DES96 - Improved DES Security

Dr.Mohammed M. Alani

Department of Computer Engineering and Information Systems,
College of Computer Engineering and Sciences,
Gulf University, Kingdom of Bahrain
m.alani@d-crypt.org

Abstract **– The Data Encryption Standard (DES) has shown noticeable signs of aging during the last two decades. In this paper we develop a system that is a DES-variant with more resistance towards the possible attacks against DES. The developed system has a sub-key generation algorithm that is completely different from the original DES. The developed system uses 84-bit initial key instead of the 56-bit key originally used. It has substitution boxes inside the key generation algorithm and mod2 additions. The choice of arrangement of substitution boxes in the main algorithm for each round is sub-key dependent.**

The result of the design is a DES-variant cryptographic system that has higher resistance against brute-force attack, differential cryptanalysis, and linear cryptanalysis. The proposed system design also cancelled the weak-keys and complement keys properties of the DES.

Keywords- **des, encryption, des-variant, encryption, cryptanalysis**

I. INTRODUCTION

The DES was designed by IBM team in 1974. It was adopted as a standard in 1976. Ever since, DES was a target of different attacks [1-5]. Many attacks broke the DES when having less than 16 rounds. The differential cryptanalysis presented by Biham and Shamir in 1991 and linear cryptanalysis presented by Matsui in 1993 are the most important attacks to DES [1-5].

As the attacks evolve, the needs for new stronger systems increase. Many systems were designed in the last two decades such as RC2, LOKI, BlowFish, SAFER and many others [5]. International Data Encryption Algorithm (IDEA) was presented in 1990. It has better performance characteristics than the others [2].

Recently, a new standard was adopted; Advanced Encryption Standard (AES). The AES presented very strong security and options of implementation as compared to DES [6].

The aim of this work is to design a secure DES-Variant cryptographic system with the minimum possible key. It is also required to provide a system that overcomes the weaknesses of the original DES.

The reason we are trying to improve DES is to introduce an algorithm that provides acceptable security, as compared to the AES, and at the same time, does not require the intensive processing, time, and memory requirements as the AES does.

II. DESIGN CONCEPTS

The present design is concentrated to overcome the weaknesses of DES with the least possible key-length, time requirements, and memory requirements. It is important to provide more non-linearity inside the encryption algorithm to reduce the usefulness of linear and differential cryptanalysis.

The weak-keys, semiweak-keys, and possibly-weak keys are to be cancelled because of their effect on the generating the sub-keys. In addition, the complement-keys property is to be cancelled too by the designed algorithm.

The key-length was one of the major problems in DES. With the increasing computing abilities now days, the brute-force attack to a 56-bit key is applicable. The most important attacks to fight are differential and linear cryptanalysis. These two attacks depend heavily on the design of the S-Boxes of the DES.

III. THE PROPOSED ALGORITHM

The proposed key generation algorithm has 96-bit key length from which only 84 bits are used after removing the parity bits. A 7-bit left shift takes place in each round. The system also has a part to indicate the arrangement of the S-Boxes of each round, a stage of S-Boxes inside the key generation algorithm itself, and more linear permutations and Permuted Choice to provide more diffusion.

The proposed key generation algorithm can be seen in figure 1 and is described in the following steps:

Step 1:

The 96-bit key enters an initial permutation that discards the 12 parity bits to give an 84-bit key. The initial permutations are shown in figure 2.

Step 2:

The 84 bits are now divided into three parts:

a. 48 bits enters the S-Boxes to produce a 32-bit output.
b. 28 bits enter a permuted choice to produce a 16 bit output. This permuted choice is shown in figure 3.
c. 8 bits are processed as the following: each two adjacent bits are XORed together to produce 4 bits.

Step 3:

The leftmost 16 bits of the 32-bit output of Step (2,a) are swapped with the 16-bit output of Step (2,b) and all these outputs are combined to produce a 48-bit block to be sent to the main algorithm as K1 (the first sub key).

978-1-4244-7534-6/10/$26.00 ©2010 IEEE

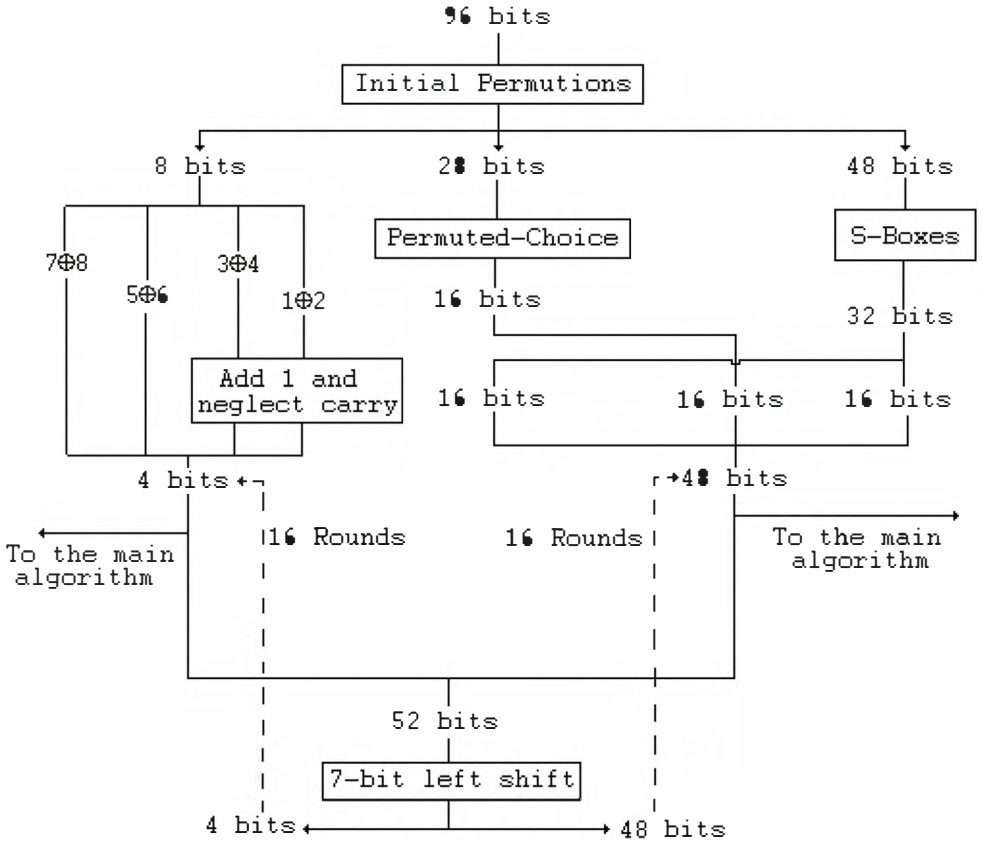

Fig. 1 The proposed key generation algorithm

87	57	43	47	92	25	62	2	61	66	45	4
34	94	70	30	77	22	81	5	76	20	42	55
95	75	38	41	50	85	52	79	23	67	51	21
73	19	53	89	17	9	84	44	13	74	69	27
29	90	1	31	35	14	65	33	11	28	93	6
3	83	58	12	78	7	91	37	18	15	63	26
86	54	49	71	36	59	86	60	68	39	10	46

Fig. 2 Initial Permutations

9	22	5	12	27	1	13	16
14	19	21	3	8	7	11	28

Fig. 3 Permuted choice

Step 4:

The 4-bit output from Step (2,c)is used twice after adding 1 to the two least significant bits and discarding the carry. First, the 4 bits are sent to the main algorithm to control the arrangement of the S-Boxes. The first bit determines whether to swap boxes 2 and 3, the second bit is used to control the swapping of boxes 1 and 7, the third controls boxes 4 and 6, and the fourth controls boxes 5 and 8. The 4 bits are then recombined with the 48 bits to prepare the sub-key of the next round.

Step 5:

For the next round, a shift of 7 bits to the left takes place and the rightmost 48 bits are sent to the main algorithm and the leftmost 4 bits are dealt with as the output of Step (2,c), and so on for 16 rounds.

The only change to the main algorithm was the 4 bits sent with each sub-key to determine the arrangement of the S-Boxes for each round.

IV. Properties of the Proposed System

The proposed DES96 system has the following advantages over DES:

a. The 84-bit key instead of the original 56-bit key is aimed to resist brute-force attack. This would give $2^{84}\approx1.934*10^{25}$ trials instead of $2^{56}\approx7.205*10^{16}$.

b. The S-Boxes inside the key generation algorithm are aimed to reduce linearity. This is to resist linear cryptanalysis providing a non-linear operation. The non-linear operation was chosen to be the same S-Boxes of the main algorithm in order to reduce memory requirements (for software implementation) and the components needed (in hardware implementation). And it is done only once to reduce the time required for sub-key generation which is convenient for key generation [3].

c. The permutations inside the sub-key generation algorithm are to provide more diffusion [2, 5].

d. Controlling the arrangement of the S-Boxes of the main algorithm of each round by the sub-keys is aimed to resist both linear and differential cryptanalysis. Because these two attacks depend heavily on the structure of the S-Boxes [2-4].
e. The addition of 1 and neglecting the carry provide two benefits; first the cancellation of weak, semi-weak, and possibly-weak keys, and second is the cancellation of the complement-keys property.
f. The 7-bit left shift provides, at least, 15 different sub-keys for each initial key. Any number less than 7 will provide more similar sub-keys. It is clear that the number of shifts must not be a factor of 52, because it will produce similar patterns.

V. Test Results

Three tests have been done. These are used here to check randomness, and the avalanche effect [1].

a. Randomness test:
This simplified test is performed by calculating the numbers of zeros and ones in the ciphertext resulting from the DES96 encryption and the results are compared to those of the plaintext. The test were applied to text files, audio files, video files, document files, and executable program files as these are the most common files to be encrypted. The results are shown in table I.

b. Avalanche test for changing plaintext bits:
One, two and three bits were changed in the plaintext and the change in the corresponding output ciphertext is measured in terms of hamming distance measure [1]. Table II shows the results of this test.

c. Avalanche test for changing key bits:
In this test, one, two, and three bits were changed in the initial key bits and the change in the output ciphertext is measured using hamming distance measure. Table III shows the results of this test.

The results of the above tests show that the proposed DES96 system provides good randomness properties. The proposed system also shows better avalanche characteristics and randomness properties when compared to the original DES system.

TABLE I

THE RESULTS OF RANDOMNESS TEST

File Type	File size (bits)	Zeros in plaintext (%)	Ones in plaintext (%)	Zeros in cipher-text (%)	Ones in cipher-text (%)
Text	1332136	56.22	43.78	49.99	50.01
Audio	1000224	52.12	47.88	50	50
Video	988920	53.69	46.31	49.99	50.01
Doc.	1101880	43.58	56.42	49.97	50.03
Program	1090328	45.81	54.19	49.99	50.01

TABLE II

THE RESULTS OF CHANGING PLAINTEXT BITS (AVALANCHE TEST)

Input Number	Hamming distance for changing 1 bit	Hamming distance for changing 2 bits	Hamming distance for changing 3 bits
1	30	43	52
2	35	41	45
3	33	40	41
4	36	39	46
5	34	39	44
6	37	43	44
7	32	44	44
8	33	40	44
9	33	43	47
10	36	42	46
11	37	42	46
12	32	41	49
13	34	43	51
14	30	44	47
15	31	43	53
16	32	39	48
17	31	42	49
18	35	41	49
19	33	41	50
20	33	41	47
21	35	48	46
22	34	44	47
23	34	49	50
24	32	48	53
25	34	41	48

TABLE III

THE RESULTS OF CHANGING KEY BITS (AVALANCHE TEST)

Input Number	Hamming distance for changing 1 bit	Hamming distance for changing 2 bits	Hamming distance for changing 3 bits
1	31	40	50
2	33	41	43
3	32	40	41
4	32	37	45
5	34	38	42
6	36	40	44
7	31	42	41
8	31	39	42
9	33	40	47
10	34	41	44
11	36	40	43
12	30	40	49
13	32	41	51
14	30	40	47
15	31	41	50
16	27	37	45
17	31	40	46
18	33	41	49
19	31	38	48
20	33	41	45
21	34	43	44
22	35	41	47
23	29	45	50
24	32	42	50
25	34	40	47

VI. Conclusion

As implementations of the original DES show many weaknesses, a DES-variant cryptographic system is designed to overcome most of the weaknesses. The designed system, DES96, is introduced here to resist brute-force attack, differential cryptanalysis, and linear cryptanalysis. These attacks are considered in the design because they are the most effective attacks against the original DES.

DES96 has a 96-bit initial key, sub-key dependent S-Boxes for each round, S-Boxes inside the key generation algorithm, and other features that strengthen it against known attacks. It also cancels the weak-keys and complement-keys properties of the original DES.

The system was tested for randomness and avalanche effects. The results have shown that DES96 is a reliable cryptographic system. The proposed system when compared to DES has better avalanche characteristics.

References

[1] Lamia A. Mohammed, "Designing and Testing Cryptosystem", M.Sc. Thesis, Department of Computer Science, College of Science, Baghdad University, Baghdad, Iraq, 2000.

[2] B. Schneier, *Applied Cryptography*, John Wiley & Sons, New York, 1996.

[3] E. Biham, "On Matsui's Linear Cryptanalysis", in *Proceedings of EUROCRYPT'94*, page 341.

[4] E. Biham and A. Shamir, "Differential Cryptanalysis of the full 16-round DES", in *Proc. Of CRYPTO'92*, page 487.

[5] B. Beckett, *Introduction to Cryptography and PC Security*, McGraw-Hill Companies, London, U.K., 1997.

[6] *AES*, IETF RFC 3602.