New Data Encryption Standard Algorithm

K.Anchugam and M.Tamilselvi

Abstract

A goal is the design of any encryption algorithm must be security against unauthorized attacks. Within the last decade, there has been a vast increase in the accumulation and communication of digital computer data in both the private and public sectors. Much of this information has a significant value, either directly or indirectly, which requires protection. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. Performance and security level is the main characteristics that differentiate one encryption algorithm from another. Here introduces a new method to enhance the performance of the Data Encryption Standard (DES) algorithm is introduced here. This is done by replacing the predefined XOR operation applied during the 16 round of the standard algorithm by a new operation depends on using two keys, each key consists of a combination of 4 states (0, 1, 2, 3) instead of the ordinary 2 state key (0, 1). This replacement adds a new level of protection strength and more robustness against breaking methods. The New Comparative Study between DES, 3DES and AES within Nine Factors achieving an efficiency, flexibility and security, which is a challenge of researchers.

Keywords

Comparison of DES, 3DES and AES, DES, Encryption, Decryption

I. INTRODUCTION

cryptography is a collection of mathematical techniques used to ensure confidentiality of information. The process of scrambling a message with the help of a key is called Encryption. The process of unscrambling a message using an appropriate key is called decryption.

Kryptos = secret, graphy = writing

→Only someone use the key can understand an encrypted message.

Manuscript received April 19,2012

- K.Anchugam-Department of Computer Applications, V.S.B. Engineering College, Karur, Tamilnadu, India. (e-mail: anchugam.mca@gmail.com).
- M.Tamilselvi-Department of Computer Applications, V.S.B. Engineering College, Karur, Tamilnadu, India. (e-mail: mtamilselvi587@gmail.com).

Cryptography -- from the Greek for "secret writing" is the mathematical "scrambling" of data so that only someone with the necessary ***key*** can "unscramble" it.

Cryptography is usually referred to as "the study of secret", while now a days 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 in figure 1.

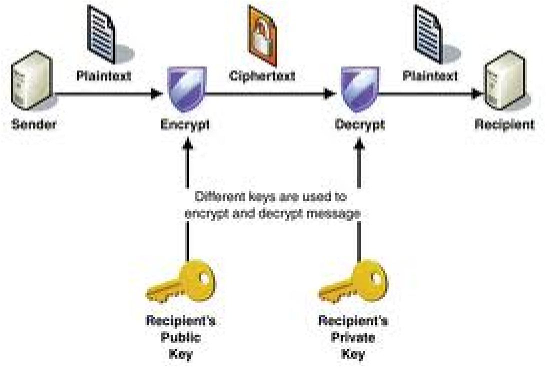


Figure 1. Encryption/Decryption

Cryptography Goals:[2]

1. CONFIDENTIALLY- Information in computer transmitted information is accessible only for reading by authorized parties.
2. AUTHENTICATION- Origin of message is correctly identified with an assurance that identity is not false.
3. INTERGRITY- Only authorized parties are able to modify transmitted or stored information.
4. NON REPUDIATION- Requires that neither the sender, nor the receiver of message be able to deny the transmission.
5. ACCESS CONTROL- Requires access may be controlled by or for the target system.
6. AVAILIBILITY- Computer system assets are available to authorized parties when needed.

Characteristics of a cryptographic algorithm:

The main characteristics of cryptographic algorithm are

a) Level of security

b) Performance

c) Ease of implementation

a) Level of Security: -

The level of security is defined by an upper bound on the objective and is called the 'Work Factor'.

Manuscript received April 5, 2013
Manuscript revised April 20, 2013

Work Factor: The minimum amount of work required to compete the private key when given the public key, or in the case of the symmetric key scheme to determine the secret key.

Which algorithm is most effective for the given objective, will be determined by the basic properties of the algorithm. Algorithm could provide very different functionality depending on its mode of operation or usage.

b) Performance:-

Performance refers to the efficiency of an algorithm in a particular mode of operation. For example, the number of bits/sec at which it can encrypt may rate an encryption algorithm.

c) Easy of Implementation:-

The difficulty of realizing the algorithm in a practical instantiation, and might include the complexity of implementing in an either software or a hardware environment. For example, in an environment where computing power is limited, one may have to trade off very high level of security for better system performance.

Aspects of Security:-

To assess the security needs, of an organization effectively and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfied those requirements. The approach is to consider three aspects of information security.

1) Security Attack - Any action that compromises the security of information owned by an organization.

2) Security Mechanism - A mechanism that is designed to detect, prevent or recover from a security attack.

3) Security Services - A service that enhances the security of the data processing system and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanism to provide the service.

II. CRYPTOGRAPHY ALGORITHM – DES (DATA ENCRYPTION STANDARD)

Without doubt the first and the most significant modern symmetric encryption algorithm is that contained in the Data Encryption Standard (DES).The DES was published by the United States' National Bureau of Standards in January 1977 as an algorithm to be used for unclassified data (information not concerned with national security).

The Data Encryption Standard (DES), as specified in FIPS Publication 46-3, is a block cipher operating on 64-bit data blocks. The encryption transformation depends on a 56-bit secret key and consists of sixteen Feistel iterations surrounded by two permutation layers: an initial bit permutation *IP* at the input, and its inverse *IP*−1 at the output. The structure of the cipher is depicted in Figure 2. The decryption process is the same as the encryption, except for the order of the round keys used in the Feistel iterations.[12] The 16-round Feistel network, which constitutes the cryptographic core of DES, splits the 64-bit data blocks into two 32-bit words, LBlock and RBlock (denoted by *L*0 and *R*0). In each iteration (or round), the second word *Ri* is fed to a function ***f*** and the result is added to the first word *Li*. Then both words are swapped and the algorithm proceeds to the next iteration. The function f of DES algorithm is key dependent and consists of 4 stages.

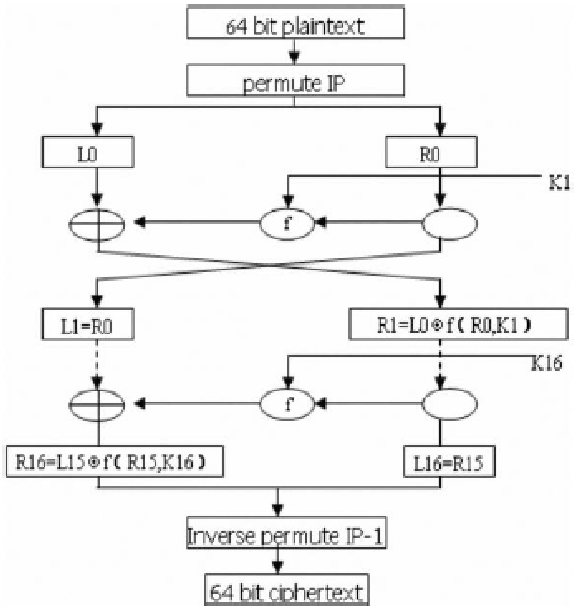


Figure 2.DES Algorithm

1. Expansion (E): The 32-bit input word is first expanded to 48 bits by duplicating and reordering half of the bits.[11]

2. Key mixing: The expanded word is XORed with a round key constructed by selecting 48 bits from the 56-bit secret key, a different selection is used in each round.

3. Substitution. The 48-bit result is split into eight 6-bit words which are substituted in eight parallel 6×4-bit S-boxes. All eight S-boxes are different but have the same special structure.

4. Permutation (P): The resulting 32 bits are reordered according to a fixed permutation before being sent to the output.

The modified RBlock is then XORED with LBlock and the resultant fed to the next RBlock register.The unmodified RBlock is fed to the next LBlock register. With another 56 bit derivative of the 64 bit key, the same process is repeated.

```
Pseudo Code : DES  Algorithm
INPUT: plaintext m1 . . . m64; 64-bit key K=k1 . . . k64 (includes 8 parity bits).
OUTPUT: 64-bit ciphertext block C=c1 . . .c64.
1. ( key schedule) Compute sixteen 48-bit round keys Ki, from K.
2. (L0, R0) □ IP(m1, m2,. . .m64) (Use IP Table to permute bits; split the result into left and right 32-bit halves L0=m58m50 . . . m8,R0=m57m49 . . . m7)
3. (16 rounds) for i from 1 to 16, compute Li and Ri as follows
3.1. Li=Ri-1
3.2. Ri = Li-1 XOR f (R i-1, Ki)
where f(Ri-1, Ki) = P(S(E(Ri-1) XOR Ki)), computed as follows:
(a) Expand Ri-1 = r1r2 . . . r32 from 32 to 48 bits, T □E(Ri-1).
(b)  T  '                                    □-bitT
character strings: T '= (B1 . . . B8)
(c)T "                              □(S1(B1), S2(B2
Here Si(Bi) maps to the 4-bit entry in row r and column c of Si
(d)T'"                                          □
of T"=t1t2 . . . t32, yielding t16t7 . . . t25.)
4. b1b2 . . . b64                               □
L16, R16.)
5. C        □-1 (IPb1b2 . . . b64).
6. End.
```

Algorithm 1. DES Algorithm

III. IMPROVED OPERATION OF FOUR STATES IN DES

To increase the security and key space, that makes the encryption algorithms more robustness to the intruders, a new manipulation bits process has been added in by using different truth table for manipulation bits process work on 4- states (0,1,2,3) , while the traditional binary process (XOR) work on (0, 1) bits only. The symbol # has been used to refer to the operator that execute this process use truth tables that shown in figure 3.[7]

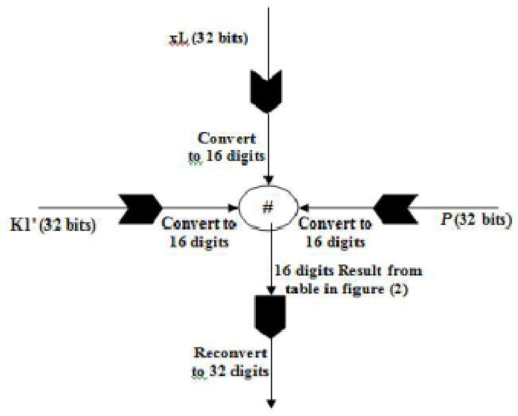


Figure 3.Design of Modified DES Algorithm

The new operation needs 3 inputs, the first one specify the table number that should be used to calculate the result among the 4 tables, the other 2 inputs define the row and column number in the specified table where the cross point of them gives the result.

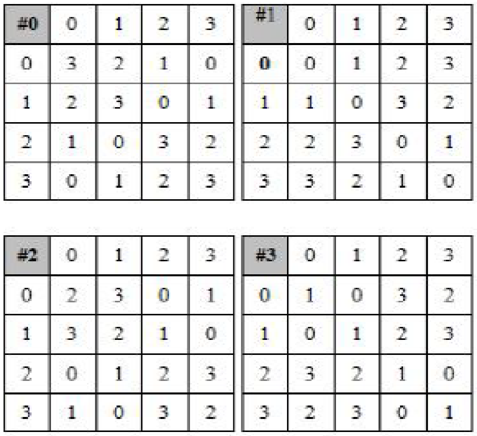
Here, example for # operation, this operation need 3 inputs, first one specify the table number that should be used to calculate the result among the four truth tables as shown in Table 1, the other 2 inputs define the row and column number in the specified table where the cross point of them gives the result this result is in 16 digits.

Input in 32 bit binary format

10010111010100101010011110100010001

Which is converted into the number 2 1 1 3 1 1 0 2 2 2 1 3 2 2 0 2 1

Input 1: 0 1 3 0 1 2 2 3 1
Input 2: 3 2 2 1 0 1 2 1 1
Input 3: 1 0 0 2 1 3 2 1 2
Result : 3 0 2 3 1 2 2 2 2



#0	0	1	2	3
0	3	2	1	0
1	2	3	0	1
2	1	0	3	2
3	0	1	2	3

#1	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

#2	0	1	2	3
0	2	3	0	1
1	3	2	1	0
2	0	1	2	3
3	1	0	3	2

#3	0	1	2	3
0	1	0	3	2
1	0	1	2	3
2	3	2	1	0
3	2	3	0	1

Table 1.Truth Table

IV. PROPOSED ALGORITHM OF DES

This research proposed a new improvement to the DES algorithm. The proposed improvement makes use of the new operation defined in the previous section, operation (#) applied during each round in the original DES algorithm, where another key is needed to apply this operation, this key may come in binary form and convert to a 4-states key. Here, originally DES algorithm linear cryptanalysis and differential cryptanalysis attacks are heavily depends on the S-box design.

Consequently, multiple keys will be used in each round of the original DES, the first key Ki will be used with the ***f*** function. The second key will be the first input to the # operation, the second input will be the output of the ***f*** function, and the third input to the # operation will be the value Li, Algorithm shows the three 32-bits input to the # operation ,and the 32-bits output, with places needed to convert these 32- bits to 16-digits. These three inputs to the # operation should be firstly converted from 32 bits to a 16 digits each may be one of four states (0,1,2, 3), i.e., each two bits converted to its equivalent decimal digits.

Algorithm of modified data encryption standard with 4 state operations:

```
Pseudo Code: New DES Algorithm
INPUT: plaintext m1 . . . m64; 64-bit two keys K=k1 . . . k64 and K'=k1' . . . k64' (includes 8 parity bits).
OUTPUT: 64-bit cipher text block C=c1 . . .c64.
1. ( key schedule) Compute sixteen 48-bit round keys Ki, from K.
1.1. (key schedule) compute sixteen 32-bit round keys Ki', from K'
2. (L0, R0)
permute bits; split the result into left and right 32-bit halves L0=m58m50 . . . m8,R0=m57m49 . . . m7)
3. (16 rounds) for i from 1 to 16, compute Li and Ri as follows:
3.1. Li=Ri-1
3.2. Ri = Li-1 # f (R i-1, Ki)
where f(Ri-1, Ki) = P(S(E(Ri-1) Å Ki)), computed as follows:
(a) Expand Ri-1 = r1r2 . . . r32 from 32 to 48 bits
T ← E(Ri-1). (Thus T= r32r1r2 . . . r32r1.)
 (b) T' ← T XOR Ki . Represent T ' as eight 6-bit character strings: T ' = (B1 . . . B8)
(c)T " ← F where Function
F = ((((((( S1+S2) mod 2 ^ 32) XOR S3) + S4) mod 2^32) XOR S5) +S6)mod 2^32
Here, Si(Bi) maps to the 8 bit entry in row r and column c of Si
(d)T"' ← P(T"). (Use P per table to permute the 32 bits of T"=t1 t2 …. t32, yielding t16t7 . . . t25.) and the operation # in Ri = Li-1 # f (R i-1, Ki) is computed as follows:
(I)Convert the 32 bits resulted from f (R i-1, Ki) into 4-states 16 digits call it f '
(II) Convert the 32 bits of Li-1 to 4-states 16 digits call it Li-1'
(III) Convert the 32 bits of Ki' to 4-states 16 digits call it Ki"
(IV) Compute Ri by applying the # operation on f ', Li-1', and Ki" according to truth tables shown in Table.
4. b1 b2 . . . b64          □ (R16, L16).
   (Exchange final blocks L16, R16.)
5. C ←IP-1 (b1b2 . . . b64). (Transpose using IP-1 C = b40b8 . . . b25.)
6. End.
```

Algorithm 2 Modified DES Algorithms

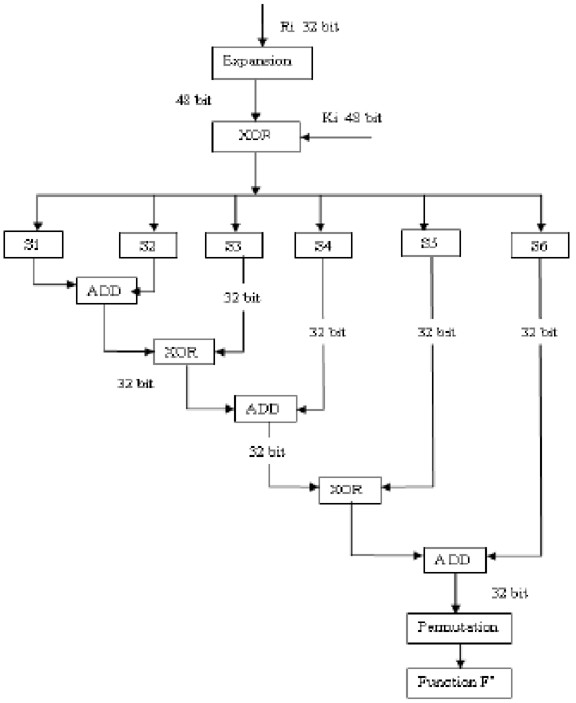


Figure 4.Function F Design

Here, using this proposed algorithm solve example .Our Input Message is 0123456789ABCDEF which is our plain text is converting into cipher text using this proposed algorithm. Here, there are 16 rounds for convert plain text to cipher text. In each round it contain two keys ,conversion of 16 bit data to 32 bit data and vice versa.

First we convert plain text into binary format also we have to convert key into binary format which is also in hex format. Now, performing all operation of this proposed algorithm and get the cipher text. Function F we have to given 8 bit input using that input we got 32 bit o/p from the s-box and perform XOR operation and ADD operation.

Step 1: Create Sub keys: K1 to K16 Key =133457799BBCDFF1

Step 2: Initial Permutation of Message which is given by User.
Step 3: for i =1 to 16 round Ln = Rn-1 Rn = Ln-1 # f(Rn-1,Kn)
Step 4: Convert 16 bit data into 32 bit data.

After complete one round we got
F' = 11 33 22 03 01 03 33 02
L' = 30 30 00 00 30 30 33 33
K' = 31 12 12 13 20 21 13 20
R1= 31 01 20 02 12 13 01 12

Here, R1 value found using truth table and got 16 bit data that is converted into 32 bit data.

R1 = 1101 0001 1000 0010 0110 0111 0001 0110

After completing all 16 rounds we got L16R16 value.

L16: 0000 1011 0011 0011 1110 1010 1001 0100
R16: 1111 0010 0111 0000 0000 0110 1111 0100
R16 L16 = 1111 0010 0111 0000 0000 0110 1111 0100 0000 1011 0011 0011 1110 1010 1001 0100

Now, Inverse of IP has been performed:

IP-1: 1010 0000 1110 1100 0000 0111 1000 1000 0111 0001 0111 1001 0101 101 0100 1011

So, finally we got our cipher text **A0EC07887178594B**

Now, compare this solution with our original des algorithm we got avalanche effect and also solve cryptanalysis attack.

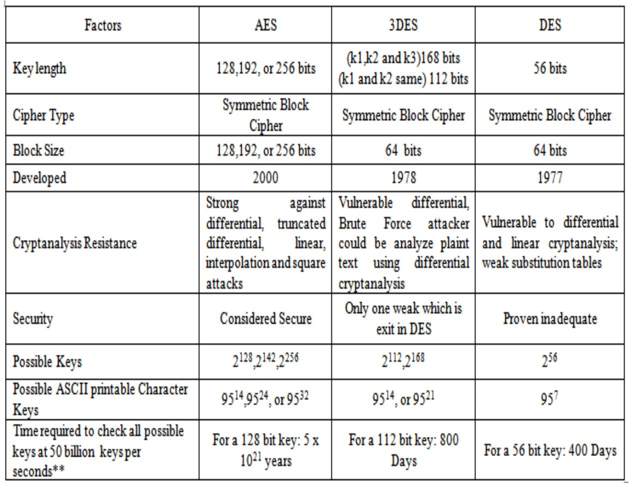
V.COMPARISON BETWEEN AES, 3DES AND DES:

Advance Encryption Standard (AES) and Triple DES (TDES or 3DES) are commonly used block ciphers. Whether you choose AES or 3DES depend on your needs. In this section it would like to highlight their differences in terms of security and performance (Seleborg, 2004).Since 3DES is based on DES algorithm, it will talk about DES first. DES was developed in 1977 and it was carefully designed to work better in hardware than software. DES performs lots of bit manipulation in substitution and permutation boxes in each of 16 rounds. For example, switching bit 30 with 16 is much simpler in hardware than software. DES encrypts data in 64 bit block size and uses effectively a 56 bit key. 56 bit key space amounts to approximately 72 quadrillion possibilities. Even though it seems large but according to today's computing power it is not sufficient and vulnerable to brute force attack. Therefore, DES could not keep up with advancement in technology and it is no longer appropriate for security. Because DES was widely used at that time, the quick solution was to introduce 3DES which is secure enough for most purposes today.3DES is a construction of applying DES three times in sequence. 3DES with three different keys (K1, K2 and K3) has effective key length is 168 bits (The use of three distinct key is recommended of 3DES.). Another variation is called two-key (K1 and K3 is same) 3DES reduces the effective key size to 112 bits which is less secure. Two-key 3DES is widely used in electronic payments industry. 3DES takes three times as much CPU power than compare with its predecessor which is significant performance hit. AES outperforms 3DES both in software and in hardware [17],[18].The Rijndael algorithm has been selected as the Advance Encryption Standard (AES) to replace 3DES. AES is modified version of Rijndael algorithm. Advance Encryption Standard evaluation criteria among others was [13],[14],[15],[16]:

- Security
- Software & Hardware performance
- Suitability in restricted-space environments
- Resistance to power analysis and other implementation attacks.

Rijndael was submitted by Joan Daemen and Vincent Rijmen.When considered together Rijndael's combination of security, performance, efficiency, implement ability, and flexibility made it an appropriate selection for the AES. By design AES is faster in software and works efficiently in hardware. It works fast even on small devices such as smart phones; smart cards etc.AES provides more security due to larger block size and longer keys.AES uses 128 bit fixed block size and works with 128, 192 and 256 bit keys. Rigndael algorithm in general is flexible enough to work with key and block size of any multiple of 32 bit with minimum of128 bits and maximum of 256 bits.AES is replacement for 3DES according to NIST both ciphers will coexist until the year2030 allowing for gradual transition to AES. Even though AES has theoretical advantage over 3DES for speed and efficiency in some hardware implementation 3DES may be faster where support for 3DES is mature.

Table 1: Comparison between AES, 3DES and DES



Factors	AES	3DES	DES
Key length	128,192, or 256 bits	(k1,k2 and k3)168 bits (k1 and k2 same) 112 bits	56 bits
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Block Size	128,192, or 256 bits	64 bits	64 bits
Developed	2000	1978	1977
Cryptanalysis Resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable differential, Brute Force attacker could be analyze plaint text using differential cryptanalysis	Vulnerable to differential and linear cryptanalysis; weak substitution tables
Security	Considered Secure	Only one weak which is exit in DES	Proven inadequate
Possible Keys	2^{128},2^{142},2^{256}	2^{112},2^{168}	2^{56}
Possible ASCII printable Character Keys	95^{14},95^{24}, or 95^{32}	95^{14}, or 95^{21}	95^{7}
Time required to check all possible keys at 50 billion keys per seconds**	For a 128 bit key: 5 x 10^{21} years	For a 112 bit key: 800 Days	For a 56 bit key: 400 Days

VI. CONCLUSION

In this paper a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism and comparative study between DES, 3DES and AES. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. There are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable. By adding additional key, modified S-Box design, modifies function implementation and replacing the old XOR by a new operation as proposed by this thesis to give more robustness to DES algorithm and make it stronger against any kind of intruding. A comparative study between DES, 3DES and AES were presented in to nine factors, Which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys, time required to check all possible key at 50 billion second, these eligible's proved the AES is better than DES and 3DES.

Acknowledgment

I would like to thank the management of V.S.B Engineering college, Karur. And I would like to extend my sincere thanks to the Principal, HOD and faculty members of Computer Applications Department, V.S.B Engineering College, Karur for their encouragement to publish this paper.

REFERENCES

[1] National Bureau of Standards – Data Encryption Standard, Fips Publication 46, 1977.

[2] O.P. Verma, Ritu Agarwal, Dhiraj Dafouti,Shobha Tyagi " Performance Analysis Of Data Encryption Algorithms " , 2011

[3] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha "Performance Evaluation of Symmetric Cryptography Algorithms", IJECT, 2011.

[4] Diaa Salama, Abdul Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoun"Performance Evaluation of Symmetric Encryption Algorithm ", IJCSNS, 2008

[5] Dr. Mohammed M. Alani " Improved DES Security" ,International Multi-Conference On System, Signals and Devices, 2010

[6] Tingyuan Nie, Teng Zhang "A Study of DES and Blowfish Encryption Algorithm",TENCON, 2009

[7] Afaf M. Ali Al- Neaimi, Rehab F. Hassan "New Approach for Modified Blowfish Algorithm Using 4 – States Keys", The 5th International Conference On Information Technology, 2011

[8] J.Orlin Grabbe "The DES Algorithm Illustrated"

[9] Dhanraj, C.Nandini, and Mohd Tajuddin "An Enhanced Approch for Secret Key Algorithm based on Data Encryption Standard", International Journal of Research And Review in Computer Science, August 2011

[10] Gurjeevan Singh, Ashwani Kumar, K.S. Sandha "A Study of New Trends in Blowfish Algorithm ", International Journal of Engineering Research and Application,2011

[11] W. Stallings, Cryptography and Network Security: Principles and Practices, 5th ed., Prentice Hall, 1999.

[12] B.Scheier, Applied Cryptography: Protocols, Algorithms and Source Code in C,2nd ed.., John Wiley & Sons, 1995.

[13] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "Novel Approach for Cover File of Hidden Data in the Unused Area Two within EXE File Using Distortion Techniques and Advance Encryption Standard.", Proceeding of World Academy of Science Engineering and Technology (WASET),Vol.56, ISSN:2070-3724, P.P 498-502.

[14] M. Abomhara, Omar Zakaria, Othman O. Khalifa , A.A.Zaidan, B.B.Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advance Encryption Standard ", International Journal of Computer and Electrical Engineering (IJCEE), ISSN: 1793-8198,Vol.2 , NO.2, April 2010, Singapore.

[15] A.W. Naji, Shihab A. Hameed, B.B.Zaidan, Wajdi F. Al-Khateeb, Othman O. Khalifa, A.A.Zaidan and Teddy S. Gunawan, " Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standared and Distortion Techniques", International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No 1 ISSN: 1947-5500, P.P 73-78,3 Aug 2009, USA.

[16] Hamdan. Alanazi, Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan, "New Frame Work of Hidden Data with in Non Multimedia File", International Journal of Computer and Network Security, 2010, Vol.2, No.1, ISSN: 1985-1553, P.P 46-54,30 January, Vienna, Austria.

[17] Alaa Taqa, A.A Zaidan, B.B Zaidan ,"New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm", International Journal of Computer and Electrical Engineering (IJCEE), Vol.1 ,No.5, ISSN: 1793-8163, p.p.566-571 , December (2009). Singapore.

[18] A.A.Zaidan, B.B.Zaidan, Hamid.A.Jalab," A New System for Hiding Data within (Unused Area Two + Image Page) of Portable Executable File using Statistical Technique and Advance Encryption Standard ", International Journal of Computer Theory and Engineering (IJCTE), 2010, VOL 2, NO 2, ISSN:1793-8201,Singapore.

K.Anchugam is presently working as Lecturer in Department of Computer Applications, at V.S.B. Engineering College, Karur, Tamilnadu, India. She has received her B.Sc(Computer Science) degree from Sri Saradha College of Arts and Science, Karur, Tamilnadu, India in 2002. She has received

her MCA degree from M.Kumarasamy College of Engineering, Karur, Tamilnadu, India in 2005.

M.Tamilselvi is Lecturer at Department of Computer Applications, Faculty of Engineering, Anna University, Karur, Tamilnadu, India. She has received her B.Sc degree from Navarasam Arts and Science College, Arachalur, Tamilnadu, India in 2007. She has received her MCA degree from Nandha Engineering College, Erode, Tamilnadu, India in 2010.