International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 11 (2015) pp. 29327-29335

http://www.ripublication.com

Analysis of Avalanche Effect In Modified Des Algorithm

Dr. Raja Sekhar Krovi[1], Pujyasri Jetty[2]
[1]Professor, Department of Computer Science and Engineering,
K L University, Vaddeswaram, Guntur District, Andhra Pradesh, India.
rajasekhar_cse@kluniversity.in
[2]Student, Department of Computer Science and Engineering,
K L University, Vaddeswaram, Guntur District, Andhra Pradesh, India.
pujyasri.jetty@gmail.com

Abstract

Data Encryption Standard (DES) is an encryption algorithm which is primarily used in applications where block cipher mode of operation is required. It is further modified as Double DES (2DES), Triple DES (3DES) in order to provide added security due to extra key length. DES is susceptible to brute force attack and 2DES for meet in middle attack. In this paper we implement a modified DES algorithm in Cipher Block Chaining mode of operation in which key generation procedure differs by using a 112 bit key and the plain text is encoded using a modified playfair technique as input to DES encryption function. Variations in the avalanche affect are observed in the results. Experimental results exhibit a higher avalanche effect in 60% of the cases using the modified DES algorithm.

Key Words: Data Encryption Standard (DES), Avalanche effect, PlayFair cipher, Brute force attack, meet in middle attack.

Introduction

Des Algorithm

Data Encryption Standard (DES) is adopted in 1977 by National Bureau of Standards, which now is the National Institute of Standards and Technology. The algorithm is referred as the Data Encryption Algorithm (DEA). It is a symmetric encryption algorithm and is a block cipher. It follows the Feistal Structure.

Plain Text: 64-bits[1].
Key: 56- bits (of the 64 bits given only 56 bits are used.)
Number of rounds: 16.
Cipher Text: 64- bits.

A 64 bit input plain text and a 64 bit key are taken as the input in DES algorithm. From the 64 bit input key by using permutation function a 56 bit key is obtained. It serves as the master key to generate the 16 round keys for the encryption.

Key Generation Algorithm:

1. The 56 bit key after permutation serves as master key.
2. For every round 'i' the 56 bit key is divided into two halves (C_{i-1}, D_{i-1}) of 28 bits each.
3. The two halves are subjected to left circular shift (by one or two bits depending upon the round) to obtain C_i, D_i.
4. Now Permuted Choice - 2 (permutation function) is applied on the output of (iii) to obtain the 48 bit round key K_i.
5. C_i, D_i serve as input to round 'i+1' and the process is repeated to generate the 16 round keys.

Encryption Algorithm:

1. The plain text is taken as input for initial permutation function and a 64 bit output is obtained.
2. The obtained 64 bit output is now subjected to round function for the 16 rounds of the encryption process with the respective round key.
3. The 64 bit output of 16 th round is swapped (left, right 32 bits).
4. The swapped 64 bits are then subjected to inverse initial permutation function and the result obtained is the cipher text.

The DES decryption algorithm is same as the encryption algorithm but the inputs, order of keys differ. The cipher text is the input for decryption algorithm. The keys in decryption algorithm are used in the reverse order to the order used in the encryption algorithm.

Double, Triple Des Algorithm

DES algorithm is susceptible to brute force attack due to its small key size (56 bit key). Hence the 2DES, 3DES algorithms are proposed as an extension to the DES algorithm to mitigate this defect.

In the 2DES algorithm a 112 bit key is used and the DES encryption algorithm is applied twice, encrypting the [lain text with both the keys. But this is no added advantage as by using the meet in the middle attack the effective resultant key size is in order of 2^{56} not 2^{112} which is not a vast improvement from DES where it is 2^{55}.

Thus 3DES algorithm is proposed which has a 168 bit key, DES is applied thrice using the three 56 bit keys (as encryption by Key1, decryption by Key2, encryption by Key3) during the 3DES encryption algorithm. The 3DES overcomes the disadvantage of both the brute force and meet in the middle attack. But the encryption and decryption take more time. But this is accepted standard as per 'NIST Special Publication 800-67 Revision 1 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher'.

Modified Des: Key Generation

In paper [2] a modified DES key generation algorithm which incorporates the features of DES, Playfair cipher and Vigenere cipher is proposed. In addition to the added advantage of increased avalanche effect a 112 bit key is incorporated in our proposed modification thereby enhancing security.

In modified DES algorithm a 128 bit key is the input. It is further divided into two keys (denoted by A, B) of 64 bit each.

Algorithm:

1. The 64 bit keys A, B are subjected to DES key generation algorithm in order to obtain two sets of 16 round keys denoted by A_1, A_2, A_3…… A_{16} and B_1, B_2, B_3…… B_{16}.
2. In the modified DES key generation a pair of round keys for the round 'i' A_i, B_i are taken and subjected to the rail fence cipher.
3. Let $_{Ai}$, $_{Bi}$ be denoted as
   A_i [a1, a2, a3……, a47, a48]
   B_i [b1, b2, b3……, b47, b48]
4. Using the rail fence cipher of depth 8 both the keys are combined as follows in a 8*12 matrix

a1	a9	a17	a25	a33	a41	b1	b9	b17	b25	b33	b41
a2	a10	a18	a26	a34	a42	b2	b10	b18	b26	b34	b42
a3	a11	a19	a27	a35	a4	b3	b11	b19	b27	b35	b43
a4	a12	a20	a28	a36	a44	b4	b12	b20	b28	b36	b44
a5	a13	a21	a29	a37	a45	b5	b13	b21	b29	b37	b45
a6	a14	a22	a30	a38	a46	b6	b14	b22	b30	b38	b46
a7	a15	a23	a31	a39	a47	b7	b15	b23	b31	b39	b47
a8	a16	a24	a32	a40	a48	b8	b16	b24	b32	b40	b48

5. The data is filled column wise and it will be read row wise. The rows 1 to 4 for key A_i, rows 5 to 8 for the key B_i.

Thus the new modified keys A_i, B_i are:

A_i^1 [a1, a9, a17, a25, a33, a41, b1, b9……, a2, a10……, b34, b42, a3, a11… ……b35, b43, a4, a12…….b36, b44]

B_i^1 [a5, a13, a21, a29, a37, a45, b5, b13……, a6, a14……, b38, b46, a7, a15 ……b39, b47, a8, a16…….b40, b48].

Let the modified sets of round keys be denoted by A^1, B^1.

Advantage:

2DES is susceptible to meet in middle attack in spite of its 112 bit key. For a known pair of plain text and cipher text 2^{56} operations or tries are required to get the correct keys instead of 2^{112}. This is because for every pair of keys K1, K2 and plain text P, Cipher text C in 2 DES

E(P, K1) = D(C, K2).

Here the 56 bit keys K1, K2 have 2^{56} different possible combinations. And we can use brute force for each combination, encrypt or decrypt the data respectively, match the results in a table and retrieve the keys K1, K2 using the above equation. Thus the exhaustive search is in order of 2^{56} using brute force for both the keys.

In modified DES algorithm this defect is rectified. As rail fence cipher is used in the generation of the 16 round keys here both the 56 bit keys A, B influence both the sets of the round keys generated [3] thus increasing complexity. Thus in order to obtain the keys the key space is 2^{112}.

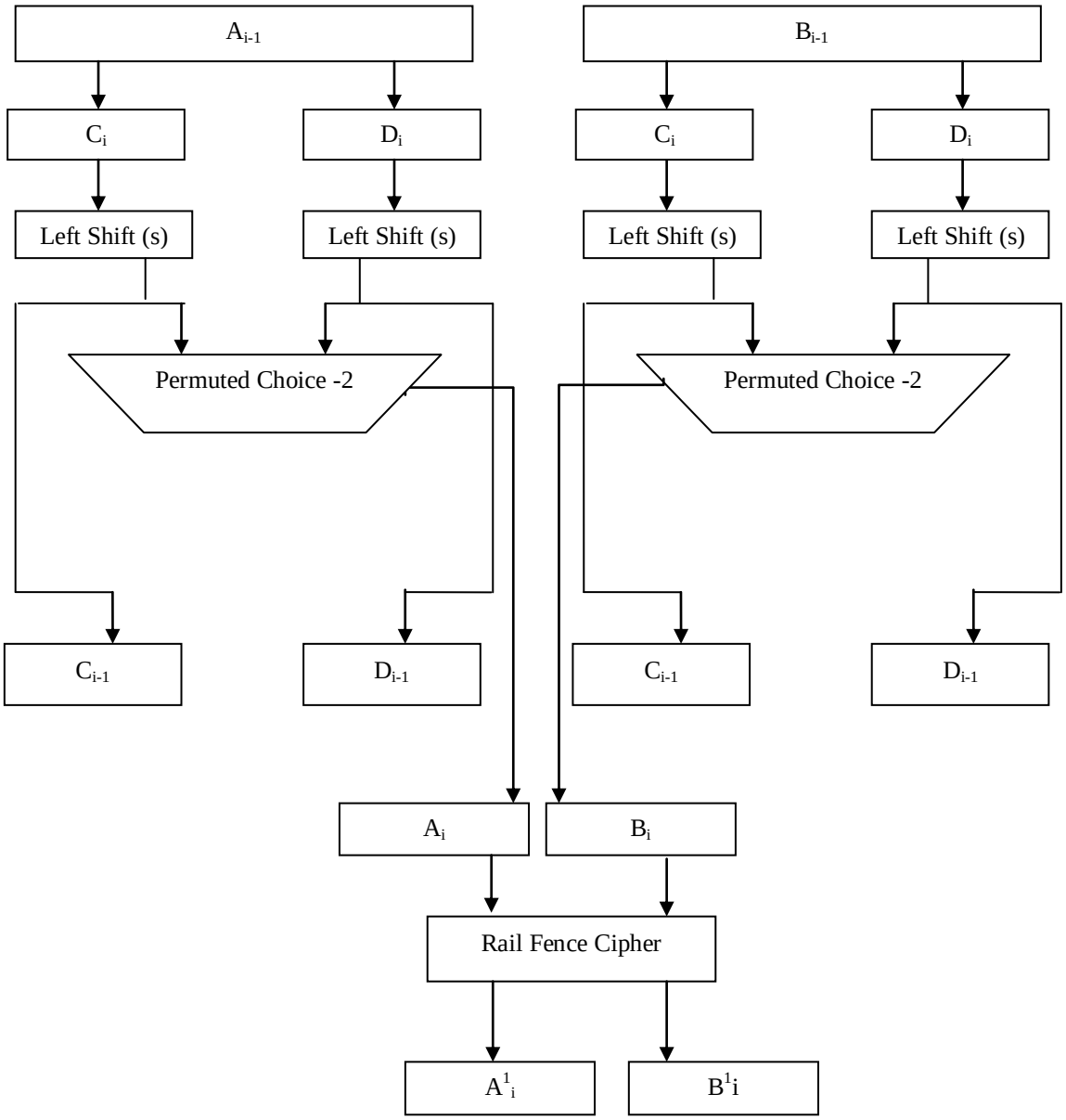

Figure 1: Single Round Key Generation in Modified DES algorithm.

Modified Des: Encryption

In paper [4] and [5] the plain text is encoded in various binary formats before encrypting it with the DES algorithm. This resulted in higher avalanche effect due to the scrambling of the plain text done prior.

Similarly in the modified DES algorithm the plain text is subjected to a modified playfair cipher before it is given as input to the DES algorithm. The modified algorithm combines the principle of scrambling of bits or data as done in classical encryption techniques in combination with the block cipher which results in an increase in avalanche effect and complexity [6].

In playfair cipher technique only a 5*5 matrix is considered and it accommodates only 25 characters of English language (either Capital or Small case). The letter 26, white spaces, special characters etc… are not present. In paper [7] it is further modified by considering both sets of English alphabet and special characters. In the proposed algorithm we further improvise by considering all the 128 ASCII characters.

Playfair Cipher (Modified):

Key Generation:

1. The playfair cipher in this algorithm consists of a 8*16 matrix as key 128 ASCII values for the 128 characters. The key is generated using the two 64 bit keys A, B.
2. The 64 bits of A are Xor ed with the respective bits in B to obtain the 64 bits. These 64 bits represent 8 ASCII values (any repetitions are omitted) which form the 1 to 8 characters of Row1 of the Playfair cipher key.
3. The remaining ASCII values are filled row wise to form the playfair cipher key.

Encryption:

From the input plain text initially the first pair of characters is taken, let their ASCII values be p1, p2. They are encrypted as follows:

1. If both p1, p2 are in the same row in the playfair key matrix then they are replaced with the value present to the left of them respectively.
2. If both p1, p2 are in the same column in the playfair key matrix then they are replaced with the value present below them respectively.
3. If both p1, p2 are equal then they are replaced with the value present to the left of them.
4. If p1, p2 are present in a different row and column then p1 is replaced by the value present in same row but in the column of p2 and p2 is replaced with a value from same row but present in the column of p1.

The procedure is repeated for all pairs of plain text characters (p2, p3), (p3, p4)….. (p_{n-1}, p_n) [8].

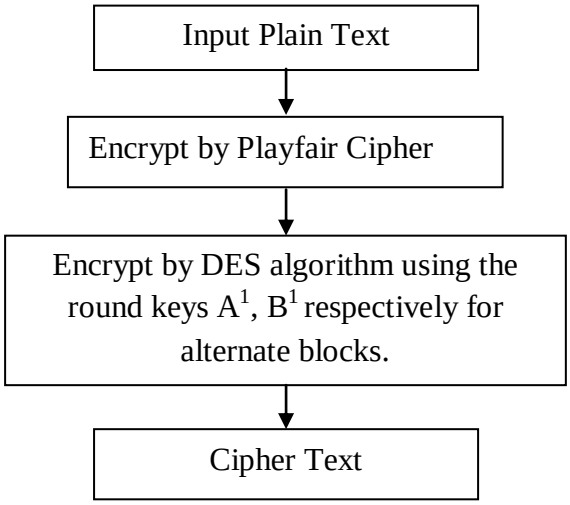

Figure 2: Modified DES algorithm

Evaluation Parameter – Avalanche Effect

Avalanche effect is the number of bits of change in cipher text due to one bit change in plain text [9]. Higher avalanche effect indicates that the confusion and diffusion properties in the algorithm are higher thus implying an increased security in the algorithm. Diffusion property is to ensure that each bit of plain text impacts many bits of the cipher text thus dissipating its statistical structure. It is equivalent to each cipher text getting affected by many bits of plain text. Similarly the Confusion property is to ensure that the statistical relationship between the cipher text and the key is very complex. Higher avalanche effect is a desirable property [10] as it implies higher diffusion property. In this paper the avalanche effect exhibited in DES algorithm and the modified DES algorithm is evaluated.

Results and Analysis

The following results are being observed for the given plain text and keys in case of DES and the modified DES.

Input: Computer Science

Key 1: 12345678

Key 2: ABCDEFGH

For the given plain text encryption is done in DES using the Key 1 and then avalanche effect is observed with respect to change of each bit in plain text for bits 1 to 64.

Similarly the encryption is done as per modified DES using Key 1 and Key 2 (generates two sets of round keys, each set used to encrypt alternate blocks) and avalanche effect is studied for a single bit variation in the plain text for each of the 1-64 bits.

The results of the avalanche effect observed in case of DES and modified DES algorithms for the bit complement or change from bit 1 to bit 64 of plain text are tabulated in the Table 1.

Table 1: Avalanche effect in DES, Modified DES algorithm due to change in Bit 1 to 64.

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

From the results shown in table 1 we can consider 3 cases where the maximum avalanche effect is observed with respect to the proposed modified DES algorithm.

Case 1: When bit 62 is complemented in plain text, in DES algorithm a change of 31 bits is observed whereas in modified DES it is 42 bits, resulting in a 34% increase of Avalanche effect.

Case 2: When bit 56 is complemented in plain text, in DES algorithm a change of 30 bits is observed whereas in modified DES it is 38 bits, resulting in a 26% increase of Avalanche effect.

Case 3: When bit 33 is complemented in plain text, in DES algorithm a change of 20 bits is observed whereas in modified DES it is 41 bits, resulting in a 105% increase of Avalanche effect. But this is an abnormal case as in DES the avalanche of 20 bits is very low and far less than the strict avalanche criteria.

Conclusion

The avalanche effect is analyzed in DES and in the proposed modified DES algorithm. We can observe an increase in avalanche effect in 60% of the cases in modified DES algorithm when compared to the DES algorithm. An increase of 34% in the avalanche effect (26%, 105% in specific instances) which is a significant increase can be observed in the results stated above. Higher avalanche effect is an indicator for high diffusion and confusion properties thereby increasing the security and complexity of the algorithm. The statistical analysis and cryptanalysis become more difficult. Due to the 112 bit key used it is less susceptible to brute force attack than the DES, due to the modification in the key generation mechanism we are able to overcome the problem of meet in middle attack noticed in 2DES algorithm in case of known plain and cipher text.

Future Scope

In the key generation procedure of the modified DES algorithm several other transposition techniques such as route cipher, columnar transposition, double transposition, Myszkowski transposition, disrupted transposition etc… maybe used. Some of them may provide added security to the key due their additional complexity. Avalanche effect can be analyzed in each of the cases.

References

[1] Data Encryption Standard announced by Federal Information Processing Standards Publication 46-3, October 25, 1999.

[2] Saeed, F., Rashid, M., 2010, “Integrating Classical Encryption with Modern Technique”, International Journal of Computer Science and Network Security (IJCSNS), Volume 10, No.5, pp.280-285.

[3] Awadh Kishor Singh., and Seema Varshney., 2014, “Enhanced Data Encryption Standard using Variable Size Key (128N Bits) and 96 Bit Subkey,” International Journal of Computer applications, ISSN 0975 – 8887, Volume 98-No.8, pp.11-14.

[4] Radhika Rani Chintala., Pujyasri Jetty., 2014, "Systematic study of Avalanche effect in Triple DES using various binary codes," International Journal of Applied Engineering Research, ISSN 0973 – 4562, Volume 9, Number 24, pp.30099 – 30108.

[5] Mandal, A.K., Tiwari, A., 2012, "Analysis of Avalanche Effect in Plain text of DES using Binary Codes", International Journal of Emerging Trends & Technology in Computer Science (ITETTCS), ISSN 2278-6856, Volume1, Issue 3, pp.166-171.

[6] Sriram Ramanujan, Marimuthu Karuppiah, 2011, "Designing an algorithm with high avalanche Effect", International Journal of Computer Science and Network Security (IJCSNS),Volume 11, No.01, pp.106-111.

[7] Subhajit Bhattacharyya., Nisarga Chand., and Subham Chakraborty., 2014, "A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323 , Volume 3, Issue 2, pp.308 – 312.

[8] Sastry, V.U.K., Ravi Shankar, N., Durga Bhavani,S., 2010, "A Generalized Playfair Cipher involving Intertwining, Interweaving and Iteration," International Journal of Network and Mobile Technologies, ISSN 1832 – 6758, Volume 1, Issue 2, pp.45-53.

[9] Agarwal, H., Sharma, M., 2010, "Implementation and analysis of various cryptosystems", India Journal of Science and Technology, ISSN: 0974 - 66846, Volume 3, No. 12, pp.1173-1176.

[10] Stallings, W., 2011, "Cryptography and Network Security – Principles and Practices", Edition -5, Prentice Hall Publications.