Military Technical College
Kobry Elkobbah,
Cairo, Egypt

ICEENG 99

2nd International Conference
on Electrical Engineering
ICEENG 99

THE MODIFIED-I/O DES BLOCK CIPHER

Mostafa Abdel-Kader[1] **Mohamed Sharrawy[2]** **Alaa ELdin Fahmy[3]**
Hithem Youseef Zorkta[4]

ABSTRACT

Data Encryption Standard (DES) has been broken [1]. The classical alternative, triple-DES, is too expensive for many users, taking three times the computation of DES itself [1]. Therefore, the modified-I/O DES has been presented. The modified-I/O DES is based on DES but it is stronger than DES itself. It uses 120 bits key length and it is much faster than triple-DES.

1. INTRODUCTION

In 1974, the National Bureau of Standards (NBS), now the National Institute of Standards and Technology (NIST), published a request in the August 27th issue of the Federal Register, asking for proposals for a standard cryptographic algorithm. They eventually received an algorithm based on LUCIFER, an algorithm developed by IBM in the early 1970's. After rigorous testing and a mysterious reduction of the key size from 112 bits to 56 bits, the DES was adopted as a federal standard on November 23, 1976 and was authorized for use on all unclassified government communications. The terms of the standard require that the DES be reviewed every 5 years. As of 1995, there is still no government-endorsed alternative to the DES [2]. The DES algorithm uses a 56 bits key and operates on blocks of 64 bits of data. The data undergoes 16 iterations each driven by a 48 bits iteration key; for the iteration key a selection of the 56 master bits is made (which bits are used in each iteration is fixed and public). In each iteration, half of the data is passed unchanged and combined with the key to mess up the other half. For more details about the architecture of DES one can consult [3][4]. With a 56- bit key, there is a large but

1 Prof. Dr., Communication dept., Military Technical College.
2 Ass. Prof. Dr., Computer dept., Military Technical College.
3 Ph.D., Radar dept., Military Technical College.
4 Ph.D. Candidate, Computer dept., Military Technical College.

limit to the number of keys you need to check, on average 2^{55}, which is the same as $3.6 * 10^{16}$. Pick an acceptable time for cracking a key (say two hours) and you know how many keys you have to check per second (5 trillion). That may sound impossible, but it isn't. A $10 Application- Specific Integrated Circuits (ASIC) chip can test 200 million keys per second. A $10 million investment in ASIC will build a DES- cracker that can break a key every six minutes, and a $300 million investment can break a key every twelve seconds [5][6].

Two ways were used to aging the DES, either modifying the DES itself, or using the DES as a component of a new version of the DES. In the first way, several suggestions were made in the last two decades in order to strengthen DES, which can be briefed as follows:

- Increasing the number of rounds from 16 to 32, 64 or even more [7];
- Multiple encryption or larger key size [8];
- Independent sub keys (768 bits) [9];
- Dramatic increase of the key scheduling complexity [10][11];
- Random key dependent S-boxes (as in Khufu [12]);
- Key-dependent invariant S-boxes transformation [13].
- In the second way, we can see the triple-DES [1][14].

In this paper, a new proposal is introduced (MODIFIED-I/O DES), which is based on DES, but it is stronger than DES (120 bits key length are used) and it is faster than the classical alternative triple-DES.

2. THE PROPOSED STRUCTURE FOR MODIFIED-I/O DES

Figure 1 shows the proposed structure for modified-I/O DES.

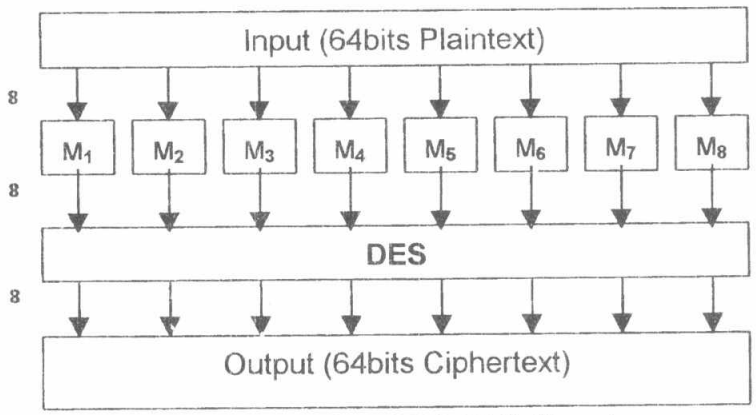

Fig.1 Modified-I/O DES Structure

The substitution tables (we call it here M-layers) are filled with the output of a chaotic generator (CG), which will be discussed in the next section. These substitution tables are initialized before ciphering, and its contents will not be changed during the session key. The message information flows through DES itself, after it has been modified with M-layers. This means that the overall cipher cannot possibly be weaker than DES.

2.1 How to Fill the M-Layers

The M-Layers is simply eight one-dimensional arrays with 256-byte length for each. A chaotic generator (CG) is used to fill these layers as follows:

1. $X_n = X_0$, initial point, $X_0 \in (0,1)$.
2. While $I < 8$, Do:
3. While $j < 256$, Do:
4. $Y = (X_{n+1} * 1000) \% 256$.
5. Test Y, if it was produced and selected to be one of the layer's elements;
6. YES: Ignore Y
7. NO : Save Y in the corresponding position in the layer
8. $X_n = X_{n+1}$
9. Go to Step4

2.2 M-Layers in Encryption

As seen in Fig1, we have a 64 bits plaintext to be encrypted;

- Divide the 64 bits plaintext into 8 blocks each 8 bits length.
- Change each block into its decimal value in [0-255], so the output of this step is $Y_1\ Y_2\ Y_3\ Y_4\ Y_5\ Y_6\ Y_7\ Y_8$
- Where Y_I is the decimal value for block I, $1 \le I \le 8$
- $C_I = M_I[Y_I]$ where $C_I \in [0\text{-}255]$
- Change each C_I into 8 bits binary form.
- The final output is 64 bits, which will be the input to the DES.

2.3 M-Layers in Decryption

- Divide the input (64 bits, output of DES in the decryption mode) into 8 blocks.
- Change each block into its decimal value in [0-255], so the output of this step is $K_1\ K_2\ K_3\ K_4\ K_5\ K_6\ K_7\ K_8$
- Search the layer M_I for the value K_I until $K_I = M_I[X_I]$ where $X_I \in [0\text{-}255]$
- Change each X_I into 8 bits binary form.
- The final output is 64 bits, which will be the original plaintext.

3. HOW TO MAKE USE OF CHAOS

Most of electrical engineers try to avoid chaos in their design. But here, we introduce how to make use of chaos in the field of cryptography. In this way, we present the one-dimensional (1-D) chaotic map to build a random number generator. One of the most known non-linear 1-D chaotic maps is the logistic map [15]. It can be described by the following difference equation:

$$X_{n+1} = \mu X_n (1 - X_n), \qquad X_n \in (0,1)$$

Where, μ represents a non-linear parameter, which affects the behavior of the map dramatically. That is, it brings the map from a fixed point to the route of chaos.

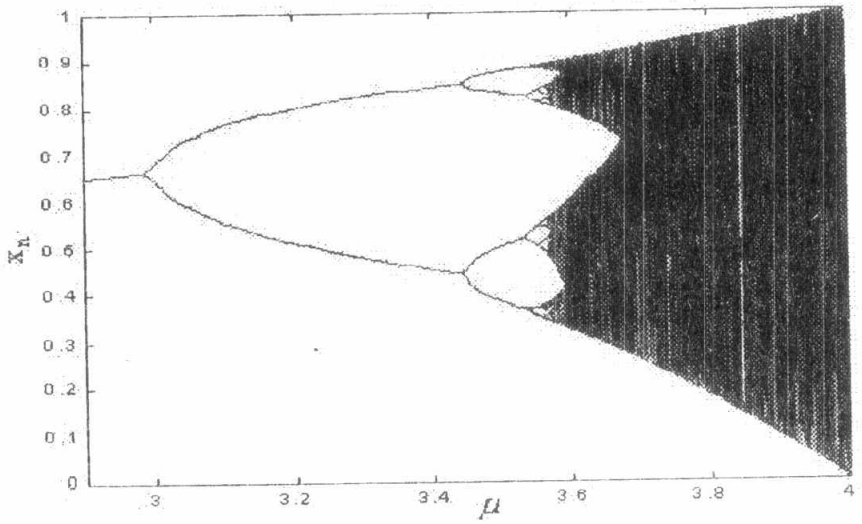

Fig.2 Bifurcation Diagram Of 1-D Chaotic Map

Figure 2 can briefly illustrate the global behavior of the 1-D chaotic map. It is clear that, for $\mu \cong 3$, we have a fixed point, increasing $\mu \cong 3.4$, we have period-2. Increasing μ slightly we get period-4, and so on until $\mu \cong 3.56$ the chaotic region begins, and we have an infinite number of solutions. We use the chaotic region, with $\mu \cong 3.9$, to construct our random number generator, which we call it Chaotic Generator (CG).

4. MODIFIED-I/O DES STRENGTH AND SIMULATION RESULTS

Rather than attempt to analyze the whole design at once, it seems worthwhile to discuss the strength of the substitution layer and its effect on the design. In this way, we have a better chance of seeing the overall strength when we use it with a combination of the strength of the DES itself.

4.1 With Known Substitutions

In Modified-I/O DES structure, all data flow through every layer in it. Even, if the substitutions are known, they do not undo the confusion that DES provides. Therefore, the absolute minimum strength of Modified-I/O DES with known substitutions is the same as DES. Many researchers made great efforts to cryptanalyze DES. Their work lead to development of two powerful methods of cryptanalysis of iterative ciphers: differential cryptanalysis [16] and linear cryptanalysis [17]. Recently, Davies' attack [18] has been improved to be capable of breaking DES faster than exhaustive search [19]. Those are the only known methods of breaking DES faster than half of exhaustive search, they require huge amounts of 2^{47}, 2^{43} and 2^{50} plaintexts, respectively. In fact, these attacks on DES are impractical (due to the enormous amounts of data required).

4.2 With Known DES Key

Here we try to understand the strength of the fencing layer (M-Layers). If we assume that the DES key is known, then, the only remaining strength is in the fencing layer.

Thus, here we examine the ability of the input substitutions to hide the value going into the DES ciphering. The attack consists of trying all possible plaintext values until the known ciphertext value appears on the output. This will identify a single element in each input substitution. For a given 64-bit input value, there are eight 8-bit values, which select some value in eight different keyed input substitutions. There are 256 possible values for each of the eight substitutions, for 256^8 or 2^{64} possibilities. Therefore, the strength of Modified-I/O DES with a known DES key is 64 bits.

The Chaotic Generator (CG) has been used to fill the M-Layers. It has the following cryptographic properties:

- Nonlinear function with a chaotic behavior;
- Non-linear parameter μ, which dramatically affects the behavior of the map;
- Very sensitive to the initial conditions;
- Unpredictable, and
- Uproducable.

Local randomness tests have been applied to the resulting ciphertext, as shown in Figs (3.1-3.3). It is clear that the resulting ciphertext has a randomness behavior. C++ programs were used to simulate the DES algorithm, on 233MHz PC with 32MB RAM, and the measured time in encryption and decryption operations were considered as standard values. The substitution layer ($M_1 - M_8$) was added on the same program and the time was measured again. Table 4.1 illustrates these values in comparative with the original DES and the classical alternative triple-DES.

Table 4.1 Comparative Evaluation (key length- computation time)

DES	Modified-I/O DES	Triple-DES
56 bits key length	120 bits	168 bits
T (time unit)	1.2T (time unit)	3T(time unit)

5. CONCLUSION

When the DES key is known, but the fencing substitutions are unknown, the strength of modified-I/O DES is 64 bits. When the fencing substitutions are known, but the DES key unknown, the strength of modified-I/O DES is 56 bits. These operations are independent; therefore, when both the fencing substitutions and the DES key are unknown, the strength of modified-I/O DES is 120 bits. A120-bit key search will identify the DES key and one element in each of eight small substitutions; for a complete break, the remaining 255 values in those eight substitutions must still to be found. Thus, the strength of modified-I/O DES exceeds 120 bits.

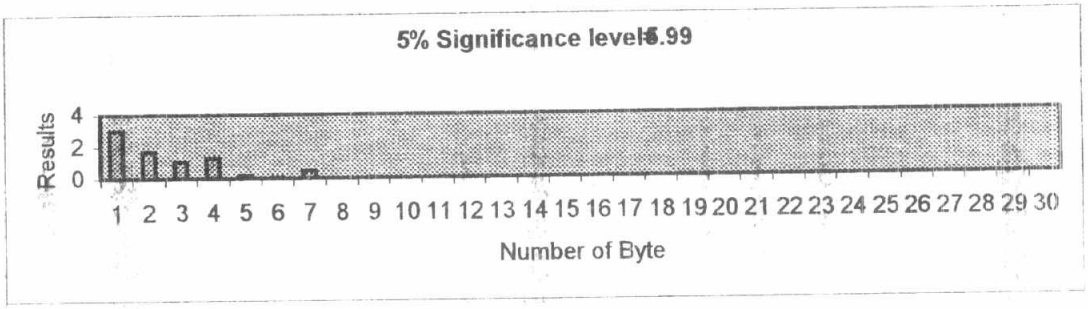

Fig 3.1 Serial Test

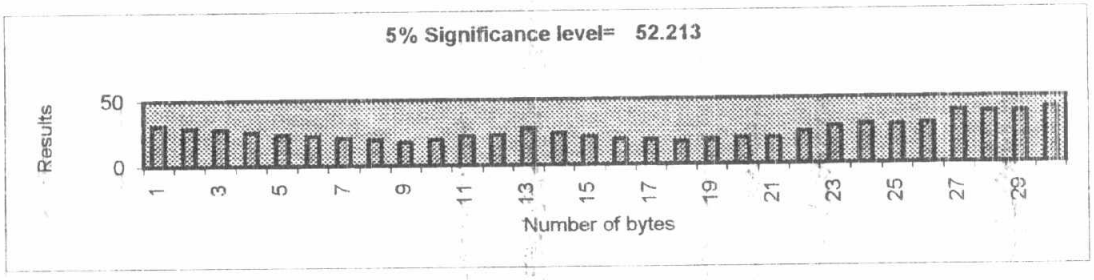

Fig 3.2 Frequency Test

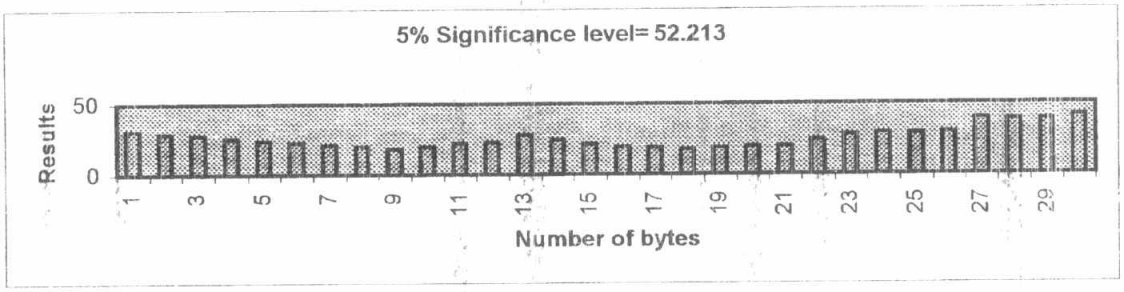

Fig 3.3 Poker Test

Table 4.2 AutoCorrelation Test

Number of tested bytes	χ^2 calculated	χ^2 at 5%	Result
8	0.15469	7.77497	pass
24	6.12737	26.2840	pass
40	10.7716	42.5520	pass
56	23.3051	61.6580	pass
72	21.5428	79.0781	pass
88	39.4908	97.3478	pass
104	71.6227	116.300	pass
120	34.6539	134.366	pass
136	29.4621	150.200	pass
152	61.8513	168.900	pass
168	50.8689	186.143	pass

REFERENCES

[1] http://www.io.com/~ritter/FENCED.HTM
[2] http://home.sprynet.com/sprynet/hafeez/crypto.htm
[3] Douglas R. Stinson, Cryptography: Theory and Practice CRC Press 1995, 0-8493-8521-0.
[4] http://www.sar.usf.edu/~magilo/security/des.htm
[5] http://www.viacorp.com/books.html/crypto.html
[6] M. Blaze, W. Diffie, R. L. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M.Wiener, Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, January 1996.
[7] M. Hellman, R. Merkle, R. Schroeppel, L. Washington, W. Diffie, S. Pohling, P. Schweitzer, Results of an Initial Attempt to cryptanalyze the NBS Data Encryption Standard, Information Systems Laboratory Report, Stanford University, November 1976.
[8] W. Diffie, M. Hellman, Exhaustive Cryptanalysis of the NBS Data Encryption Standard, IEEE Computer, Vol. 10, No. 6, pp. 74 - 84, June 1977.
[9] Thomas A. Berson, Long key variants of DES, Advances in Cryptology, Proceedings of CRYPTO'82, pp. 311 – 313, 1982.
[10] Lars Knudsen, On the Design of Secure Block Ciphers, Fast Software Encryption, Proceedings of Cambridge security workshop, pp. 9 – 11, December 1993.
[11] J. Quisquater, Y. Desmedt, M. Davio, The Importance of 'Good' Key Scheduling Schemes, Proceedings of CRYPTO'85, pp. 537 – 542, 1985.
[12] Ralph C. .Merkle, Fast Software Encryption Functions, lecture Notes in Computer Science, Advances in Cryptology, Proceedings of CRYPTO'90, pp. 476 – 501, 1990.
[13] Eli Biham, Alex Biryukov, How to Strengthen DES Using Existing Hardware, Proceedings of ASIACRYPT'94, pp. 398 – 412, 1994.
[14] http://www.swiss.ai.mit.edu/60...froomkin-metaphor/partIAB.html
[15] G.L. Baker and J.P. Gollub, Chaotic Dynamics an introduction, Cambridge University Press, 1990.
[16] Eli Biham, Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.
[17] Mitsuru Matsui, Linear Cryptanalysis Method for DES Cipher, Proceedings of EUROCRYPT'93, pp. 386 - 397, 1993.
[18] D.W. Davies, Investigation of a Potential Weakness in the DES Algorithm, private communications, 1987.
[19] Eli Biham, Alex Biryukov, An Improvement of Davies' Attack on DES, Proceedings of EUROCRYPT'94, 1994.