International Journal of Research

International Journal of Research (IJR)

e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015

Available at http://internationaljournalofresearch.org

Encryption and Decryption of Textual Data with Symmetric Key Cryptography and Improved Des Method Based on Irrational Number

Jai Singh[1], Md. Firoz Alam[2]

M.Tech Scholar, AL-Falah University, Haryana, India

EMAIL: zaismac@gmail.com[1], firoz2k@gmail.com[2]

Assit. Prof. Kamil Hasan

AL-Falah University, Haryana, India

EMAIL: kamilhasan@gmail.com

Abstract

In this paper we encrypt textual data with symmetric key cryptography based on irrational numbers, an improved scheme that enhances the randomness of sub-Key is proposed, in which the permutation is controlled by irrational number. DES (the Data Encryption Standard) is a symmetric block cipher developed by IBM. The algorithm uses a 56-bit key to encipher/decipher a 64-bit block of data. The key is always presented as a 64-bit block, every 8th bit of which is ignored. However, it is usual to set each 8th bit so that each group of 8 bits has an odd number of bits set to 1. DES (Data Encryption Standard) is a cryptographic standard. However, the applications of it are limited because of the small key space.

Key Words:

DES (Data Encryption Standard); Symmetric Key; Cryptography; Encryption; Decryption; Private Key; Ciphertext;

Introduction

DES is the most widely used symmetric algorithm in the world, despite claims that the key length is too short. Ever since DES was first announced, controversy has raged about whether 56 bits is long enough to guarantee security.

The key length argument goes like this. Assuming that the only feasible attack on DES is to try each key in turn until the right one is found, then 1,000,000 machines each capable of testing 1,000,000 keys per second would find (on average) one key every 12 hours. Most reasonable people might find this rather comforting and a good measure of the strength of the algorithm.

Those who consider the exhaustive key-search attack to be a real possibility (and to be fair the technology to do such a search is becoming a reality) can overcome the problem by using double or triple length keys. In fact, double length keys have been recommended for the financial industry for many years.

Use of multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times. If we consider a triple length key to consist of three 56-bit keys K1, K2, K3 then encryption is as follows:

- Encrypt with K1
- Decrypt with K2
- Encrypt with K3

Decryption is the reverse process:

- Decrypt with K3
- Encrypt with K2
- Decrypt with K1

Setting K3 equal to K1 in these processes gives us a double length key K1, K2.

Setting K1, K2 and K3 all equal to K has the same effect as using a single-length (56-bit key). Thus it is possible for a system using triple-DES to be compatible with a system using single-DES.

History and Concepts Used for DES

In January 1977, the U.S. Government adopted a product cipher developed by IBM as its official standard for unclassified information. This cipher, DES (Data

Encryption Standard), was widely adopted by the industry for use in security products. It is no longer secure in its original form, but in a modified form it is still useful. We will now explain how DES works.

Plaintext is encrypted in blocks of 64 bits, yielding 64 bits of ciphertext. The algorithm, which is parameterized by a 56-bit key, has 19 distinct stages. The first stage is a key-independent transposition on the 64-bit plaintext. The last stage is the exact inverse of this transposition.

The stage prior to the last one exchanges the leftmost 32 bits with the rightmost 32 bits. The remaining 16 stages are functionally identical but are parameterized by different functions of the key. The algorithm has been designed to allow decryption to be done with the same key as encryption, a property needed in any symmetric-key algorithm. The steps are just run in the reverse order. An outline of DES is shown in figure 1.

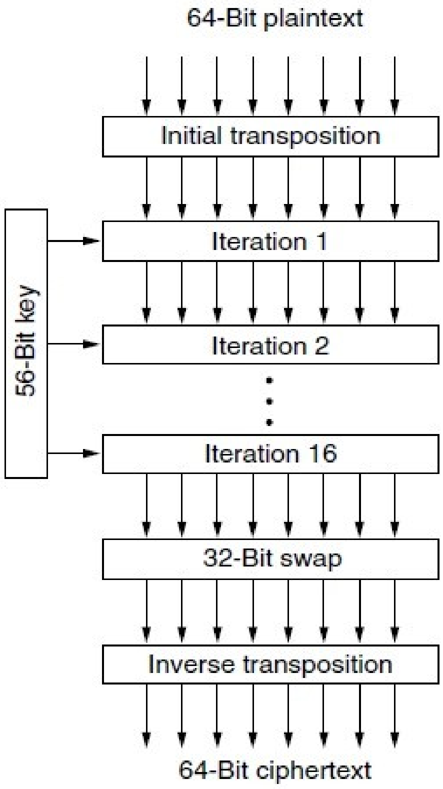


Figure 1: General Outline

The operation of one of these intermediate stages is illustrated in Figure 2. Each stage takes two 32-bit inputs and produces two 32-bit outputs. The left output is simply a copy of the right input. The right output is the bitwise XOR of the left input and a function of the right input and the key for this stage, Ki. Pretty much all the complexity of the algorithm lies in this function.

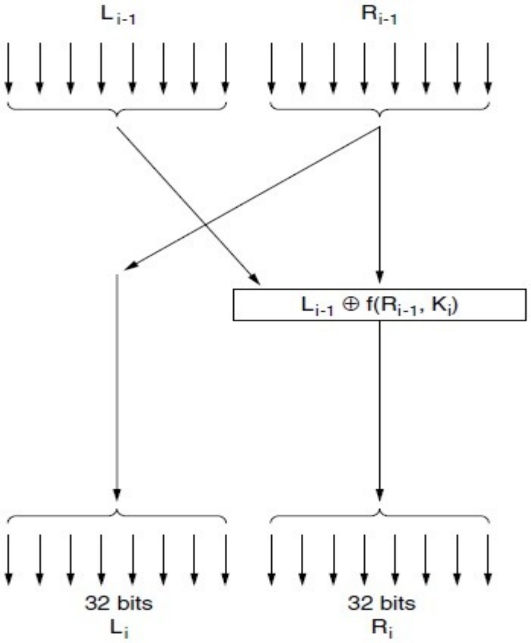


Figure 2: Detail of one iteration. The circled + mean exclusive OR.

The function consists of four steps, carried out in sequence. First, a 48-bit number, E, is constructed by expanding the 32-bit Ri − 1 according to a fixed transposition and duplication rule. Second, E and Ki are XORed together. This output is then partitioned into eight groups of 6 bits each, each of which is fed into a different S-box. Each of the 64 possible inputs to an S-box is mapped onto a 4-bit output. Finally, these 8 × 4 bits are passed through a P-box.

In each of the 16 iterations, a different key is used. Before the algorithm starts, a 56-bit transposition is applied to the key. Just before each iteration, the key is partitioned into two 28-bit units, each of which is rotated left by a number of bits dependent on the iteration number. Ki is derived from this rotated key by applying yet another 56-bit transposition to it. A different 48-bit subset of the 56-bits is extracted and permuted on each round.

A technique that is sometimes used to make DES stronger is called **whitening**. It consists of XORing a random 64-bit key with each plaintext block before feeding it into DES and then XORing a second 64-bit key with the resulting ciphertext before transmitting it. Whitening can easily be removed by running the reverse operations (if the receiver has the two whitening keys). Since this technique effectively adds more bits to the key length, it makes an exhaustive search of the key space much more time consuming. Note that the same whitening key is used for each block (i.e., there is only one whitening key).

DES is based on two fundamental attributes of cryptography: Substitution (confusion) and transposition (Diffusion). DES consists of 16 steps, each of which called as a Round. Algorithm:-

[1] In the first step, the initial 64-bit plain text block is handed over to in Initial Permutation (IP) function.

[2] The Initial permutation is performed on plain text.

[3] The initial permutation produce two halves of permuted block: Left Plain text (LPT) and Right Plain Text (RPT).

[4] Now, each of LPT and RPT goes through 16 rounds of encryption process, each with its own key:

a) From the 56-bit key, a different 48-bit Sub-key is generated using Key Transformation.

b) Using the Expansion Permutation, the RPT is expended from 32 bits to 48 bits.

c) Now, the 48-bit key is XORed with 48-bit RPT and resulting output is given to the next step.

d) Using the S-box substitution produced the 32-bit from 48-bit.

e) These 32 bits are permuted using P-Box Permutation.

f) The P-Box output 32 bits are XORed with the LPT 32 bits.

g) The result of the XORed 32 bits are become the RPT and old RPT become the LPT.This process is called as Swapping.

h) Now the RPT again given to the next round and performed the 15 more rounds.

[5] After the completion of 16 rounds the Final Permutation is performed.

Cryptography Terminology

a) **Plaintext**: The original intelligible message.

b) **Cipher text**: The transformed message.

c) **Cipher**: An algorithm for transforming an intelligible message to unintelligible by transposition.

d) **Key**: Some critical information used by the cipher, known only to the sender & receiver.

e) **Encipher**: (Encode) the process of converting plaintext to cipher text using a cipher and a key.

f) **Decipher**: (Decode) the process of converting cipher text back into plaintext using a cipher & key.

g) **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

h) **Cryptology**: Both cryptography and cryptanalysis

i) **Code**: an algorithm for transforming an intelligible message into an unintelligible one using codes.

j) **Hash algorithm**: Is an algorithm that converts text string into a string of fixed length.

k) **Secret Key Cryptography (SKC)**: Uses a single key for both encryption and decryption

l) **Public Key Cryptography (PKC)**: Uses one key for encryption and another for decryption

m) **Pretty Good Privacy (PGP)**: PGP is a hybrid cryptosystem.

n) **Public Key Infrastructure (PKI)**: PKI feature is Certificate authority.

Implementation Work and Concepts

It is no longer a question to attack the 56-bit key with the development of computer technology. The attacker can decipher DES within 20 hours through exhaustive key search.

DES based on Irrational Number

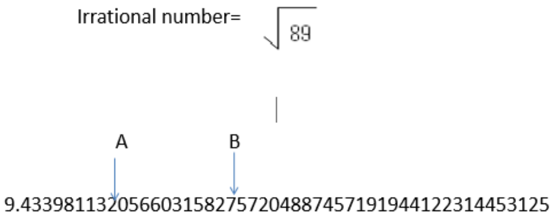
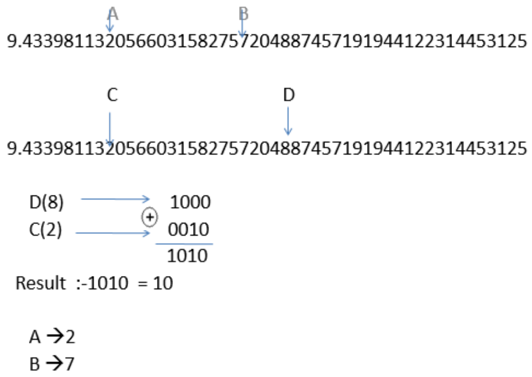


Figure 3: Example of irrational number.



Since result of XOR is even therefore we shift(left) the original key (59357) by A=2 bit

Initial key : 0000000000000000000000000000000000000000010110101110010010110010
Permutated key: 000000000000000000000000000000000010110111100101011001 00

In above images we just understood the irrational implementation in DES.

The 64-bit key is controlled by irrational number to shift before the sub-key being produced. Therefore the key is not directly involved in the production of the sub-keys.

In order to increase the randomness of sub-key, the production and the selection of ‘a’ and ‘b’ are all controlled by irrational number. The Location information of ‘a’ and ‘b’, used for shifting, is transmitted to the receiver through the safe channel. The location information will be one part of the key.

Advantage of irrational number in DES

The running time that DES took as much as that of the DES based on irrational number

Based on the same plain text and key, the cipher text of DES after several simulations is the same

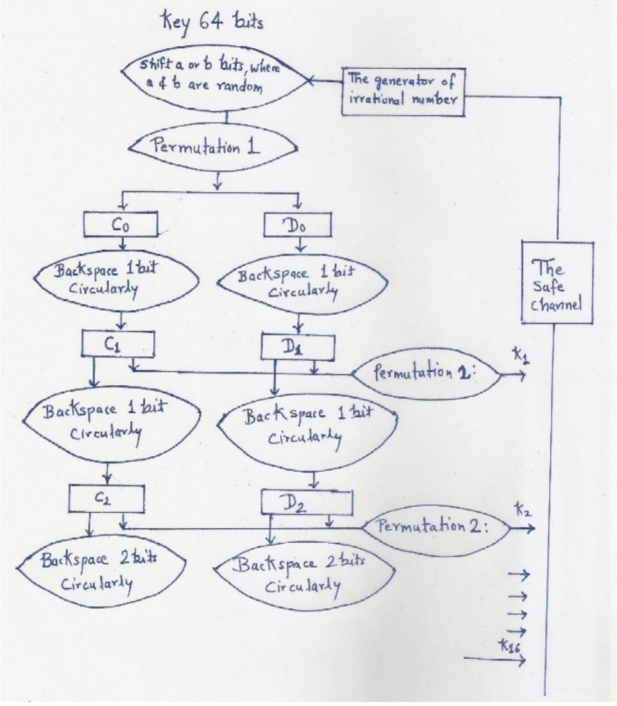

Key 64 bits
shift a or b bits, where a & b are random
The generator of irrational number
Permutation 1
C0
D0
Backspace 1 bit Circularly
Backspace 1 bit Circularly
The Safe channel
C1
D1
Permutation 2:
K1
Backspace 1 bit Circularly
Backspace 1 bit Circularly
C2
D2
Permutation 2:
K2
Backspace 2 bits Circularly
Backspace 2 bits Circularly
K16

Figure 4: implementation of key 64 bits when generate irrational number.

Results Simulation and Discussion

Now step of simulation

After code run we get the figure below

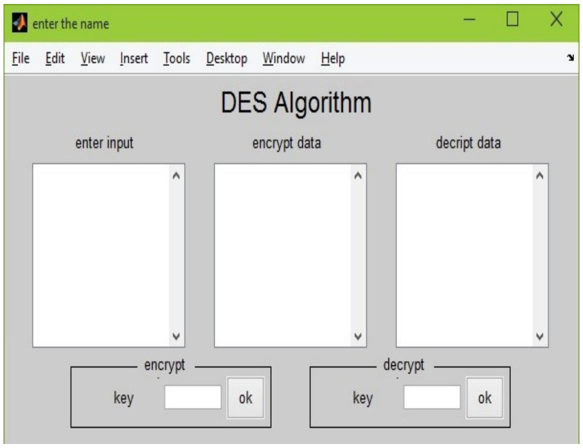
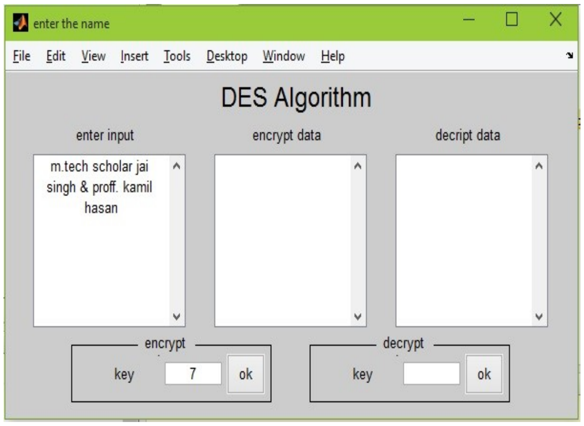


Figure 5: DES Algorithm for input, encryption and decryption

Step 1: In figure 5 we have option to input text and input any numeral key for encryption.

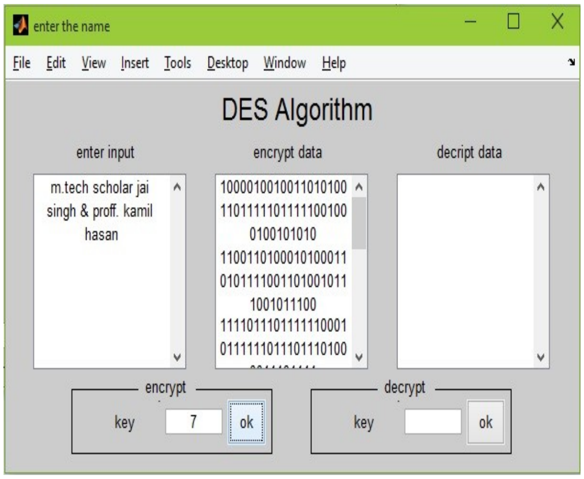


m.tech scholar jai singh & proff. kamil hasan

key 7

Figure 6: written name in enter input column of DES algorithm.

Step 2: After input text we apply numeral 7 Key for encryption of data shown in figure 6 or figure 7.



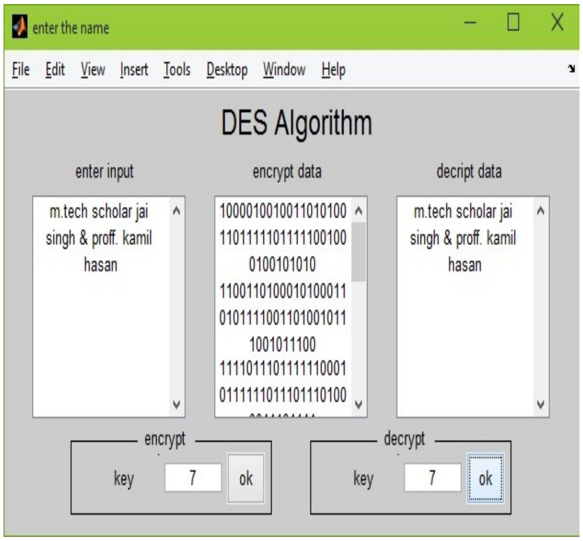
m.tech scholar jai singh & proff. kamil hasan

1000010010011010100
1101111101111100100
0100101010
1100110100010100011
0101111001101001011
1001011100
1111011101111110001
0111111011101110100

key 7

Figure 7: Encrypted data shown in binary code.

Step 3: After clicking on OK on encrypt key thereafter encrypted data generated shown in figure 7.



m.tech scholar jai singh & proff. kamil hasan

1000010010011010100
1101111101111100100
0100101010
1100110100010100011
0101111001101001011
1001011100
1111011101111110001
0111111011101110100

m.tech scholar jai singh & proff. kamil hasan

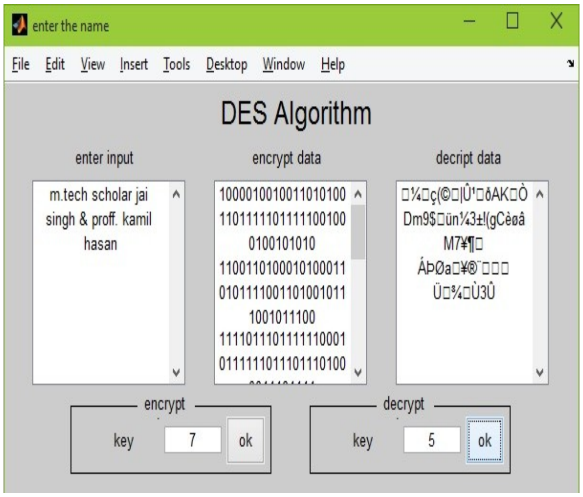
key 7

key 7

Figure 8: decrypted text data

Step 4: for decryption we first input the same numeral Key in decrypt as 7 then we get decrypted data same as enter input.

But if we enter different Key like 5 instead of 7 in above decrypt key then we get altered or corrupt data from input data which shown in figure 9.



m.tech scholar jai singh & proff. kamil hasan

1000010010011010100
1101111101111100100
0100101010
1100110100010100011
0101111001101001011
1001011100
1111011101111110001
0111111011101110100

□¼□ç(©□|Û¹□ðAK□Ò
Dm9$□ün¼3±!(gCèøâ
M7¥¶□
ÁÞØa□¥®¨□□□
Ü□¾□Ù3Û

key 7

key 5

Figure 9: Corrupted decrypt data

Conclusion

This paper clearly improve the DES method by applying irrational number with DES scheme. DES is mostly used for long message but we need security because we use only one key for encryption and decryption so we add irrational number to enhance more security and by applying this method we get idea to apply more new method to secure more DES scheme and in future we can use DES to secure even our html website or many over internet & communication fields.

References:

[1.] Sombir Singh, International Journal of Advanced Research in Computer Science and Software Engineering "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", Volume 3, Issue 6, June 2013, ISSN: 2277 128X

[2.] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, November 16, 2005.

[3.] Subbarao V. Wunnava, "Data Encryption Performance and Evaluation Schemes", Florida International University, Miami, FL Ernest0 Rassi; Florida Intemational University, Miami, FL 0-7803-7252-2/02/$10.00 0 2002 IEEE Proceedings IEEE Southeastcon 2002.

[4.]Gaurav Shrivastava, "Analysis Improved Cryptosystem Using DES with RSA" VSRD-IJCSIT, Vol. 1 (7), 465-470, 2011.

[5.]A Tanenbaum, Computer Networks, 5th Edition.

[6.]Narender Tyagi, Anita Ganpati, International Journal of Advanced Research in Computer Science and Software Engineering “Comparative Analysis of Symmetric Key Encryption Algorithms”, Volume 4, Issue 8, August 2014, ISSN: 2277 128X.

[7.]Alam Md Imran, Khan Mohammad Rafeek. “Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013, pp.713-720.

[8.] Akanksha Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", International Journal on Computer Science and Engineering (IJSCE), Vol. 4 No. 09 sep 2012.

[9.] Kuppuswamy, P. and Al-Khalidi, S.Q.Y. (2012), ‘Implementation of Security through simple symmetric key algorithm based on modulo 37’, International Journal of Computers & Technology, Vol. 3, No. 2, pp. 335-338.

[10.] Jai Singh, Kanak Lata and Javed Ashraf, International Journal of Current Engineering and Technology, “Image Encryption & Decryption with Symmetric Key Cryptography using MATLAB”, ©2015 INPRESSCO®, All Rights Reserved, Vol.5, No.1 (Feb 2015), E-ISSN 2277 – 4106,
P-ISSN 2347 –5161 Available at http://inpressco.com/category/ijcet, pp. 448-451.