American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-7, Issue-4, pp-13-22
www.ajer.org
Research Paper Open Access

Design and Simulation DES Algorithm of Encryption for Information Security

Mohammed A. Hameed [1], Ahmed I. Jaber [2]dr Jamhoor M.Alobaidy[3], Alaa A. Hajer[4]

(BiladAlrafidain University College ,Computer Techniques)1(Iraq- Diyala)[1]
(University of Diyala /Iraq-Electrical power and machineDep.)[2]
(BiladAlrafidain University College ,Computer Techniques)2 (Iraq- Diyala)[3]
(BiladAlrafidain University College ,Electrical power Dep.)1 (Iraq- Diyala)[4]
Corresponding author:Mohammed A. Hameed

ABSTRACT :*The demand for protection increases, if the confidentiality of the information is of very high value. Security is very essential to avoid the unauthorized disclosure or alteration of the information. Due to the great change in technologies nowadays, a number of multimedia data is being generated and transmitted, leaving our own data vulnerable to be edited, modified and duplicated. Digital documents are therefore being faced by innumerable threats as they are very easy to copy and distribute. Cryptography is an art of secret writing, which authenticates data and important messages as well as protects the systems from valid attacks. One of the best existing security algorithms to provide data security is DATA Encryption Standard (DES). It comprises of encryption and decryption process each associated with a key which is supposed to be kept secret. In this paper the software C## used for the purpose of synthesis and simulation of DES algorithm. The data encryption standard is also known as DES. DES has been the most extensively used encryption algorithm standard in recent times. Encryption and decryption comprise of cryptography. Cryptography terminology is used in the data encryption standard along with standard algorithm to hide the original text. DES applies the cipher algorithm to each data block. Data encryption is being used to hide the true meaning of data so that it is very hard to attack or crack.*

KEYWORDS *-encryption, C##,DES, Decryption, Cryptography, file, cipher text.*

Date of Submission: 23-03-2018 Date of acceptance: 07-04-2018

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. Section 2 will give a quick overview of cryptography and its main usages in our daily life; in addition to that it will explain some of the most used terms in cryptography along with a brief description of each of the compared algorithm to allow the reader to understand the key differences between them. Section 3 will show the results achieved by other contributions and their conclusions. Section 4 will walk through the used setup environment and settings and the used system components. Section 5 illustrates the performance evaluation methodology and the chosen settings to allow a better comparison. Section 6 gives a thorough discussion about the simulation results, and finally section 7 concludes this paper by summaries the key points and other related considerations. The introduction of the paper should explain the nature of the problem, previous work, purpose, and the contribution of the paper. The contents of each section may be provided to understand easily about the paper.

II. DESCRIPTION AND DEFINITION SYSTEM

- ***Cryptography***: it is the science or study of techniques of secret writing and message hiding(Dictionary.com2009). Cryptography is as broad as formal linguistics which obscures the meaning from those without formal training. It is also as specific as modern encryption algorithms used to secure transactions made across digital networks. Cryptography constitutes any method in which someone
- attempts to hide a message, or the meaning thereof, in some medium.
- ***Plaintext: it*** is the original intelligible message or data that is fed into the algorithm as input.
- ***Cipher:*** An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods
- ***Key:*** some critical information used by the cipher, known only to the sender & receiver.
- ***Ciphertext:*** it is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different.
- ***Cryptanalysis:*** The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking.
- ***Cryptology:***The science of both cryptography and cryptanalysis called cryptology.
- *Encryption algorithm:* The encryption algorithm performs various substitutions and transformations on the plaintext.
- ***Decryption algorithm:*** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.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.

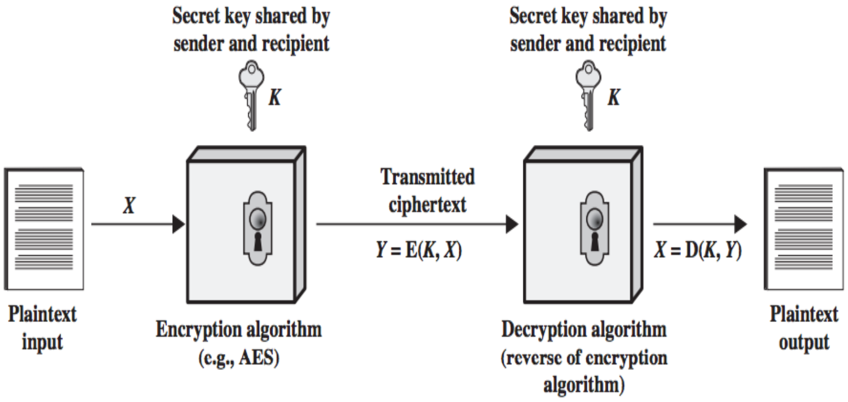

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig.1 Encryption-Decryption Flow

illustrates the overall structure of the simplifies DES, which will refer to as S-DES. The S-DES encryption algorithm takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit block of ciphertext as output. The S-DES decryption algorithm takes an 8-bit block of ciphertext and the same 10-bit key used to produce the ciphertext as input and produces the original 8-bit blockof plaintext. The encryption algorithm involves five functions: an initial permutation (IP); a complex function labelled fake, which involves both permutation and substitution operations and depends on a key input; a simple permutation function (SW) that switches the two halves of the data; the function fK again;and finally, a permutation function that is the inverse of the initial permutation(IP−1).The function f_k takes as input not only the data passing through the encryptionalgorithm, but also an 8-bit key.

III. BLOCK CIPHER

A block cipher is an encryption algorithm that encrypts a fixed size of n-bits of data - known as a block - at one time. The usual sizes of each block are 64 bits, 128 bits, and 256 bits. So, for example, a 64-bit block cipher will take in 64 bits of plaintext and encrypt it into 64 bits of cipher text. In cases where a bit of plaintext is shorter than the block size, padding schemes are called into play. Majority of the symmetric ciphers used today are actually block ciphers. DES, Triple DES, AES, IDEA, and Blowfish are some of the commonly used encryption algorithms that fall under this group shown in figure.2. Block encrypts a group of plaintext symbols as one block.

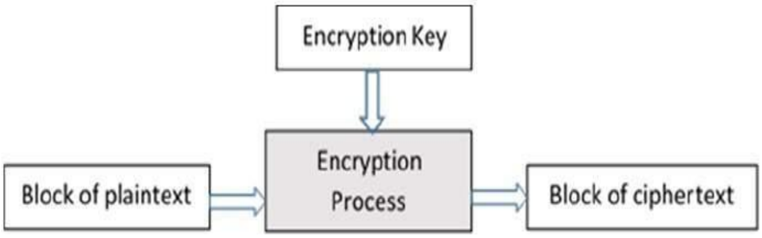


Figure 2. Block encrypt a group

DES, which stands for Data Encryption Standard, used to be the most popular block cipher in the world and was used in several industries. It's still popular today, but only because it's usually included in historical discussions of encryption algorithms. The DES algorithm became a standard in the US in 1977. However, it's already been proven to be vulnerable to brute force attacks and other cryptanalytic methods. DES is a 64-bit cipher that works with a 64-bit key. Actually, 8 of the 64 bits in the key are parity bits, so the key size is technically 56 bits long.

IV. STREAM CIPHERS

Stream cipher functions on a stream of data by operating on it bit by bit. Stream cipher consists of two major components: a key stream generator, and a mixing function. Mixing function is usually just an XOR function, while key stream generator is the main unit in stream cipher encryption technique. For example, if the key stream generator produces a series of zeros, the outputted ciphered stream will be identical to the originalplain text. Figure 3 shows the operation of the simple mode in stream cipher.

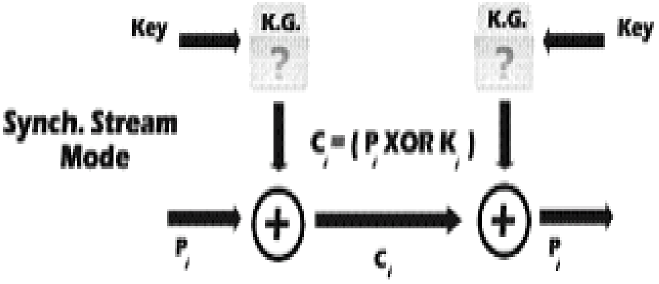
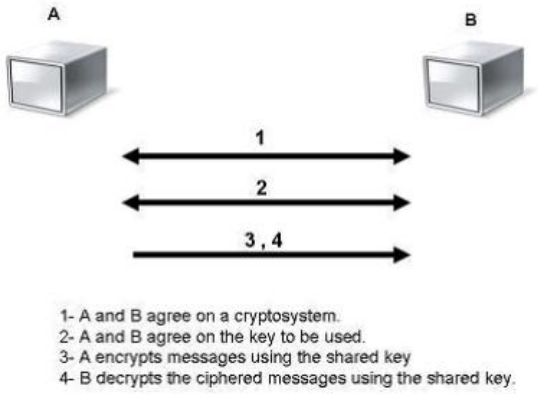


Fig. 3 Stream Cipher (Simple Mode)

V. SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

Data encryption procedures are mainly categorized into two categories depending on the type of security keys used to encrypt/decrypt the secured data. These two categories are: Asymmetric and Symmetric encryption techniques.

- **Symmetric Encryption:**In this type of encryption, the sender and the receiver agree on a secret (shared) key. Then they use this secret key to encrypt and decrypt their sent messages. Fig. 4 shows the process of symmetric cryptography. Node A and B first agree on the encryption technique to be used in encryption and decryption of communicated data. Then they agree on the secret key that both of them will use in this connection. After the encryption setup finishes, node A starts sending its data encrypted with the shared key, on the other side node B uses the same key to decrypt the encrypted messages.



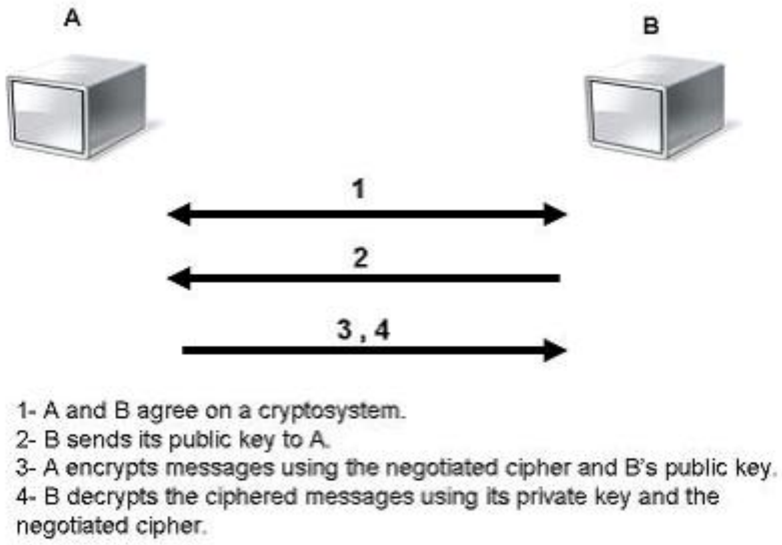
1- A and B agree on a cryptosystem.
2- A and B agree on the key to be used.
3- A encrypts messages using the shared key
4- B decrypts the ciphered messages using the shared key.

Fig.4 Symmetric Encryption

The main concern behind symmetric encryption is how to share the secret key securely between the two peers. If the key gets known for any reason, the whole system collapses. The key management for this type of encryption is troublesome, especially if a unique secret key is used for each peer-to-peer connection, then the total number of secret keys to be saved and managed for n-nodes will be n(n-1)/2

VI. ASYMMETRIC ENCRYPTION

Asymmetric encryption is the other type of encryption where two keys are used. To explain more, what Key1 can encrypt only Key2 can decrypt, and vice versa. It is also known as Public Key Cryptography (PKC), because users tend to use two keys: public key, which is known to the public, and private key which is known only to the user. Figure 5 below illustrates the use of the two keysbetween node A and node B. After agreeing on the type of encryption to be used in the connection, node B sends its public key to node A. Node A uses the received public key to encrypt its messages. Then when the encrypted messages arrive, node B uses its private key to decrypt them.



1- A and B agree on a cryptosystem.
2- B sends its public key to A.
3- A encrypts messages using the negotiated cipher and B's public key.
4- B decrypts the ciphered messages using its private key and the negotiated cipher.

Fig.5 Asymmetric Encryption

This capability surmounts the symmetric encryption problem of managing secret keys. But on the other hand, this unique feature of public key encryption makes it mathematically more prone to attacks. Moreover,asymmetric encryption techniques are almost 1000 times slower than symmetric techniques, because they require more computational processing power. To get the benefits of both methods, a hybrid technique is usually used. In this technique, asymmetric encryption is used to exchange the secret key, symmetric encryption is then used to transfer data between sender and receiver.

VII.SIMULATION AND RESULT OF DES

The simulation program writes a model by using C## and java language for DES using windows forms. When you run the program, you will see this window.This window is divided into four sections as shown in the figure 6.

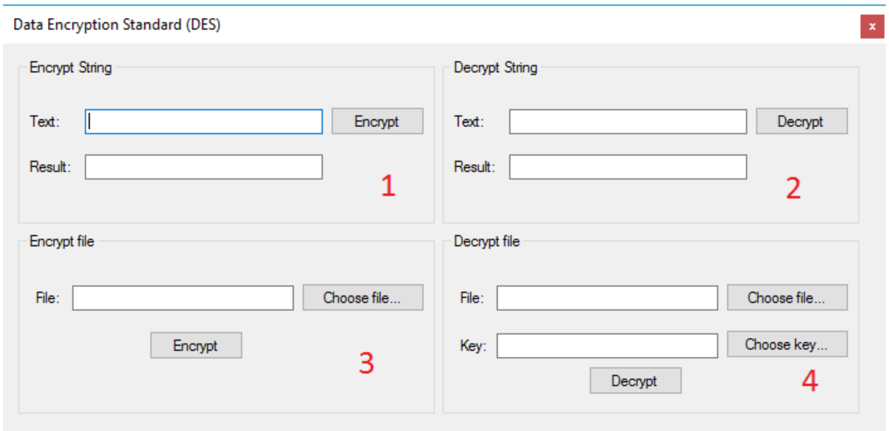


Fig.6simulation of mainwindow ofEncryption model

The first section (No. 1) through which the user can enter any word and press the encrypt button to encrypt the word and show the output of the encryption in the result box. The second Section (No. 2) through the user enters the word encrypted and click on the decrypt button and in turn the program decrypts the code and show the result in the result box. The third part (No 3) is the user entering a text file with text through the program and pressing the encrypt button to program the program to encrypt the file and the program to ask the user to save the encryption key first and then the encrypted file in the path he wants.The section 4 (No 4) The user selects the encrypted file and then the code key and presses the decrypt button to run the session by requiring the user to save the decrypted file in the path specified by the user.

1. **Encrypt String section:** write any string to encrypt it.
2. **Decrypt String section:** write any encrypted string to decrypt it.
3. **Encrypt File section**: choose any file to encrypt it.
4. **Decrypt File section:**choose any encrypted file to decrypt it.

VIII. MODELING AND TEST

Through this mainwindow the user enters the text he wants to encrypt and then presses the encrypt button as shown in the figure 6. Write any text to encrypt in encrypt string section as shown in Figure 7:

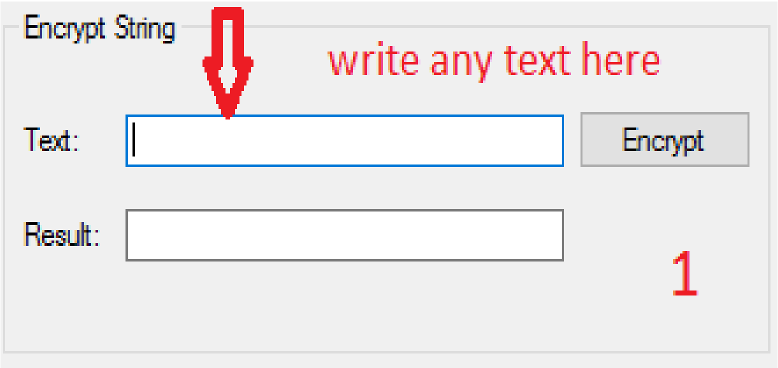
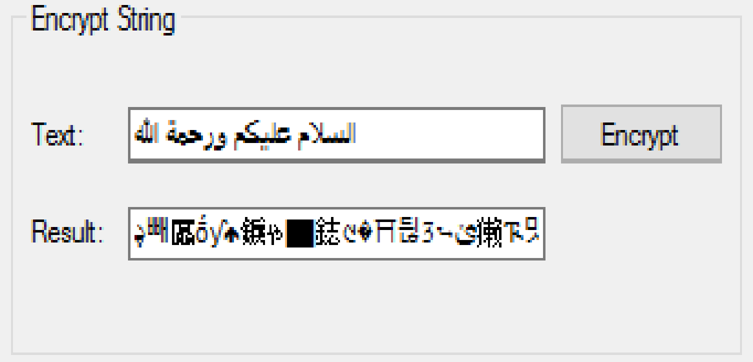


Figure 7represented Encrypt String section

At a Next step click the Encrypt button the text will be encrypted as shown in Figure 8:

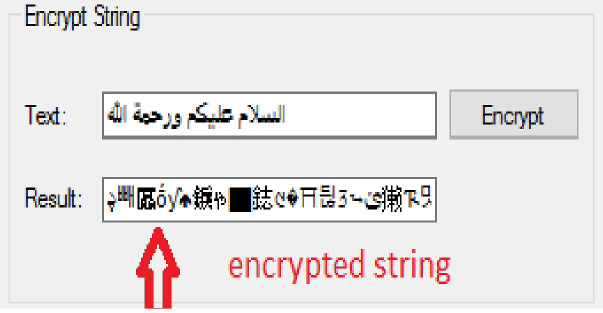


Text: السلام عليكم ورحمة الله

Result: [illegible]

Figure 8 Encrypt button the text

Gating the result an encrypted string as shown in Figure 9:

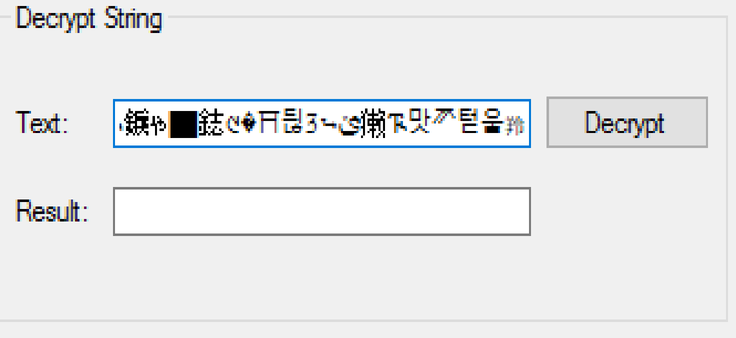


Text: السلام عليكم ورحمة الله

Result: [illegible]

Figure 9 result an encrypted string

To decrypt this string, we must to copy encrypted string to Decrypt String section shown in figure 10:

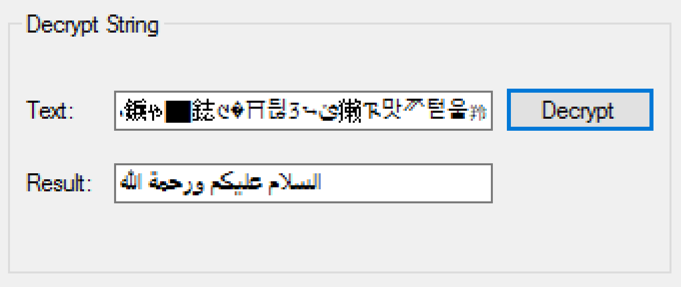


Text: [illegible]

Result:

Figure 10Decrypt StringSection

Also click Decrypt button we will gate the result as shown in figure 11:

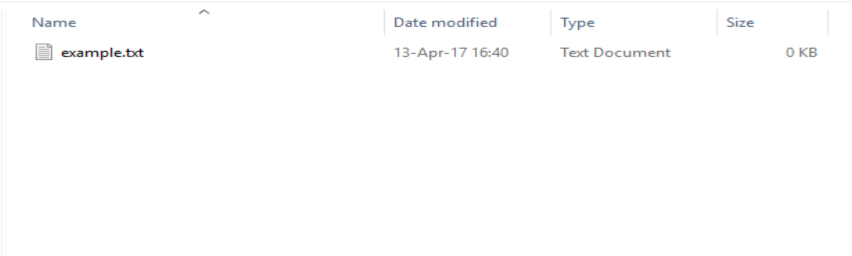


Text: [illegible]

Result: السلام عليكم ورحمة الله

Figure 11 Result Decrypt String

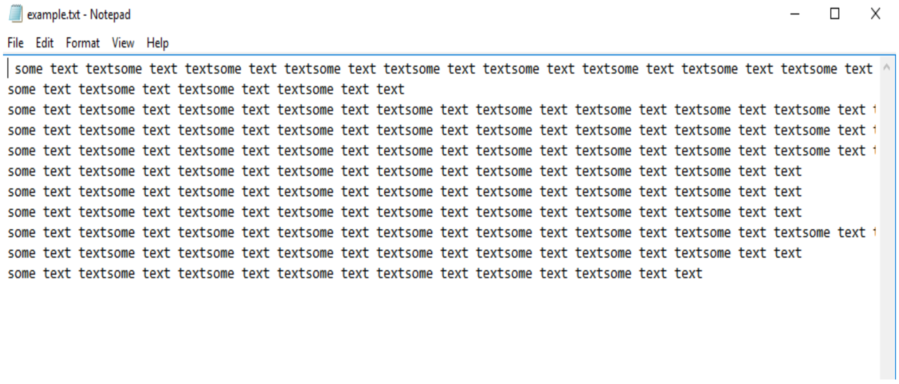
Also, can be simulate the files. First, we have to create a folder on any desktop (or anywhere) with the name DES, in this folder we make a text file and name it as you shown in figure 12 below.



Name	Date modified	Type	Size
example.txt	13-Apr-17 16:40	Text Document	0 KB

Figure 11 simulate the file encrypted

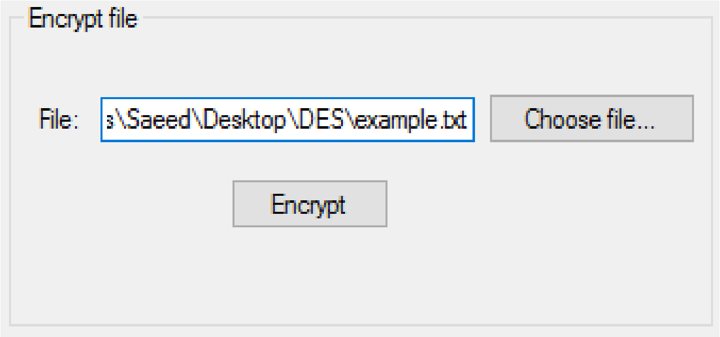
Can be write anything in the file shown in figure 12:



```
some text textsome text textsome text textsome text textsome text textsome text textsome text textsome text textsome text
some text textsome text textsome text textsome text text
some text textsome text textsome text textsome text textsome text textsome text textsome text textsome text textsome text t
some text textsome text textsome text textsome text textsome text textsome text textsome text textsome text textsome text t
some text textsome text textsome text textsome text textsome text textsome text textsome text textsome text textsome text t
some text textsome text textsome text textsome text textsome text textsome text textsome text textsome text text
some text textsome text textsome text textsome text textsome text textsome text textsome text textsome text text
some text textsome text textsome text textsome text textsome text textsome text textsome text textsome text text
some text textsome text textsome text textsome text textsome text textsome text textsome text textsome text textsome text t
some text textsome text textsome text textsome text textsome text textsome text textsome text textsome text text
some text textsome text textsome text textsome text textsome text textsome text textsome text text
```

Figure 12 write text in file

go to Encrypt file section and selection afile shown in figure 13

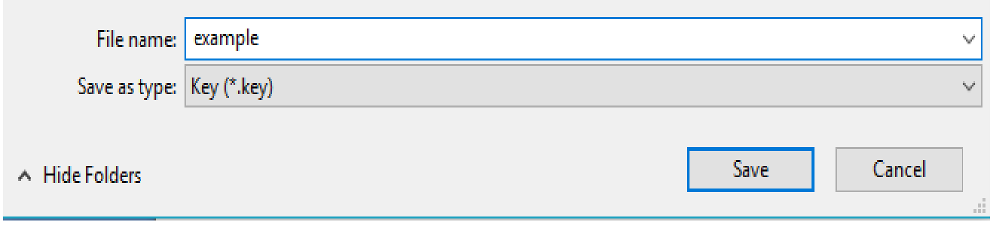


Encrypt file

File: s\Saeed\Desktop\DES\example.txt

Figure 13 selection file to the system

Next that click the Encrypt button and you have to save 2 files:
First file (the key file) save it shown in figure 14example. Key

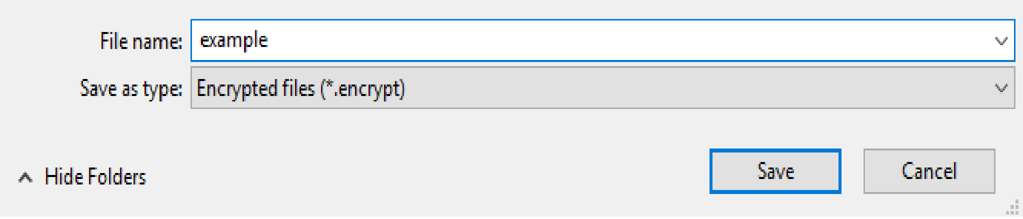


File name: example

Save as type: Key (*.key)

Figure 14example. Key

Next the second file is encrypted can be file save shown in figure 15 example. Encrypt.

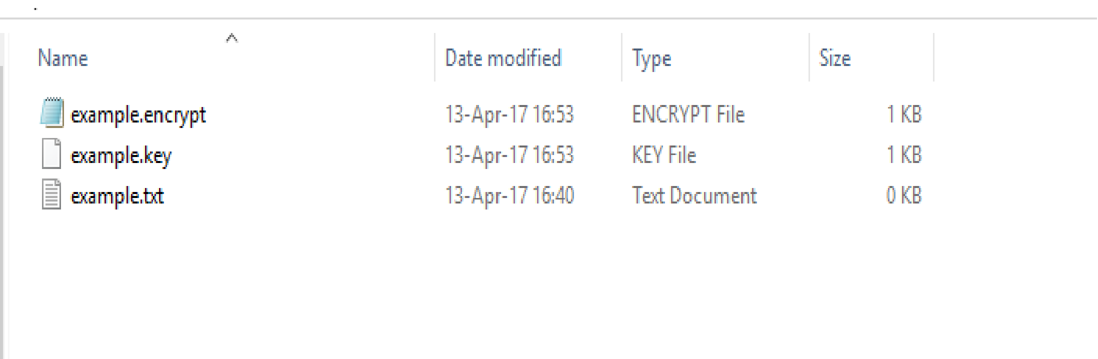


File name: example

Save as type: Encrypted files (*.encrypt)

Figure 15 Save File. Encrypt.

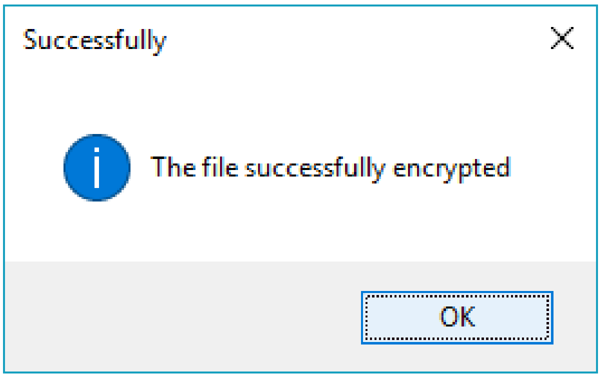
Open the folder and have to see the file encrypt and key shown in figure 16 that:



Name	Date modified	Type	Size
example.encrypt	13-Apr-17 16:53	ENCRYPT File	1 KB
example.key	13-Apr-17 16:53	KEY File	1 KB
example.txt	13-Apr-17 16:40	Text Document	0 KB

Figure 16 File Encrypt And Key

When the program will show the successfully message shown in figure 17:

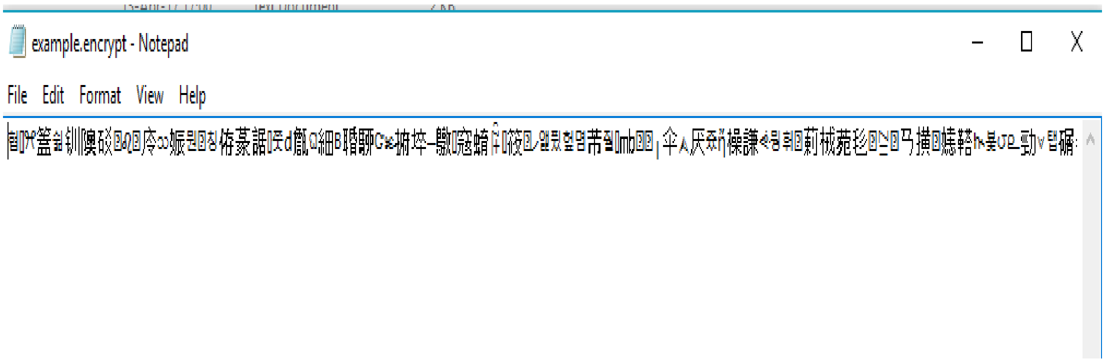


Successfully

The file successfully encrypted

Figure 17 Successfully Message

the example. Encryptcan be see thecode message shown infigure 18 below

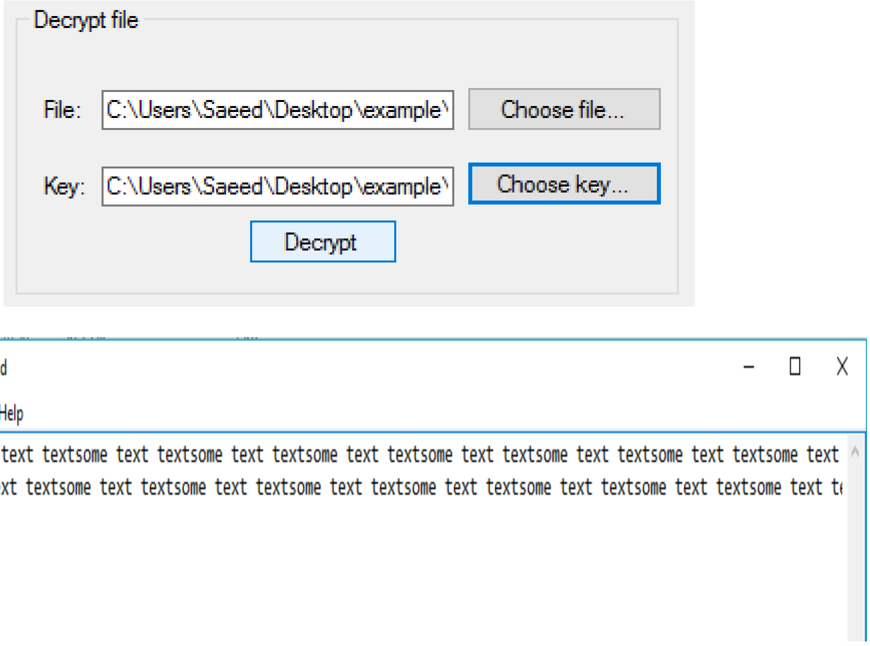


example.encrypt - Notepad

[illegible]

Figure 18example. Encrypt Code

To decrypt the encrypted file, go to Decrypt file section and choose the encrypted file and the key, click the decrypt button and having to save the decrypted file, save it shown in figure 19 example. Decrypt



File: C:\Users\Saeed\Desktop\example\

Key: C:\Users\Saeed\Desktop\example\

```
some text textsome text textsome text textsome text textsome text textsome text textsome text textsome text textsome text
ome text textsome text textsome text textsome text textsome text textsome text textsome text textsome text textsome text te
```

Figure 19 Result Decrypt File

IX. WEAK POINTS

- DES uses 16 -bits keys generated from a master 56-bit key (64 bits if we consider also parity bits)
- Weak keys: keys make the same sub-key to be generated in more than one round.
- Result: reduce cipher complexity.
- Weak keys can be avoided at key generation.
- DES has 4 weak keys – 01010101 01010101 – FEFEFEFE– E0E0E0E0 F1F1F1F1 – 1F1F1F1F 0E0E0E0E.

X. CONCLUSION

In cryptography, encryption and decryption algorithms runs important role in network security. In our research work, we analyzed the performance of existing encryption techniques like DES, word, chart or number and file algorithms. Based on the files used and the experimental and simulation result it was concluded that algorithm consumes least encryption time and DES consume maximum encryption time. We also observed that Decryption of DES algorithm. From our research work, it concluded that algorithm is better than DES algorithms.

REFERENCES

[1]. W. Stallings, Cryptography and Network Security: Principles and Practices,3rd edition, Prentice Hall, NJ, 2003.

[2]. Data Encryption Standard (DES) Algorithm

[3]. source: https://www.go4expert.com/articles/data-encryption-standard-des-algorithm-t24538/J. Orlin Grabbe , The DES Algorithm Illustrated

[4]. source: http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htmBruce Schneier, Applied Cryptography, Second Edition, John Wiley & Sons, New York, 1996.Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997.

[5]. Joseph Albahari, Ben Albahari C# 5.0 in a Nutshell: The Definitive Reference, 2015.Andrew Troelsen Pro C# 5.0 and the .NET 4.5 Framework (Expert’s Voice in .NET 2014.

[6]. Ian Griffiths Programming C# 5.0: Building Windows 8, Web, and Desktop Applications for the .NET 4.5 Framework 2015.

[7]. M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, International Journal of Modelling and Simulation, 18(2), 1998, 112-116. (8)

[8]. Note that the journal *title, volume number and issue number are set in italics*

	MOHAMMED AMER HAMEED AL-JUMAILI received his B.Sc. from al-yarmouk university engineering computer techniquse department Iraq in 2011 from, master from al-Isra university IN 2016.He is currently Assist Lecturer in the Department of computer techniquse Engineering, College of Engineering University of Bilad Alrafdyn university.
	AHMED IBRAHIM JABERreceived his B.Sc. from University of Diyala /Iraq in 2006 from power and electrical machine department, MSc from Saint-Petersburg Electro technical University "LETI" in Faculty of Industrial Automation and Electrical Engineering in 2013 .He is currently Assist .Lecturer in the Department of Electrical Power Engineering, College of Engineering University of Diyala Iraq.
	Dr. JamhoorMahmood AlObaidy Bsc : Salah aldienUniversity,Msc : Al mustansiriya University , Phd : Russian Federation Voronezh state University
	ALAA ABDULHUSSIAN HAJER received his B.Sc. from University of Baghdad (Alkawaizmi College) mechatronics engineering department Iraq in 2013 from, MSc from 2013 .He is currently Assist Lecturer in the Department of Electrical Power Engineering, College of Engineering University of BladAlrafdyn university.

Mohammed A. Hameed "Design and Simulation DES Algorithm of Encryption for