مجلة
كلية التــراث الجامعة

مجلة علمية محكمة
متعددة التخصصات نصف سنوية
العدد الأربعون
30 آب 2024
ISSN 2074-5621

رئيس هيئة التحرير
أ.د. جعفر جابر جواد

مدير التحرير
أ.م. د. حيدر محمود سلمان

رقم الايداع في دار الكتب والوثائق 719 لسنة 2011

مجلة كلية التراث الجامعة معترف بها من قبل وزارة التعليم العالي والبحث العلمي بكتابها المرقم (ب 3059/4) والمؤرخ في (2014/ 4/7)

Application To Protect Conversations While Transmitted Over The Internet

May Sabri Mohmmed

Computer Science Department, University Of Technology

Abstract

The great development of Internet applications with the increasing users within this open environment cause many problems related to data security and Internet web sites of intrusion certain users or attacking by others, so significant loss of data and information used for any purpose will occurs, there are more of security measures to be taken consideration account for the purpose of protection of sites and data, both from theft, alteration or destruction.

This research builds a data protection system that is exchanged through text chat as a proposed protection system is used to improve the work of the DES algorithm by introducing a process as an intermediate stage rather than an S-Box similar to the encryption process using the RSA method, Security and high efficiency to protect data when it is transmitted over the normal networks or the Internet by combining the two methods where the data is sent encrypted to the other party, the proposed system has been implemented on the local network between the two devices running on Windows (10) As well as applied on the Internet in a continuous manner.

Keywords: Cryptography, RSA, DES, TCP/IP, Winsock.

تطبيق لحماية المحادثات عند ارسالها عبر الانترنيت

الخلاصة

تتسبب بخلق مشاكل كثيرة تتعلق بأمنية ان التطور الكبير لتطبيقات الانترنيت مع تزايد المستخدمين ضمن هذه البيئة المفتوحة البيانات ومواقع الانترنيت من تطفل بعض المستخدمين او المهاجمة لها من قبل البعض الاخر بقصد التخريب وبتالي ضياع كبير للبيانات والمعلومات المستعملة لغرض ما، هناك كثيرمن الاجراءات الامنية التي تؤخذ بنظر الاعتبار لغرض حماية المواقع والبيانات سواء من السرقة، التحوير او التخريب.

يقوم هذا البحث ببناء نظام حماية للبيانات المتبادلة عبر الدردشة المتمثلة بالنصوص حيث انه تم استخدام نظام حماية مقترح تشبه عملية التشفير (S-Box) وذلك من خلال ادخال عملية كمرحلة وسطية بدلا من (DESلتحسين عمل خوارزمية ( ) اذ انهما توفران امنية وكفاءة عالية لحماية البيانات عند انتقالها عبر الشبكات العادية او شبكة RSAباستخدام طريقة (الانترنيت من خلال الدمج بين الطريقتين حيث يتم ارسال بيانات مشفرة الى الطرف الاخر، تم تطبيق النظام المقترح على وكذلك تم تطبيق عمله على شبكة الانترنيت بشكل متصل. (Windows 10الشبكة المحلية بين جهازين يعملان بنظام (الدردشة.,) TCP/IP،، ((DES) (RSA(،(Winsock) **الكلمات المفتاحية:** التشفير،

1. Introduction

Data protection is a major concern for information security professionals. Due to the rapid development of the means of exchanging information over the Internet and its large quantities, it is necessary to develop methods to protect the Information from intruders (Hackers or Crackers)

by writing cryptographic algorithms with fast processing and data protection. Like (AES, DES, RSA ...etc.).[1]

In the past decades, there has been tremendous growth in the field of digital storage and communication of data, triggered by several substantial breakthroughs like the internet and the vast development communications' wireless. Those recent communication technology and information will require sufficient security, for little or no cost using Web-based e-mail, telephony, or chat it's one of very important web applications [2].
The Web is vulnerable to attacks on the Web servers over the Internet, reputations can be damaged and money can be lost if the Web servers are subverted, Web applications are very easy to use, configure and manage, the short history of the Web is filled with examples of new and upgraded systems, properly installed, that are vulnerable to a variety of security attacks [3].

2. The Internet protocols

An Internet protocol was a computer networking paradigm and group of communications' protocols employed on the Internet and identical computer networks. They know as (TCP/IP) because it is extreme significant protocols, other protocols are used for sending information.
Most Internet services are based on the client/server model. Under this model, one program requests service from another program. Both programs can be running on the same computer or, as is more often the case, on different computers. The program making the request is called the client; the program that responds to the request is called the server.
Client–server systems have been operating across networks. Network communications standardized on the Internet's Transmission Control Protocol/Internet Protocol suite (TCP/IP). The most popular application programmer interface was the Berkeley 'socket' library [4].
Clients that need to use a port only for a short period get an arbitrary port allocated by the operating system. The headers for UDP and TCP packets include the IP addresses of client and server machines, and the port numbers for the client and server processes. The client composes the first packet, inserting the host's IP address once this has been determined, and the 'well known port number' for the desired service; it also inserts its own temporary port number and the IP address of the machine on which it is running. These data allow the server to send response packets that are properly addressed to the client [5].

3. Sockets

networking software support a number of different types of application programming interfaces (APIs) for communicating over an internet. The socket interface provides an API for network communication that is very close to the API provided for doing ordinary I/O with local devices. The socket interface has been implemented. On a wide variety of operating systems, and programs that access sockets can be used for implementing network communication in a heterogeneous environment in which hosts of all types must be able to communicate. A socket is an object that represents a low-level access point to the IP stack. This socket can be open or closed or one of a set number of intermediate states. A socket can send and receive packet down this connection. Figure-1 shows how two applications talk to each other across a communication network through the socket interface. In a typical communication session, one application operates as a server and the other as a client. The server provides services upon request by the client [6].

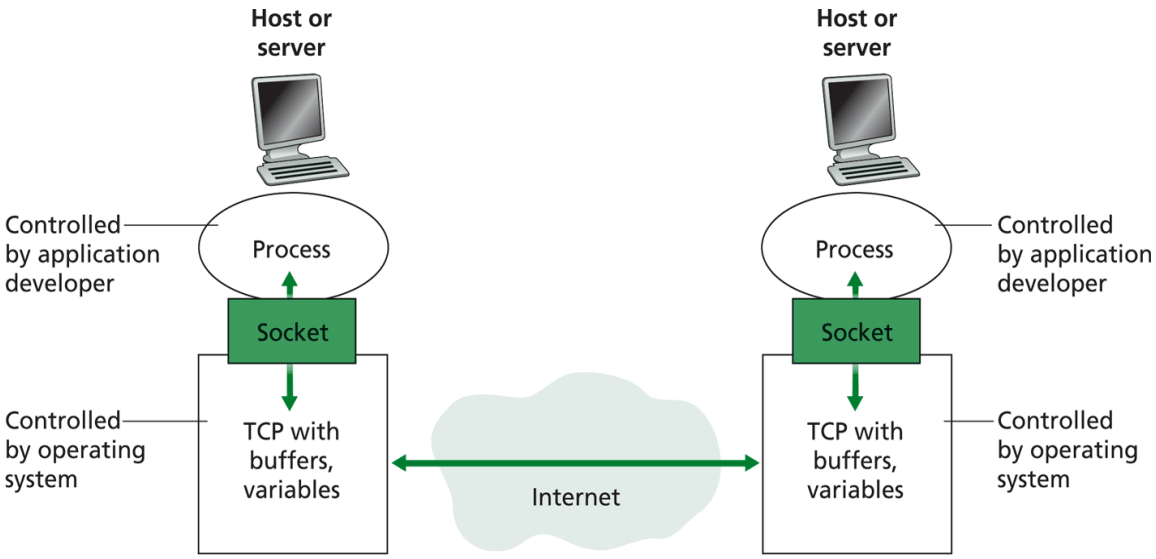
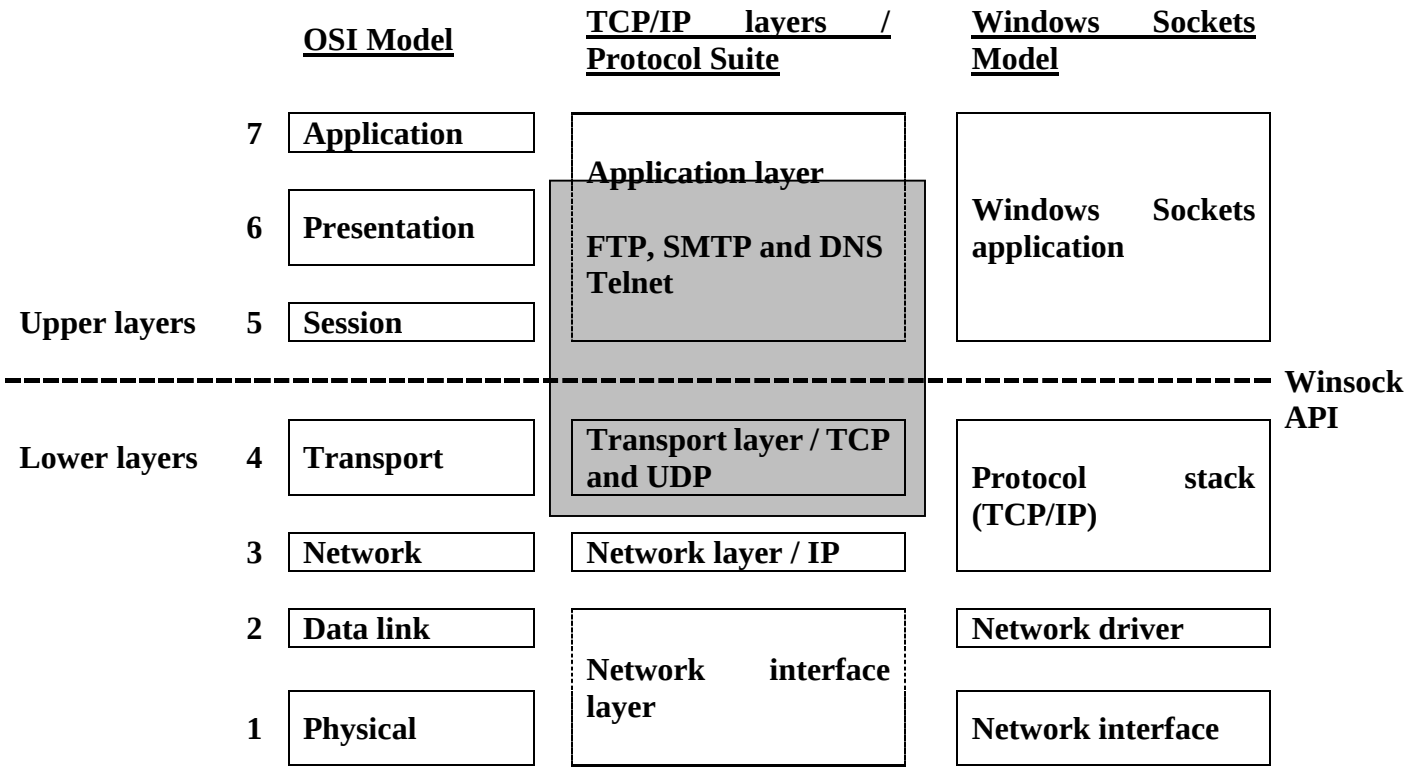


Figure (1)- Socket interface.

4. Winsock

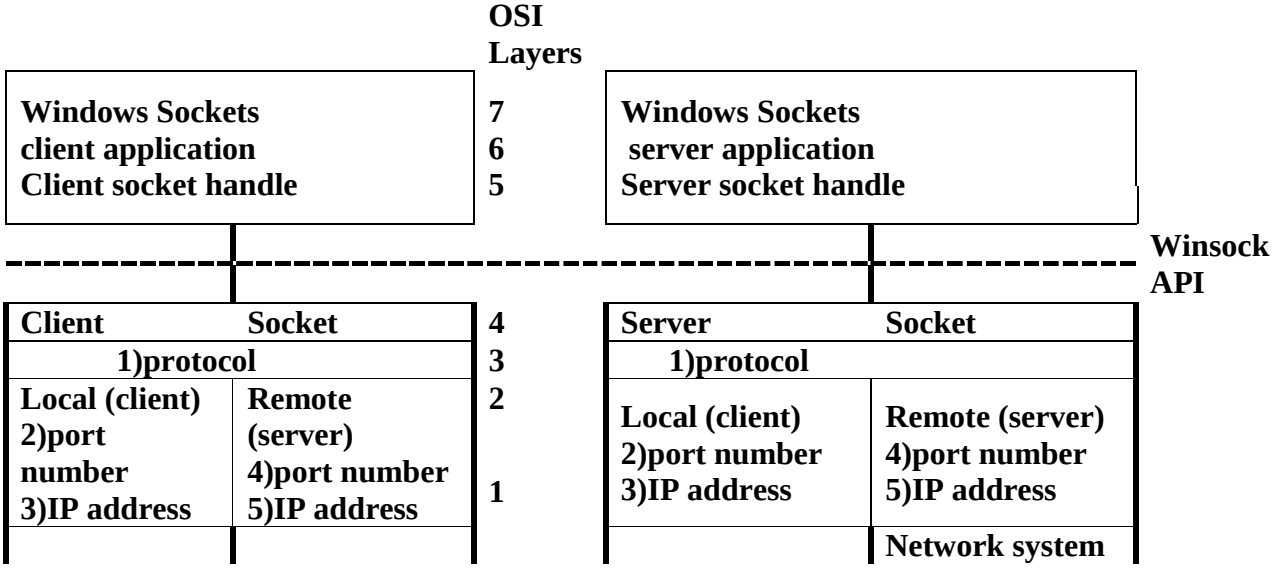
The Communication Theory of Winsock Transmission of the data file in system is carry out through Winsock control, the introduction of Winsock's communication mechanism. Implementing data communication through Winsock can divided into the following steps: - A. Server intercepts network Since TCP is a connection-oriented agreement, it has to make connection preparation before data transmission. At this time, sever intercepts whether there is information from network at any time through methods like Listen [7]. B.

Client requests connection Client specifies the hostname (or IP) and port address to send out connection request to remote server through connect.[8] C. Server allows connection request Server has two choices; one is allowing request and the other is rejecting request. If it allows request, follow-up work can continue, or transmission of bilateral data WINSOCK.DLL actually acts as a "layer" between WinSock applications and TCP/IP stack. WinSock applications can translate these commands to TCP/IP stack, and TCP/IP stack passes them on to the Internet [9]. A good comparison with TCP/IP protocol suites and OSI model can understand by figure 2 [10].



Figure(2)- the TCP/IP Protocol Suite

Client-Server Model can satisfy as shown in figure 3, based on same protocol for both Clint and Server sockets, and deciding IP address and port number for both client and server.



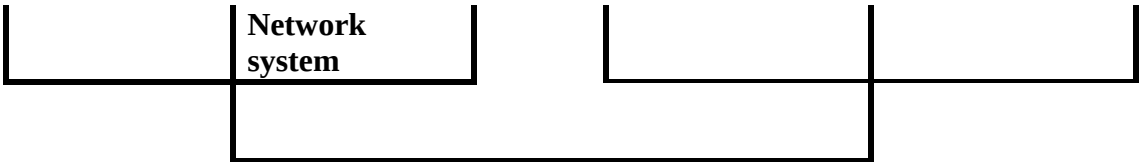


Figure (3)- Client/Server sockets [11]

5. The RSA cryptosystem

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time by using the private key. By securing the data, we are not allowing unauthorized access to it only the owner of the private key can decrypt the sensitive data. Thus, only the intended recipient of the data can decrypt it, even if the data were taken in transit.

The other method of asymmetric encryption with RSA is encrypting a message with a private key.[12]

Key Generation Algorithm

1.Choose two distinct large random prime numbers p & q such that $p \neq q$.

2. Compute $n = p \times q$.

3. Calculate: $\emptyset(n) = (p-1)(q-1)$.

4. Choose an integer e such that $1<e<\emptyset(n)$

5. Compute d to satisfy the congruence relation $d \times e = 1 \bmod \emptyset(n)$; d is kept as private key exponent.

6. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and Ø(n) secret. [20].

Encryption Algorithm.

- Plaintext $M < n$
- Ciphertext $C = M^e \bmod n$

Decryption Algorithm.

- Ciphertext C
- Plaintext $M = C^d \bmod n$

6. The RSA public key cryptosystem

The Rivest-Shamir-Adleman (RSA) from the names of those who first implemented it, the technical details of RSA work on the idea that it is easy to generate a number by multiplying two sufficiently large numbers together, but factorizing that number back into the original prime numbers is extremely difficult. The public and private key are created with two numbers, one of which is a product of two large prime numbers. Both use the same two prime numbers to compute their value. RSA keys tend to be 1024 or 2048 bits in length, making them extremely difficult to factorize. [13][14]

Key Generation Algorithm

Bob secretly chooses randomly two primes v and q of roughly the same size but not equal.[15].

- *Computes the RSA modulus* $n = v * q$.
- Compute $\varphi(n) = (v-1)(q-1)$.

- Choose a random odd integer e such that gcd ($\varphi(n), e$) = 1; $1 < e < \varphi(n)$.
- Compute the integer d such that $e * d \equiv 1 \pmod{\varphi(N)}$.

$d \equiv e^{-1} \pmod{\varphi(n)}$

-Public key: $PU = \{e, n\}$

-Private key: $PR = \{ d, n \}$

Encryption Algorithm.

- Plaintext $M < n$
- Ciphertext $C = M^e \bmod n$

Decryption Algorithm.

- Ciphertext C
- Plaintext $M = C^d \bmod$

7. Data Encryption Standard (DES*)*

today DES and its heir 3DES are known to be insecure and considered obsolete. However, modern encryption still uses similar techniques, The DES algorithm uses a key of 56-bit size. the DES takes a block of 64-bit plain text as input and generates a block of 64-bit cipher text. The process has several steps involved in it, where each step is called a round. Depending upon the size of the key being used, the number of rounds varies. For example, a 128-bit key requires 10 rounds, a 192-bit key requires 12 rounds, and so on. DES is a symmetric encryption algorithm. [16].

Symmetric Encryption

All encryption is done via a computer software program. You can easily encrypt information by yourself. One of the simplest ways to do this is through symmetric encryption. Here, a letter or number coincides with another letter or number in the encryption code. You can take any written text and substitute letters and numbers for their coded counterpart, thus encrypting the text.[17]

Asymmetric encryption

is a secure and easy way that can be used to encrypt data that you will be receiving. It is generally Done electronically. A public Key is given Out to whomever You want or posted somewhere for the public to see.They can Encrypt information using the key and send it to you.

This is Often done When writing emails. This means Encrypt the Data with the public key; it can only be read again by whomever the private key has. .[18]

Symmetric Key Cryptography

The DES most widely used symmetric key cryptographic method is the Data Encryption Standard (DES) as shown in below Figure (4) : It uses a fixed length, 56- bit key and an efficient algorithm to quickly encrypt and decrypt messages. It can be easily.[19]

Figure(4)-Symmetric Key – Triple DES

implemented in the encryption and decryption process even faster. In general, increasing the key size makes the system more secure. A variation of DES, Called Triple – DES or DES - EDE(Encrypt-Decrypt-Encrypt), Uses three applications of DES and two independent DES keys to produce an effective key length of 168 bits. Despite the Efficiency of symmetric Key cryptography, it has a fundamental weak spot –key The International Data Encryption Algorithm (IDEA) Was invented by James Massey 1991. IDEA Uses a fixed length, 128- bit key (larger than DES but smaller than Triple -DES). It is also Faster than Triple - DES. In the Early 1990s, Don Rivest of RSA Data Security, Inc., Invented the Algorithms RC2 And RC4. These use Variable length Keys and are claimed to be even faster than IDEA. .[20]

The 64 bits of the input block to be enciphered are first subjected to the following permutation, called the initial permutation (IP) that is the permuted input has bit 58 of the input as its first bit, bit 50 as its second bit, and so on with bit 7 as its last bit. The permuted input block is then the input to a complex key-dependent computation described below. The output of that computation, called the pre output, is then subjected to the following permutation which is the inverse of the initial permutation (IP-1).[21]

Table (1) show permutation of DES

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

That is, the output of the algorithm has bit 40 of the pre output block as its first bit, bit 8 as its second bit, and so on, until bit 25 of the pre output block is the last bit of the output.

Table (2) S-Box Function S1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

If S_1 is the function defined in this table and B is a block of 6 bits, then $S_1(B)$ is determined as follows: The first and last bits of B represent in base 2 a number in the range 0 to 3. Let that number be i. The middle 4 bits of B represent in base 2 a number in the range 0 to 15. Let that number be j. Look up in the table the number in the i'th row and j'th column. It is a number in
the range 0 to 15 and is uniquely represented by a 4-bit block. That block is the output $S_1(B)$ of S1 for the input B. For example, for input 011011 the row is 01, that is row 1, and the column is determined by 1101, that is column 13. In row 1 column 13 appears 5 so that the output is 0101. Selection functions $S_1,S_2,...,S_8$ of the algorithm .Since the algorithm is symmetric then the Decipher process is same Cipher process using k_{16} first.

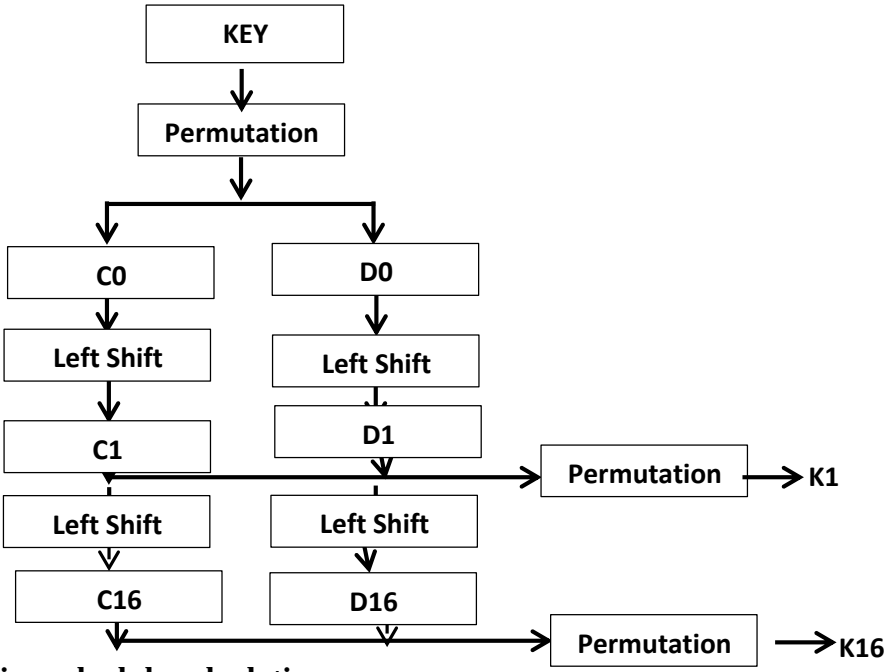


Figure (5)- Key Generation schedule calculation

8. Proposed Method

The idea of the work is to improve the work of DES algorithm by introducing the process as an intermediate stage after the exit of the results from (S-Box) similar to the encryption process using RSA method as follows: -A series of 48 bits is divided into 8 groups, each with a length of 6 bits. Each part is inserted into its own S_BOX. The output is a series of 4 bits per piece. The output is 8 parts length of 4 bits. The series is (32) bits.The change made in this method is on the string entering the S_BOX, Instead of that , The string is divided into 4 parts each with length of (12) bits called (m) and then a process ($C = M^e \bmod n$). Then the value of C is converted to the binary formula (0,1), Here we will produce three cases:

1- If (0≤C≤127), it means that it consists of 7 bits or less (0≤C≤1111111) A number of (1's) to the Right will add to become of (8) bits, Thus, the number becomes $C_{new} = (C_{old} * 2^b)-1+2^b$, Where b is the number of bits which added for example:-
C=11101=29 C= (29*2^3) +2^3-1=29*8+7=239=11101111.
C=1010=10 C= (10*2^4) +2^4-1=10*16+15=175=10101111.

2- If (128≤C≤255) it means that it consists of 8 bits (10000000≤C≤11111111) nothing is added.
3- If (C≥256), it means that it consists of 9 bits and more (C≥100000000). Here A number of bits are deleted from the Right to become 8 bits, According to equation $C_{new}=(C_{old} - X)\backslash 2^b$ where X is the value of the bits cut after being converted to decimal and b is the number of bits which cut for example:-
C=957=1110111101 C= (957-1)\$2^2$=956\4=239=11101111.
C=1533=10111111101 C= (1533-5)\$2^3$=1528\8=191=10111111.This process is very similar to the S_BOX function, which inserts 6 bits and outputs 4 bits, here there are three cases (add or Not adding or delete) these three processes increases the complexity of the output Or complicate the process of predicting outputs. On the other hand, the choice of the values (e,n)is not subject to RSA encoding requirements since we use ($C = M^e \bmod n$)in Cipher and Decipher (Bidirectional),that mean we don't need to select (e) according to Euler's equation (ed mod ∅=1) .finally preferably (n) is large which lead to create big value of (C≥256)so that the bits deletion process will become large since (0≤C≤n-1)

Cipher Algorithm

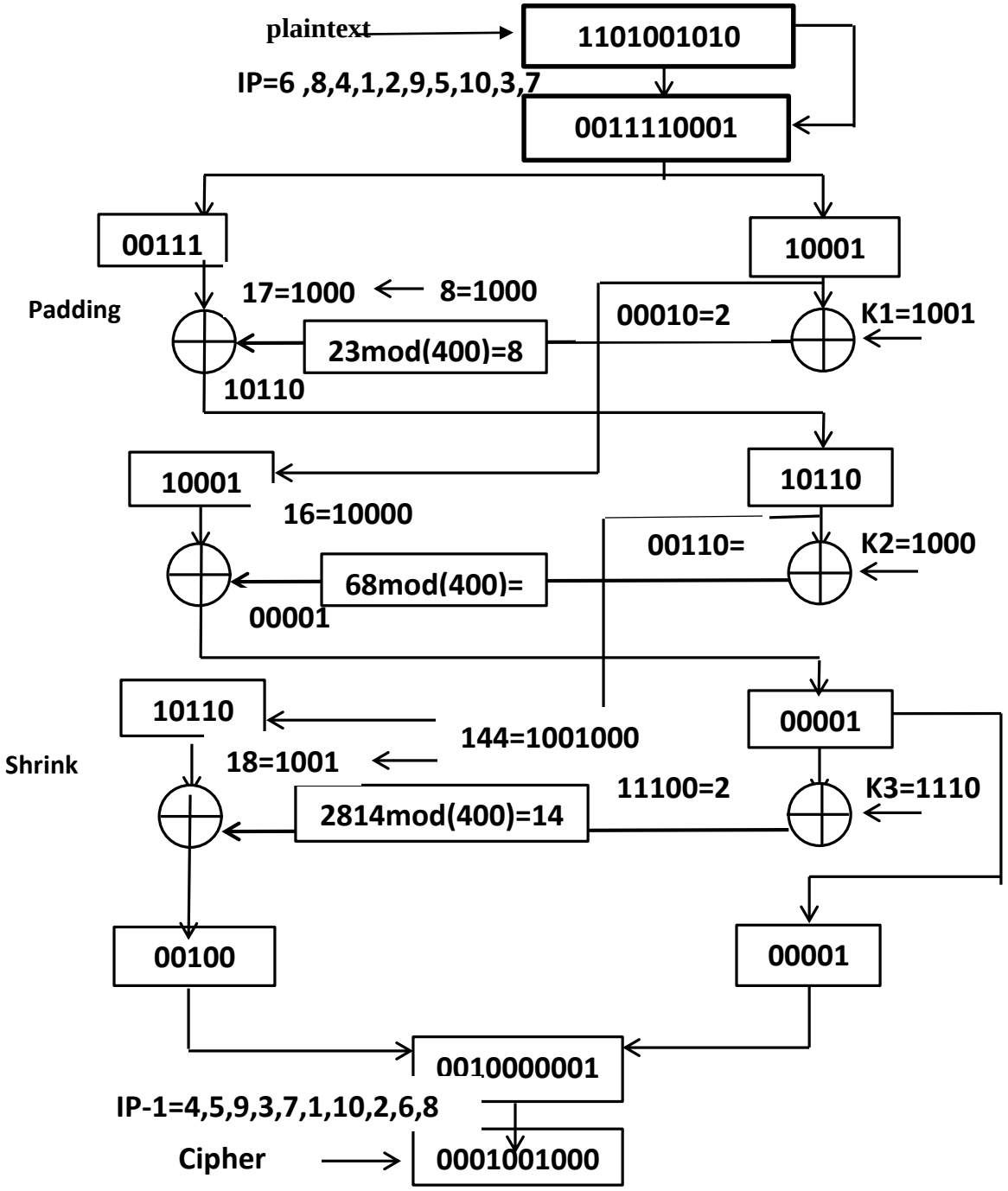
1. *generate Keys (K1,K2,,,,,,K16) .*
2. *select integer number (n) random.*
3. *Select integer number (e_1,e_2,e_3,e_4) less than (n) random.*
4. *Set S=nothing [S=""]*
5. *Input Plaintext 64 bits as a block .*
6. *permutation process(IP).*
7. *Split or divided into 2 parts left and right (L,R) each with 32 bits length.*
8. *For I = 1 to 16*
9. *Expansion right side (R_i) into 48 bits length then XOR operation with K_i*
10. *Divided the output result of ($R_i \oplus K_i$) which is 48 bits into 4 blocks each one 12 bi length.*
11. *For j = 1 to 4*
12. *Convert block number (j) to decimal form call it(m).*
13. *Calculate $C=m^{ei} mod (n)$.*
14. *.Convert (C) value into Binary form.*
15. *Concatenation ($S=S+C_{new}$).*
16. *XOR Operation $L_{new}= (L_i \oplus S)$*
17. *$R_{i+1}=L_{new}$*
18. *$L_{i+1}=R_i$*
19. *Next i*
20. *Permutation invers process (IP^{-1})*
21. *The Result is CipherText(64)bits*

Decipher Algorithm

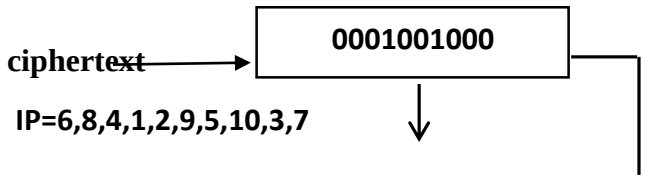
1. *generate Keys (K1,K2,,,,,,K16) .*
2. *select integer number (n) random.*
3. *Select integer number (e_1,e_2,e_3,e_4) less than (n) random.*
4. *Set S=nothing [S=""]*
5. *Input CipherText 64 bits as a block .*
6. *permutation process(IP).*
7. *Split or divided into 2 parts left and right (L,R) each with 32 bits length.*
8. *For I = 16 to 1*
9. *Expansion right side (R_i) into 48 bits length then XOR operation with K_i.*
10. *Divided the output result of ($R_i \oplus K_i$) which is 48 bits into 4 blocks each one 12 bits length.*
11. *For j = 1 to 4*
12. *Convert block number (j) to decimal form let call it(m).*
13. *Calculate $C=m^{ei} \bmod (n)$.*
14. *.Convert (C) value into Binary form.*
15. *Concatenation ($S=S+C_{new}$).*
16. *Next j.*
17. *XOR Operation $L_{new}= (L_i \oplus S)$*
18. *If i=1 then goto 25 condition of Last round no swap*
19. *$R_{i+1}=L_{new}$*
20. *$L_{i+1}=R_i$*
21. *Next i*
22. *Concatenation($L_{new} + R_i$)*
23. *Permutation invers process (IP^{-1})*
24. *The Result is Plaintext(64)bits*

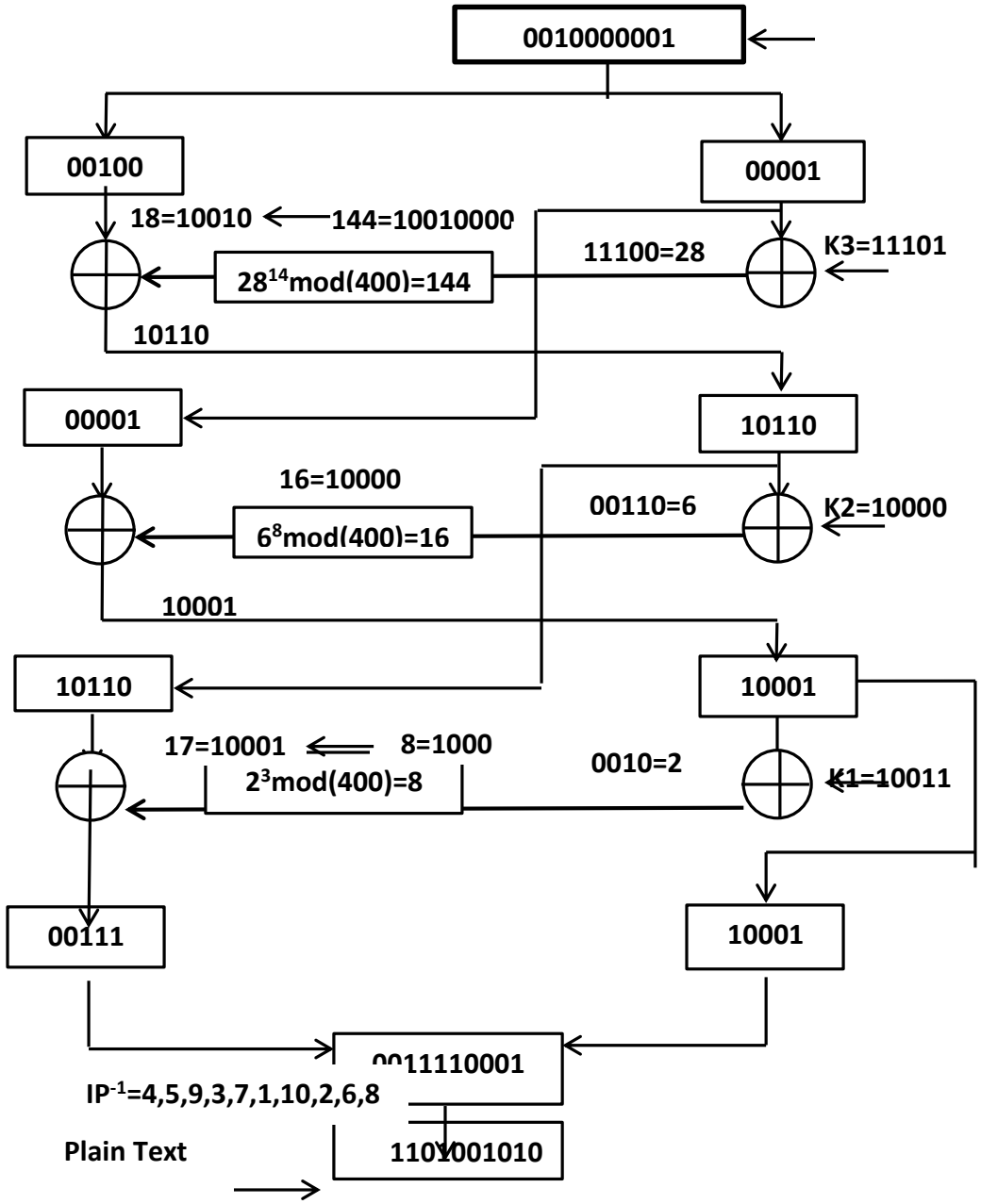
Example

Input text, Let say we have plaintext (10) bits length (1101001010) Select (n=400) random big number, select(e1,e2,e3)(3,8,14)random less than (n) and IP=6,8,4,1,2,9,5,10,3,7and IP^{-1}=4,5,9,3,7,1,10,2,6,8 In this example we will run 3 rounds only instate of 16 rounds , Let K_1=10011,K_2=10000,K_3=11101



Decipher Process





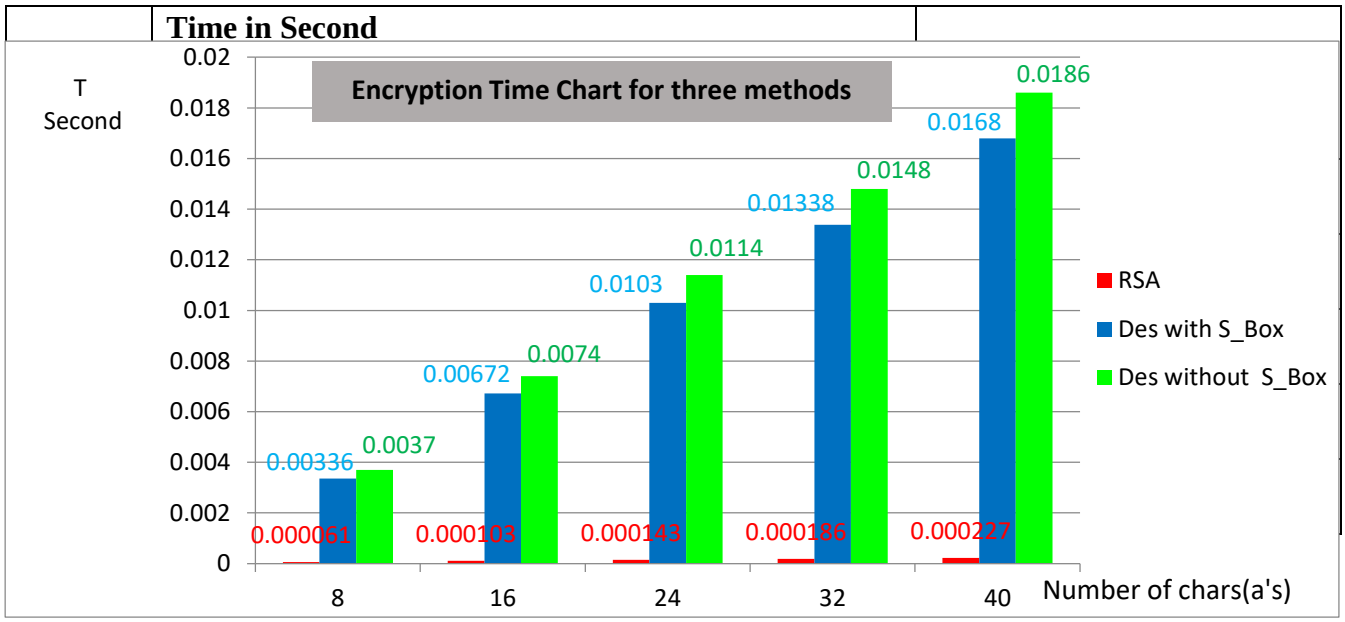
Number of a's	Time in Second				Time increase by Percentage
	RSA	Des with S_Box	Des without S_Box	Approximate (8*RSA+ Des with S_Box)	
8	0.000061	0.00336	0.0037	0.00384	[(0.0037/0.00336)-1]*100=10%

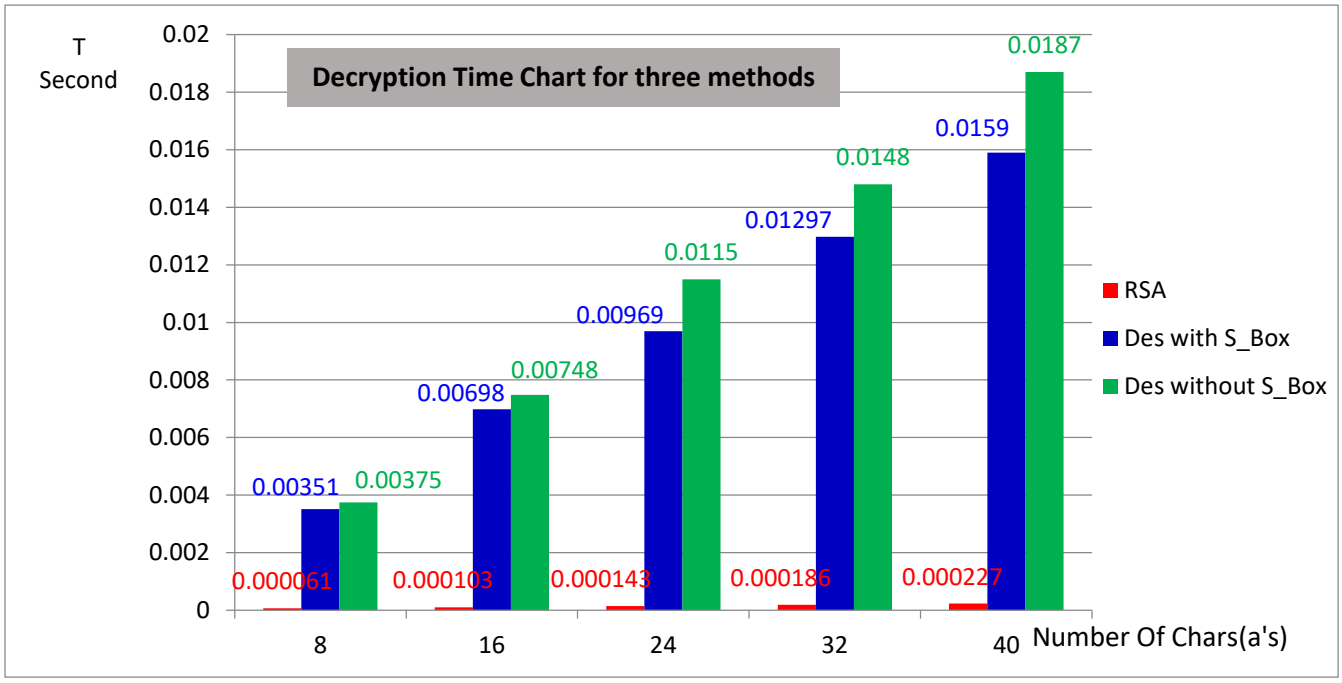
16	**0.000103**	**0.00672**	**0.0074**	**0.00754**	**[(0.0074/0.00672)-1]*100=11%**
24	**0.000143**	**0.0103**	**0.0114**	**0.0114**	**[(0.0114/0.0103)-1]*100=11%**
32	**0.000186**	**0.01338**	**0.0148**	**0.01486**	**[(0.0148/0.01338)-1]*100=11%**
40	**0.000227**	**0.0168**	**0.0186**	**0.01861**	**[(0.0186/0.0168)-1]*100=11%**

Table (3) Encryption Time

FlowChart(1)Encryption Time Chart for three methods

Table (4) Decryption Time





Flow Chart (2) Decryption Time Chart for three methods

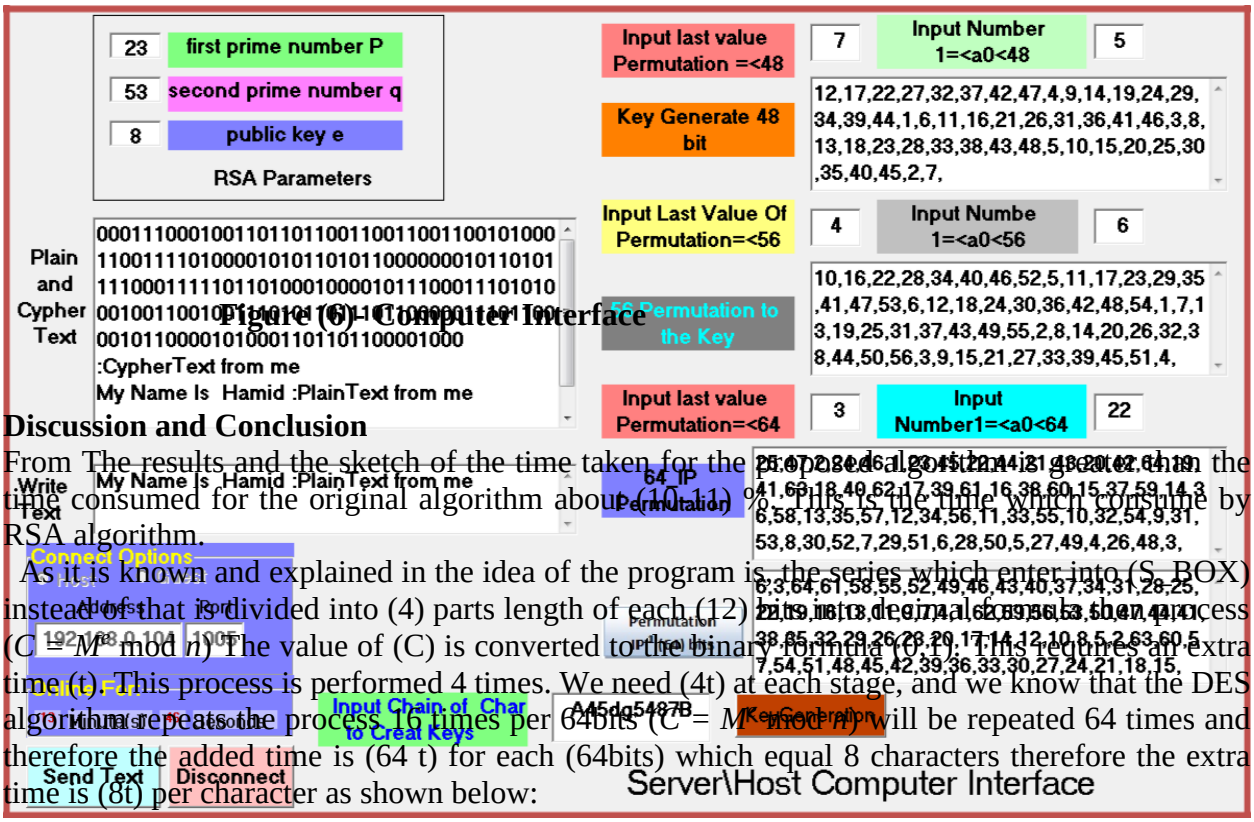


Figure (6) Computer Interface

Discussion and Conclusion

From The results and the sketch of the time taken for the proposed algorithm is greater than the time consumed for the original algorithm about (10-11) %. This is the time which consume by RSA algorithm.

As it is known and explained in the idea of the program is the series which enter into (S_BOX) instead of that is divided into (4) parts length of each (12) bits in a decimal process ($C = M^e \bmod n$) The value of (C) is converted to the binary formula (0,1). This requires an extra time (t). This process is performed 4 times. We need (4t) at each stage, and we know that the DES algorithm repeats the process 16 times per 64bits ($C = M^e \bmod n$) will be repeated 64 times and therefore the added time is (64 t) for each (64bits) which equal 8 characters therefore the extra time is (8t) per character as shown below:

- RSA time =t_1
- Time to convert binary to decimal form and vice versa =t_2
- $t=t_1+t_2$
- DES algorithm with S-Boxes (Original Algorithm) =t_3
- Total time=$8t+t_3$

For decryption, the algorithm is similar to the Encryption algorithm as shown in the algorithm diagram therefore the processes which applied on the encryption will be applied to the decryption.

1. This work design by Visual Basic and used Winsock socket to develop the program in the (Windows System), it is possible to develop this work in a different System.
2. The execution time of the proposed method doesn't have a big difference from the original methods it is about (10-11) %.
3. The proposed method is combination between DES and RSA (only encryption) cryptosystem they give us additional difficulties of the encrypted data when you use more or merge the two methods they give us additional difficulties, because they are employing the DLP and IFP in the same protocol.

Future works

1.we can establish entire secure system. we can use DES algorithm with full AES method then we will encrypt by using (k_1) first and (e_1) second then k_2,e_2 for 16 round.

2.Multimedia such as images, video, and audio can be used to transmit information in a secret way (confidentially) after encryption.

3. It is possible using other program languages such as (VB.NET) &(C#) language and in different System like Unix, Linux… etc

References

[1]	William, S., "Cryptography and Network Security: Principles and Practice "Fifth Edition, Prentice Hall, 2011.
[2]	Rémi Géraud **,** "Advances in public-key cryptology and computer Exploitation", Security [cs.CR]. PSL Research University,2017
[3]	Joel Scambray," Hacking Expose web application", 2011. Pranab Bandhu "TCPIP Model in Data Communication and Networking" American Journal of Engineering Research (AJER) volume-4, Issue-10, pp-102-107 www.ajer.org 2015.
[4]	Long Hoang. " A Study of Internet Protocols "Oulu University of Applied Sciences of Information Technology. Spring 2019.
[5]	Weijia Jia and Wanlei Zhou " Distributed Network Systems From Concepts to Implementations", Springer Science Business Media, Inc.2021

[6]	Isnar Sumartono, Andysah Putera and Utama Siahaan " Encryption of DES Algorithm in Information Security", International journal for innovative research in multidisciplinary field Volume - 4, (Oct – 2018).
[7]	Alberto Leon-Garcia & Indra Widjaja,"Communication Networks Fundamentals Concepts and Key Architecture", McGraw Companies. 2020.
[8]	Bob Quinn and Dave Shute," Windows Sockets Network Programming", Addison-Wesley Professional; 1st edition, 2010.
[9]	Pat Bonner," Network Programming with Windows Sockets", Prentice Hall, 2021.
[10]	Whai-En Chen,"Windows Socket Programming & IPv6 Translation Middleware", VoIP and IPv6 Laboratory, Dept. of Computer Science and Information Engineering National Chiao Tung University, 2004.
[11]	Bible,"Home Networking", 2nd edition, Wiley Publishing, Inc. 2004.
[12]	Doug Lowe," Networking All-In-One Desk Reference For Dummies", Wiley Publishing, Inc., 2021.
[13]	Adam Young and Moti Yung," Malicious Cryptography Exposing Crypto virology",Wiley Publishing, Inc. 2014.
[14]	John Talbot and Dominic Welsh," Complexity and Cryptography An Introduction ", Cambridge University Press, 2018.
[15]	Rolf Oppliger," Contemporary Cryptography ", Artech House, Inc. 2005.
[16]	Wenbo Mao," Modern Cryptography: Theory and Practice', Prentice Hall, 2020.
[17]	Alan G. Konheim," Computer Security and Cryptography ", John Wiley & Sons, Inc. 2017. Maria Welleda Baldoni, Ciro Ciliberto, Giulia Maria Piacentini
[18]	Cattaneo," Elementary Number Theory, Cryptography and Codes", Springer-Verlag Berlin Heidelberg. 2019.
[19]	Parsi Kalpana ,et al, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012 Data Security in Cloud Computing using RSA Algorithm Parsi Kalpana1 Asst Professor Department of CA Sreenidhi Institute of Science and Technology. Sudha Singaraju2 Asst Professor Department of CA Sreenidhi Institute of Science and Technology

[20]	International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2017 A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security Gurpreet Singh M.Tech Research Scholar, Department of Computer Science and Engineering Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India
[21]	International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139 ISSN 2320–088X A STUDY AND PERFORMANCE ANALYSIS OF RSA ALGORITHM ,M. Preetha , M. NithyaComputer Science & Application & Periyar University , India