept of the compression was upon the time duration that each algorithm can take to encrypt and to decrypt the different sizes of text files. The basic purpose of the statistical analysis in the duration time that all algorithms take to encrypt or to decrypt text files with various sizes to compare and to fine out the suitable algorithm that can be used to encrypt and to decrypt text file automatically according to range of the files sizes, the differentiation applied between five symmetrical algorithms, and they are "AES, DES, TDES, RC2 and Rijndael", and the different size of the text files which have been used in all algorithms are "10 KB, 20 KB, 50 KB, 1 MB, 2 MB, 5 MB". The analysis provided specific time duration for each algorithm that can be needed to encrypt and decrypt text files in the different sizes as follows.

4.1.1. The Results of Encryption and Decryption Process (File Size 10 KB)

It contains different time durations that each algorithm takes to encrypt and decrypt the text files.

Figure 3 refers to the encryption of 10 KB of text in various algorithms, which are shown in Table 1, it also explains the time duration that each algorithm takes to encrypt 10 KB of text file, in the role of bar plot, base in the analysis of the chart, the suitable algorithm to encrypt 10 KB of text file sorting ascending are AES with time duration 0.0424464, then TDES with 0.04615448, Rijndael with 0.0612135, DES with 0.1260590 and on the other hand the worst one for Encryption of 10 KB text file is RC2 with time duration 0.1533708, while other chart explains the performance of the time duration in the forms of plots connected with lines. Consistent with this present study findings, Prof. N. Penchalaish and Dr. R. Seshadri 2010 [16] reported the effective coding of Rijndael algorithm, Advance Encryption Standard (AED) in hardware description language, they analyzed the structure and designed a new AES. The implementation aspect of Rijndael cipher and its inverse are treated, Thus although Rijndael is

well suited to be implemented efficiently on a wide range of processors and dedicated hardware. The inconvenient with the present study findings, the compression was in the role of following points:

1) Resistance against all known's attacks.
2) Speed and code compactness on wide rangers of platforms.
3) Design simplicity, as well assist similarities and dissimilarities with other symmetric cipher.

The current study offered the result of suitable time duration for several algorithms while encrypting and decrypting various sizes of different text files.

Figure 4 shows the time duration for each algorithm within Table 2 and the time duration that each algorithm takes to decrypt 20 KB of text file in the sequence of bar plot, based in the graph analysis in which the best algorithm is TDES, then comes AES, RC2, DES, and the worst one is Rijndael for encrypting 20 KB of text file. The other shape views the result of analysis in plot point connected with lines.

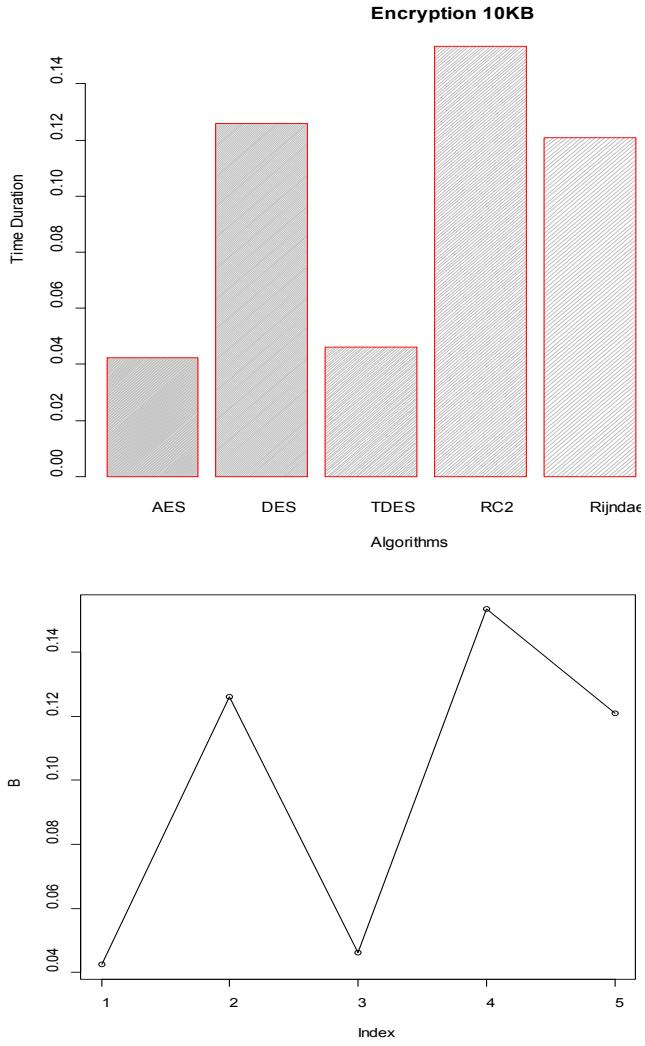

Figure 3. Charts of the encrypt process of 10 KB text file.

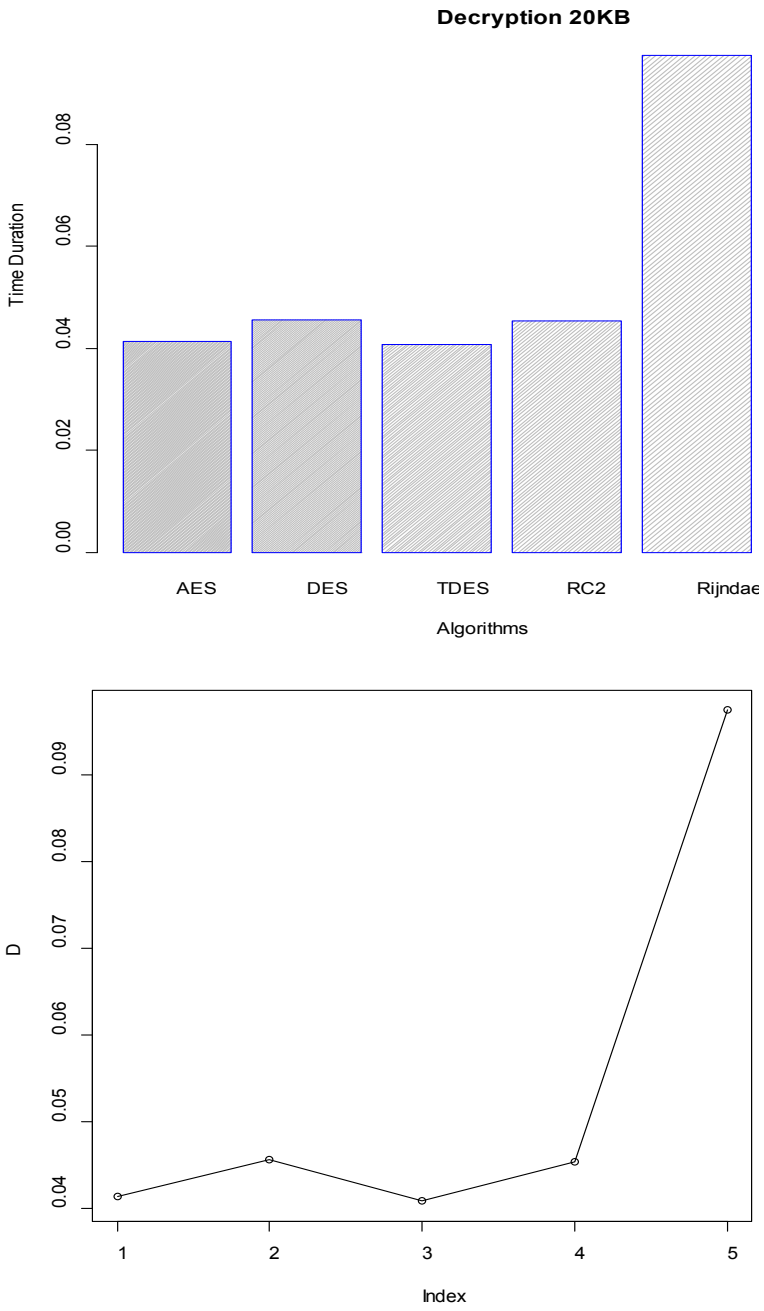

Figure 4. Charts of the decrypt process of 20 KB text file.

Table 1. The results of encryption and decryption process (file size 10 KB).

Algorithms	Key Size-UTF8	File Size	Encryption Time	Decryption Time
AES	8 bits	10 KB	0.0424464	0.0193348
DES	8 bits	10 KB	0.1260590	0.0424130
TDES	8 bits	10 KB	0.0461548	0.0684244
RC2	8 bits	10 KB	0.1533708	0.0335696
Rijndael	8 bits	10 KB	0.1209827	0.0612135

Table 2. The collection results of encryption various sizes of text file and time duration for all algorithms.

File Size	AES	DES	TDES	RC2	Rijndael
10 KB	0.0424464	0.1260590	0.0461548	0.1533708	0.1209827
20 KB	0.0768004	0.1252783	0.1501058	0.2529029	0.1191877
50 KB	0.0458027	0.1071282	0.1273674	0.1430795	0.1266462
1 MB	0.1590523	0.1543060	0.3361274	0.1747218	0.1979381
2 MB	0.2439729	0.1823020	0.3248482	0.1656537	0.2094957
5 MB	0.6157387	0.4499778	0.5217788	0.3556123	0.3387679

4.1.2. The Collection Results of Encryption Various Sizes of Text File and Time Duration for All Algorithms in the Role of Encryption Process

The table describes the collection of all algorithms which have been used in the study and their performance of time duration that each of them can take to Encrypt various sizes of text file, and those algorithms are "AES, DES, TDES, RC2, and Rijndael", including different sizes of text files which are implemented in each algorithm and the sizes are "10 KB, 20 KB, 50 KB, 1 MB, 2 MB, and 5 MB".

Figure 5 explains the time duration that each algorithm takes to Encrypt text file with different sizes, while all details of algorithms, file sizes, and time durations are shown in Table 2, after implementation of different sizes of text file in each algorithm, the out lines is that only one algorithm can be used to encrypt and decrypt specific text file, but all algorithms are not suitable for Encryption of any size of text files. Some of them are suitable for small sizes of text files and others are suitable for the big sizes of text files. Based on the statistic results and analysis that have been applied in the study, which has concentrated in the ability of performance of each algorithm in the form of encrypting different sizes of text files, and the time duration that each of them takes to encrypt various sizes of text files, the outlines of the analysis study in the performance of each algorithm in the Encryption of different sizes of text file is based on the priority of small size of text files, which sorted ascending (AES, TDES, DES, RC2, Rijndael), known that "AES" is suitable for encryption small size of the text file.

5. Recommendation and Further Work

Based on the findings of the study, different symmetric algorithms have been implemented in the study in order to find a suitable algorithm for the encryption or decryption of the specific size of the text file, and due to the results of the study, some of the algorithms are effective while encrypting small sizes of the text file and some of them are good for largest sizes of the text file. The study covered only the format of text file (.txt), it can be expanded to cover format of different types of files with different format rather than one format only, this study can be developed in order to contain more encryption algorithm instead of five algorithms.

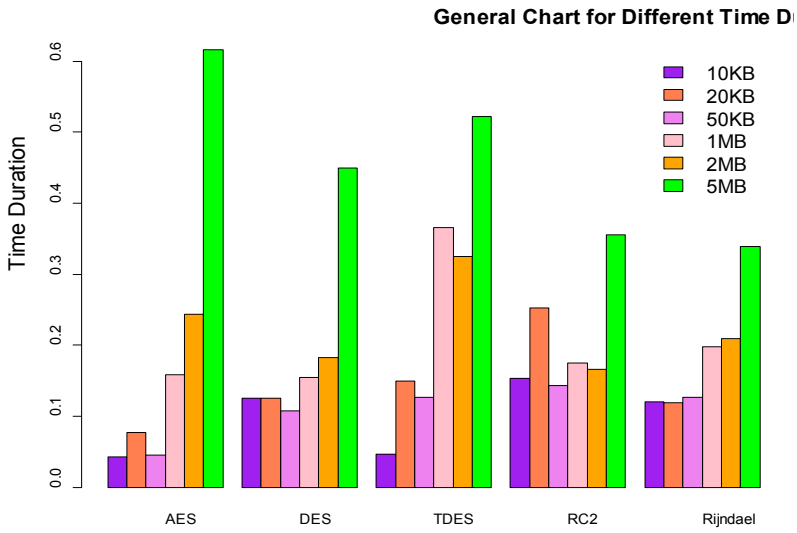

Figure 5. Chart of the collection of encryption process for various sizes of text file and time duration for all algorithms.

6. Conclusions

Five symmetrical cryptographic algorithms have been used in this study, and each algorithm has been used for encryption and decryption of different sizes of the text files, the sizes are "10 KB, 20 KB, 50 KB, 1 MB, 2 MB, 5 MB". The main concept of the study is on the role of time duration that each algorithm takes to encrypt and decrypt text file in particular, after applying this process for the all algorithms which has been used in the study, and the result was in the term of various time durations. Here are the algorithms that have been used in the study "AES, DES, TDES, RC2, Rijndael". The code written using visual studio—C# 2013, after analysis of time durations for each process, the finding was some algorithms are appropriate for the small size of the text file and others are appropriate for big size of the text file and according to this result of the analysis, the concept of the suitable crypt (suitable cryptography) has constructed, the concept is in the term of checking the size of the text file before encryption and decryption process, and the program chose suitable crypt automatically according to size of the text file, the result is analyzed by R software.

Cryptographic algorithm is used to cover or protect the data from unauthorized user in the role of confidentiality, integrity, and availability, to achieve these roles, several cryptographic algorithms are developed by many people, some of them are useful for the big amount of data, and other are useful for small amount of data. Only one algorithm can be used for both encryption and decryption the specific file, any cryptography algorithm should concern a security key this is used to encrypt and decrypt the data. The secret key can be symmetric or asymmetric.

References

[1] Kumari, S. and Chawle, J. (2015) Comparative Analysis on Different Parameters of Encryption Algorithms for Information Security. *International Journal of Innovation & Advancement in Computer Science*, **2**, 123-129.

[2] Mohiuddin Ahmed, T.M., Sazzad, S. and Elias Mollah, Md. (2012) Cryptography and State-of-the-Art Techniques. *IJCSI International Journal of Computer Science Issues*, **9**, 583-586.

[3] Bala, T. and Kumar, Y. (2015) Asymmetric Algorithms and Symmetric Algorithms: A Review. International Journal of Computer Application, International Conference of Advancement in Engineering and Technology (ICAET 2015), 1-4.

[4] Stallings, W. and Brown, L. (2012) Computer Security Principles and Practices. 2nd Edition, Microsoft Corporation United States of America, Boston, Upper Saddle River, New Jersey, 10.

[5] Kaur, A. and Kumari, S. (2014) Secure Database Encryption in Web Application. *International Journal of Advanced Research in Computer and Communication Engineering*, **3**, 7606-7608.

[6] https://www.villanovau.com/resources/iss/history-of-information-security/#.wjxaw_iy3vi

[7] Jan, C. and Van Der Lubbe, A. (1998) Basic Method of Cryptography. Cambridge University Press, Cambridge.

[8] MIDN and Lee, K. (2015) Advanced Encryption (AES) Selection Process—How Rijndael Won. Capston SM463A.

[9] Charbathia, S. and Sharman, S. (2014) A Comparative Study of Rivest Cipher Algorithm. *International Journal of Information and Computation Technology*, **4**, 1831-1838.

[10] Kumari, S. and Chwla, J. (2015) Comparison Analysis on Different Parameters of Encryption Algorithms for International Security. *International Journal of Innovation and Advancement in Computer Science*, **6**, 125.

[11] https://www.vocal.com/wp-content/uploads/2012/05/tdes.pdf

[12] Allen, J.D., Anderson, D. and Becker, J. (2015) The Unicode Standard—Version 8.0—Core Specification. Unicode, Inc.

[13] https://www.interproinc.com/blog/unicode-101-introduction-unicode-standard

[14] The Unicode® Standard Version 11.0—Core Specification. http://www.unicode.org/versions/Unicode11.0.0

[15] Wesley, A. (2000) The Unicode Standard Version 3.0—The Unicode Consortium. Addison Wesley Longman, Inc.

[16] Pencholaiah, N. and Seshadri, R. (2010) Effective Comparison of DES and Rijndael Algorithm (AES). *International Journal on Computer Science and Engineering*, **2**, 1641-1645.