International Journal of Pure and Applied Mathematics
Volume 118 No. 22 2018, 1937-1943
ISSN: 1314-3395 (on-line version)
url: http://acadpubl.eu/hub
Special Issue
ijpam.eu

MODIFICATION IN DESIGNING OF SUBSTITUTION TECHNIQUE USING 4X32 S-BOX IN DATA ENCRYPTION STANDARD

[1]Sumit Chaudhary, [2]N. K. Joshi, [3]Foram Suthar
[1]Research Scholar, Computer Science & Engineering
Uttaranchal University, Dehradun, India
[2]Professor/Vice Chancellor, Uttaranchal University, Dehradun, India
[3]Assistant Professor, Computer Science & Engineering
IIST, Rajpur, Kadi Ahmedabad, India
[1]iimtsumit@gmail.com, [2]nkjoshi2001@yahoo.com, [3]foram.suthar@iist.edu.in

Abstract: This Paper presents 4X32 S-Box techniques for Data Encryption Standard (DES). The proposed design helps in providing more security. Previous work has only 6X4 S-Box or 8X32 S-Box, which do not provide large number of options. The proposed design employs combinational logic based on DES S-Box using additive modulo and X-OR.A 48-bit text converted into 4-bit 12 S-Box where X-OR operation applied on both sides, later that output again combined with other left S-Box where additive modulo applied. The output of the algorithm give more secured output and gives more Avalanche effect.

Keywords: S-Box, Data Encryption Standard, Modified S-Box.

1. Introduction

Cryptography is the study of hiding the data which involves two processes: 1. Ciphering: which is the process of translating the readable form into the form 2. Deciphering: it is the process of translating unreadable form into readable form. Ciphering and Deciphering can be done by two types of secure key one is the symmetric key which has equal value for encryption and also for decryption and another is key which has different values for encryption and decryption. There are so many algorithms which used the asymmetric key like DES, 3DEA, IDEA, AES, RSA, Blowfish etc. There are main two key factors in each algorithm: Algorithm Type and Algorithm Mode.

All Cryptography algorithm [18] use different mathematical techniques to secure data like permutation, substitution. S-box is mainly a substitution technique and used in internal part of the function in DES, AES algorithm. S-box is the table of a collection of value in a specific manner. There are many way to generate entry of S-Box, it might possible to construct weak S-Box become cryptosystem weaker. A systematically planned and best technique to create those values in the S-box [14] is by creating using a nonlinear Boolean function, by mapping n input bits to m output bits. Maximum nonlinearity can be achieved by bent function which is special set of Boolean function. In this paper, we have proposed to modify S-box of DES [17] algorithm.

DES is standard data encryption algorithm for secure communication. DES used Feistel cipher techniques for encryption and decryption. DES is 16 round substitution and permutation network with 64-bits plaintext and 56 bits key (Initially it supports 64-bit keys size. Every 8 bits are used for checker parity so after discarding 8 bits it will become 56-bit key size).

S-box is next process after permutation, which accepts 48-bits as input from permutation and makes 32-bit output.

Total 8 S-box are created in DES algorithm. In the DES system in its first S-box, there are 16 columns having entries in hexadecimal. If a truth table is constructed by us, we will be able to have 6 input columns of zeros as well as 4 output columns of zeros and ones with 2 6 rows. The S-box is mapped as, f: {0, 1} 6 → {0, 1} 4. Thus, S-box is composed of four highly nonlinear balanced Boolean functions. Now, the 6 input bits are divided into two different halves: the middle four bits represent the columns of the S-box, while the remaining two bits on both sides represent the rows of the S-box. We will see later on how four highly nonlinear Boolean functions will generate entries for S-box. [7] [8] mainly, let us start with the understanding of the design factor of S-boxes. Let see five design factors must be meet for Boolean functions to construct cryptographically good S-box:

1. Bijection: If the S-box [15] is of ‘n x n’ bit then from input vectors a one-to-one and onto mapping to output vectors will be there. This can be explained later that how we can achieve this criterion when the S-box will be n x m bits.
2. Strict avalanche criteria: Here, there will be the change in output bit with the probability of one-half

only if a strict avalanche criterion of one input bit has changed. In Strict avalanche criteria, output vector will be significantly changed with a small/slight amount of change in the input vector. So, a function is needed that has a 50% dependency on each of its n input bits in order to achieve this effect.

3. Bit independence criterion or correlation-immunity: Here, there is a requirement that output bits should have different statistical patterns or no statistical dependencies compare to the output vectors.

4. Nonlinearity: The cryptosystem is susceptible to various attacks so nonlinearity requires S-box which should not be a linear mapping from input to output [9]. If the nonlinearity gives a bad result by linear functions and makes a cryptosystem more complex to crack so S-box will be constructed by using maximally nonlinear Boolean functions.

5. Balance: if each Boolean vector has the S-box with an equal number of 0’s and 1’s then it is known as balance. This should meet most of the standards set by the NIST. Sometimes, it can be impossible to achieve all criteria to their full potential. Sometimes criteria can be compromised due to their conflicting nature. For example, maximum nonlinearity also conflicts with balance as well as correlation immunity conflicts with high nonlinearity.

2. Literature Review

“Govind Prasad Arya, Aayushi Nautiyal, Ashish Pant, Shiv Singh & Tishi Handa” proposed methodology to design Cipher with Automatic Key Generation concept [4]. In addition, there may be a need of a ton of information to be kept immune for local devices. The ciphering of information is an essential necessity now which increases confidentiality of data. We can encrypt the data using a number of algorithms during communication. With the help of substitution and transposition techniques when have proposed cipher in this paper. Due to the use of “Random Number Generator” function cryptanalysis become more complicated. Random Number Generator makes the algorithm more secure. Also, give the advantage of transferring the key to the receiver which had plain text at random.

Author “R.L. Rivest, A. Shamir, and L. Adleman” [6] proposed work for Digital Signatures and Public-Key Cryptosystems. Here, a novel property of an encryption method is presented where revealing of an encryption key publicly, does not there by revealing the corresponding decryption key.[4] Thus, it leads to two different important consequences:

1. Now to transmit keys we don’t need Couriers or other secure means because an encryption key is publicly revealed by the intended recipient and a message can be encrypted using an encryption key. Only receiver has knowledge of the corresponding decryption key, so only he can decipher the message.

2. The private decryption key is used to secure the data. Using the corresponding public encryption key anyone can verify this signature. Signatures couldn’t be produced, and a signer couldn’t deny later on. “Electronic mail" and electronic funds transfer" system is the best example of this application.

“Manikandan.G” [2] proposed that almost all present methodology offering reliability are vulnerable to attacks be it a network or web or to a data. Effective cryptanalysis breaches it at some point of time whatsoever may be its complex algorithmic design. We can say that in general almost all practices are restricted to follow single encryption scheme for a single iteration that also on a single file basis in today’s crypto world. Well, encryption-decryption cases show that this is evident in the 99% of the cases. Thus, it becomes vital to have a need for “practically strong and infeasible to get attacked” technique. So an involvement of Cryptographic [20] enciphering and deciphering is proposed in this paper. They propose a methodology which involves it along with Splitting of Files and Merging mechanisms. Encryption and Decryption of data are done by using modified Blowfish algorithm. The cryptographic scheme is differentiated in the single algorithm by different key for changing the file slices. The output shows that system provides enhanced performance and great security and thus the better solution.

The Authors “Shah Kruti R., Bhavika Gambhava” [3] proposed the principal goal guiding the design of any cryptosystem have to be security against the hacker. Recently the uses of computer increase for communication in private and public sector. An attacker can easily get data on the base of significant value because each data has significant value in communication So that data need to be secure. So many algorithms are available for security purpose but we need to increase performance and security level periodically. In this paper, author has introduced a new concept to enhance the performance of DES algorithm. Standard algorithm used 16 round. The author has replaced redefined XOR operation which has been applying during that round. This operation is depends on two keys, where each key is combination of 4 states (0, 1, 2, 3) rather than 2 states (0, 1). This change made the algorithm more secure and robust against the attacker.

“Ms. Priya S, Ms. Anita Madona M” [11] Proposed the model for network communication system security. The best symmetric key [19] cryptography algorithm is DES in which both the client and server use a shared secret key to cipher or decipher the dotards. DES is the block cipher [15] which performs many complicated operations to change a fixed-length data of readable text into another unreadable text data of the same length. To make cryptanalysis difficult and increase the reliability of DES and also reduce the chances of burst force attack, Affine Cipher is used before the original DES algorithm. NS-2 is the best simulation tool for analysis and comparison of the performance of DES.

3. Proposed Work

The proposed scheme has defined that firstly encrypt the 64-bit plaintext with the help of enhanced key generation algorithm in which S-Box [16] is designed in the form of (4X32). The original message is first transferred into the cipher text on the basis of substitution and Permutation technique. The Substitution i.e. S-Box is defined in the modified terms as input is given as 4-bit and output is produced as 32-bit in each round. To apply this scheme we required total 12 S-Box in which every S-Box took 4-bit input and 32-bit output will be produced. Finally using additive modulo and X-OR we will get the 32-bit output.

The Enhanced DES has the following advantages over simple DES:

a. DES round will be increased and decreased on the base of Simple Columnar Transposition Technique which applies before DES algorithm and this modification increased the security level of DES.
b. Enhanced DES algorithm is more secure and difficult to break by Brute Force attack because attacker required to breaks both simple columnar approach and DES algorithm. Due to this attacker need the extra tie to hack algorithm.
c. The attacker required a random number of columnar approaches to reach the plain text to hack the key of DES.

Disadvantages of Enhanced DES

1. The extra modification is needed for modified S-Box to provide more security and this is the main disadvantages.
2. To find enhanced key generation approach output in terms of the random number generator or with applying left shift transposition not so hard because the speed of machines is very high.

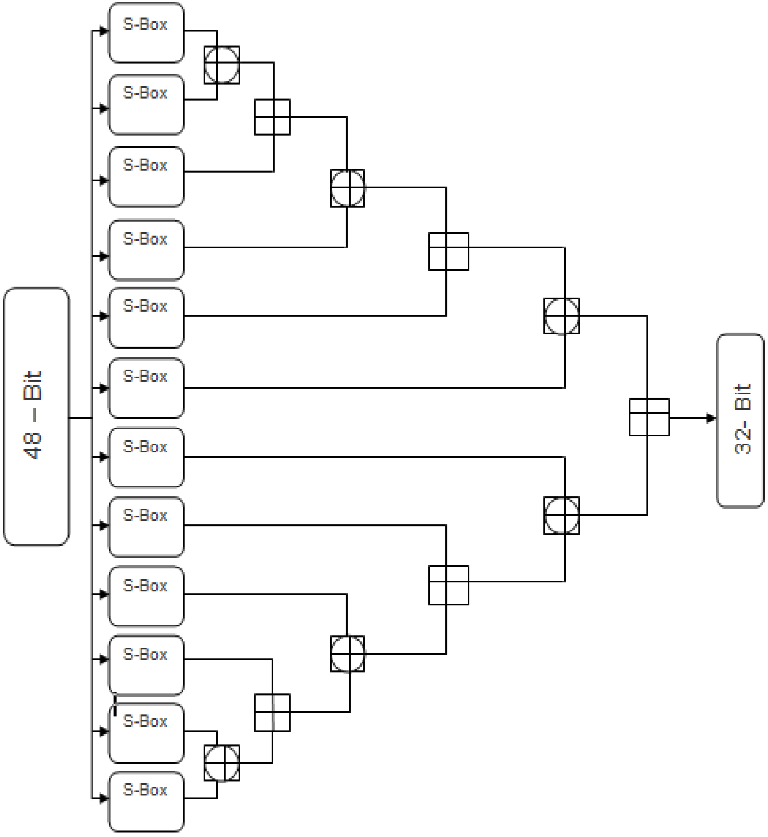
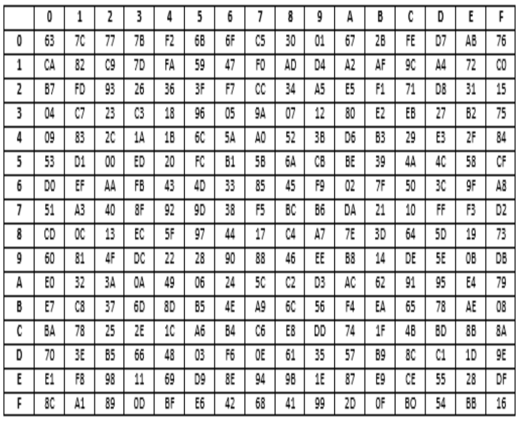


Figure 1. Proposed model of 4X32 S-BOX as modified S-BOX

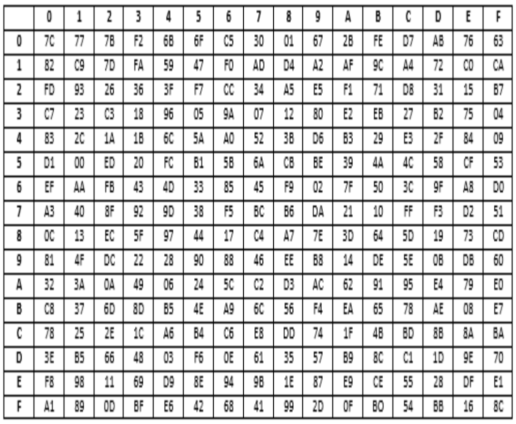
4. Result

S-Box table 1



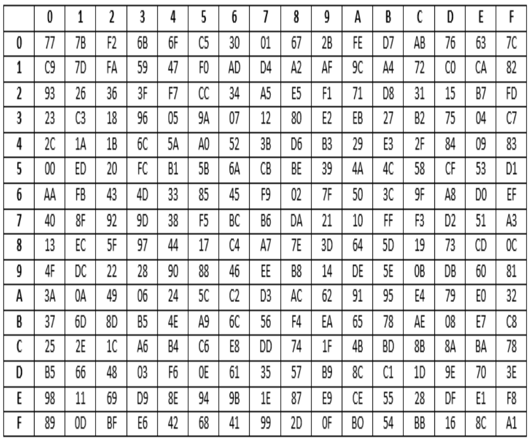
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6C	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	28	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	B5	4E	A9	6C	56	F4	EA	65	78	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	8C	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

S-Box table 2



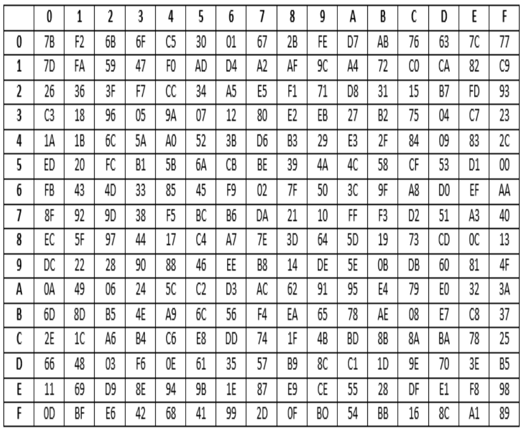
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76	63
1	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0	CA
2	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15	B7
3	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75	04
4	83	2C	1A	1B	6C	5A	A0	52	3B	D6	B3	29	E3	2F	84	09
5	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF	53
6	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8	D0
7	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2	51
8	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73	CD
9	81	4F	DC	22	28	90	88	46	EE	B8	14	DE	5E	0B	DB	60
A	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79	E0
B	C8	37	6D	8D	B5	4E	A9	6C	56	F4	EA	65	78	AE	08	E7
C	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A	BA
D	3E	B5	66	48	03	F6	0E	61	35	57	B9	8C	C1	1D	9E	70
E	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF	E1
F	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16	8C

S-Box table 3



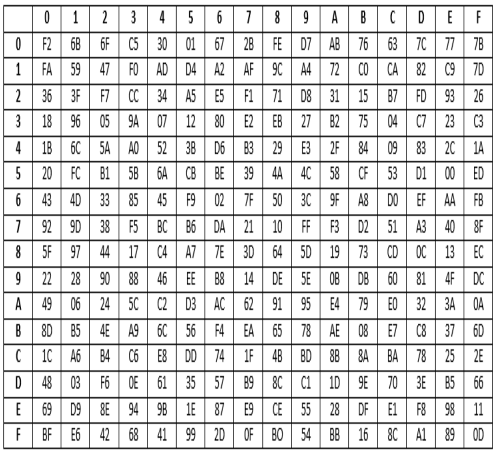
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76	63	7C
1	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0	CA	82
2	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15	B7	FD
3	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75	04	C7
4	2C	1A	1B	6C	5A	A0	52	3B	D6	B3	29	E3	2F	84	09	83
5	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF	53	D1
6	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8	D0	EF
7	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2	51	A3
8	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73	CD	0C
9	4F	DC	22	28	90	88	46	EE	B8	14	DE	5E	0B	DB	60	81
A	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79	E0	32
B	37	6D	8D	B5	4E	A9	6C	56	F4	EA	65	78	AE	08	E7	C8
C	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A	BA	78
D	B5	66	48	03	F6	0E	61	35	57	B9	8C	C1	1D	9E	70	3E
E	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF	E1	F8
F	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16	8C	A1

S-Box table 4



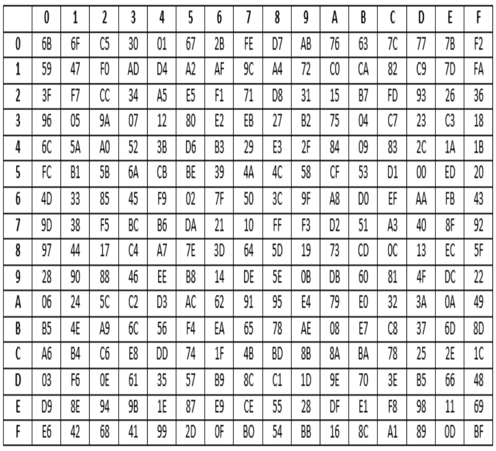
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76	63	7C	77
1	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0	CA	82	C9
2	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15	B7	FD	93
3	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75	04	C7	23
4	1A	1B	6C	5A	A0	52	3B	D6	B3	29	E3	2F	84	09	83	2C
5	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF	53	D1	00
6	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8	D0	EF	AA
7	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2	51	A3	40
8	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73	CD	0C	13
9	DC	22	28	90	88	46	EE	B8	14	DE	5E	0B	DB	60	81	4F
A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79	E0	32	3A
B	6D	8D	B5	4E	A9	6C	56	F4	EA	65	78	AE	08	E7	C8	37
C	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A	BA	78	25
D	66	48	03	F6	0E	61	35	57	B9	8C	C1	1D	9E	70	3E	B5
E	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF	E1	F8	98
F	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16	8C	A1	89

S-Box table 5



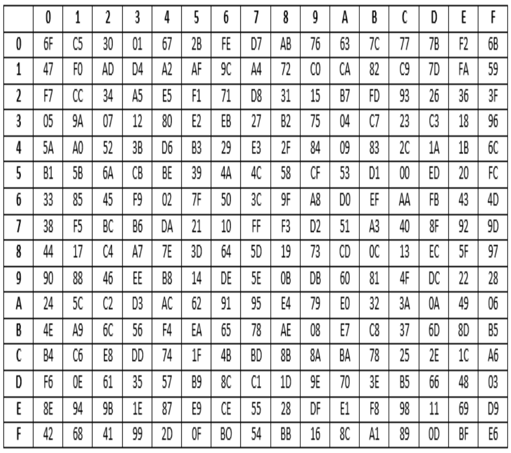
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76	63	7C	77	7B
1	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0	CA	82	C9	7D
2	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15	B7	FD	93	26
3	18	96	05	9A	07	12	80	E2	EB	27	B2	75	04	C7	23	C3
4	1B	6C	5A	A0	52	3B	D6	B3	29	E3	2F	84	09	83	2C	1A
5	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF	53	D1	00	ED
6	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8	D0	EF	AA	FB
7	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2	51	A3	40	8F
8	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73	CD	0C	13	EC
9	22	28	90	88	46	EE	B8	14	DE	5E	0B	DB	60	81	4F	DC
A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79	E0	32	3A	0A
B	8D	B5	4E	A9	6C	56	F4	EA	65	78	AE	08	E7	C8	37	6D
C	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A	BA	78	25	2E
D	48	03	F6	0E	61	35	57	B9	8C	C1	1D	9E	70	3E	B5	66
E	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF	E1	F8	98	11
F	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16	8C	A1	89	0D

S-Box table 6



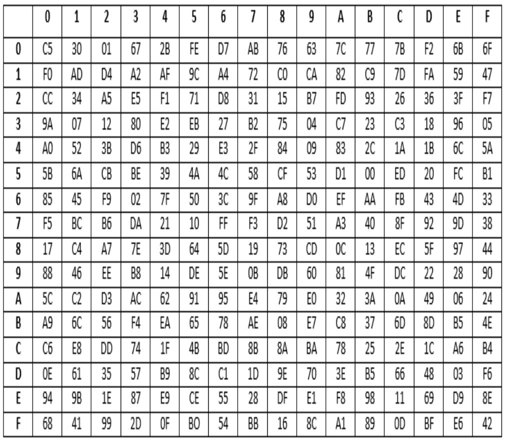
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	6B	6F	C5	30	01	67	2B	FE	D7	AB	76	63	7C	77	7B	F2
1	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0	CA	82	C9	7D	FA
2	3F	F7	CC	34	A5	E5	F1	71	D8	31	15	B7	FD	93	26	36
3	96	05	9A	07	12	80	E2	EB	27	B2	75	04	C7	23	C3	18
4	6C	5A	A0	52	3B	D6	B3	29	E3	2F	84	09	83	2C	1A	1B
5	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF	53	D1	00	ED	20
6	4D	33	85	45	F9	02	7F	50	3C	9F	A8	D0	EF	AA	FB	43
7	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2	51	A3	40	8F	92
8	97	44	17	C4	A7	7E	3D	64	5D	19	73	CD	0C	13	EC	5F
9	28	90	88	46	EE	B8	14	DE	5E	0B	DB	60	81	4F	DC	22
A	06	24	5C	C2	D3	AC	62	91	95	E4	79	E0	32	3A	0A	49
B	B5	4E	A9	6C	56	F4	EA	65	78	AE	08	E7	C8	37	6D	8D
C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A	BA	78	25	2E	1C
D	03	F6	0E	61	35	57	B9	8C	C1	1D	9E	70	3E	B5	66	48
E	D9	8E	94	9B	1E	87	E9	CE	55	28	DF	E1	F8	98	11	69
F	E6	42	68	41	99	2D	0F	B0	54	BB	16	8C	A1	89	0D	BF

S-Box table 7



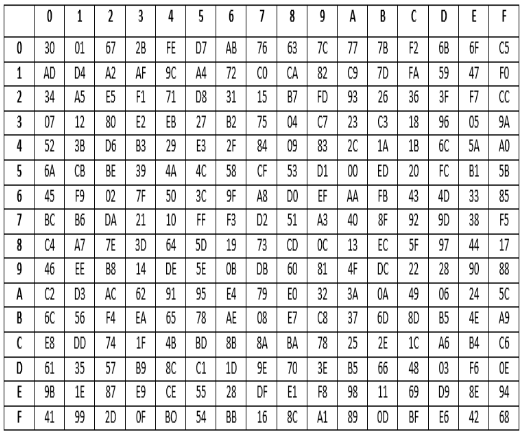
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	6F	C5	30	01	67	2B	FE	D7	AB	76	63	7C	77	7B	F2	6B
1	47	F0	AD	D4	A2	AF	9C	A4	72	C0	CA	82	C9	7D	FA	59
2	F7	CC	34	A5	E5	F1	71	D8	31	15	B7	FD	93	26	36	3F
3	05	9A	07	12	80	E2	EB	27	B2	75	04	C7	23	C3	18	96
4	5A	A0	52	3B	D6	B3	29	E3	2F	84	09	83	2C	1A	1B	6C
5	B1	5B	6A	CB	BE	39	4A	4C	58	CF	53	D1	00	ED	20	FC
6	33	85	45	F9	02	7F	50	3C	9F	A8	D0	EF	AA	FB	43	4D
7	38	F5	BC	B6	DA	21	10	FF	F3	D2	51	A3	40	8F	92	9D
8	44	17	C4	A7	7E	3D	64	5D	19	73	CD	0C	13	EC	5F	97
9	90	88	46	EE	B8	14	DE	5E	0B	DB	60	81	4F	DC	22	28
A	24	5C	C2	D3	AC	62	91	95	E4	79	E0	32	3A	0A	49	06
B	4E	A9	6C	56	F4	EA	65	78	AE	08	E7	C8	37	6D	8D	B5
C	B4	C6	E8	DD	74	1F	4B	BD	8B	8A	BA	78	25	2E	1C	A6
D	F6	0E	61	35	57	B9	8C	C1	1D	9E	70	3E	B5	66	48	03
E	8E	94	9B	1E	87	E9	CE	55	28	DF	E1	F8	98	11	69	D9
F	42	68	41	99	2D	0F	BO	54	BB	16	8C	A1	89	0D	BF	E6

S-Box table 8



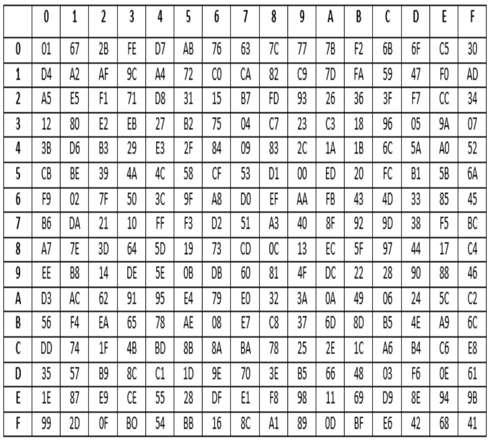
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C5	30	01	67	2B	FE	D7	AB	76	63	7C	77	7B	F2	6B	6F
1	F0	AD	D4	A2	AF	9C	A4	72	C0	CA	82	C9	7D	FA	59	47
2	CC	34	A5	E5	F1	71	D8	31	15	B7	FD	93	26	36	3F	F7
3	9A	07	12	80	E2	EB	27	B2	75	04	C7	23	C3	18	96	05
4	A0	52	3B	D6	B3	29	E3	2F	84	09	83	2C	1A	1B	6C	5A
5	5B	6A	CB	BE	39	4A	4C	58	CF	53	D1	00	ED	20	FC	B1
6	85	45	F9	02	7F	50	3C	9F	A8	D0	EF	AA	FB	43	4D	33
7	F5	BC	B6	DA	21	10	FF	F3	D2	51	A3	40	8F	92	9D	38
8	17	C4	A7	7E	3D	64	5D	19	73	CD	0C	13	EC	5F	97	44
9	88	46	EE	B8	14	DE	5E	0B	DB	60	81	4F	DC	22	28	90
A	5C	C2	D3	AC	62	91	95	E4	79	E0	32	3A	0A	49	06	24
B	A9	6C	56	F4	EA	65	78	AE	08	E7	C8	37	6D	8D	B5	4E
C	C6	E8	DD	74	1F	4B	BD	8B	8A	BA	78	25	2E	1C	A6	B4
D	0E	61	35	57	B9	8C	C1	1D	9E	70	3E	B5	66	48	03	F6
E	94	9B	1E	87	E9	CE	55	28	DF	E1	F8	98	11	69	D9	8E
F	68	41	99	2D	0F	BO	54	BB	16	8C	A1	89	0D	BF	E6	42

S-Box table 9



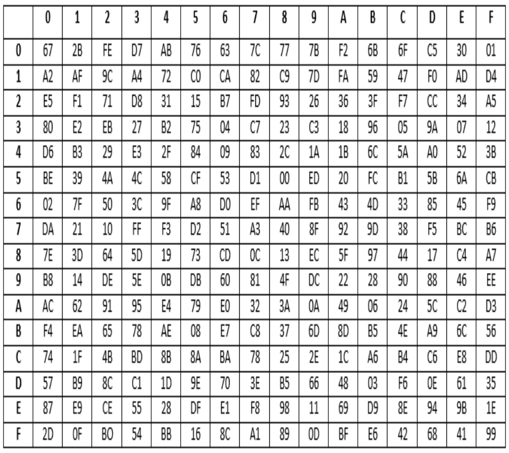
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	30	01	67	2B	FE	D7	AB	76	63	7C	77	7B	F2	6B	6F	C5
1	AD	D4	A2	AF	9C	A4	72	C0	CA	82	C9	7D	FA	59	47	F0
2	34	A5	E5	F1	71	D8	31	15	B7	FD	93	26	36	3F	F7	CC
3	07	12	80	E2	EB	27	B2	75	04	C7	23	C3	18	96	05	9A
4	52	3B	D6	B3	29	E3	2F	84	09	83	2C	1A	1B	6C	5A	A0
5	6A	CB	BE	39	4A	4C	58	CF	53	D1	00	ED	20	FC	B1	5B
6	45	F9	02	7F	50	3C	9F	A8	D0	EF	AA	FB	43	4D	33	85
7	BC	B6	DA	21	10	FF	F3	D2	51	A3	40	8F	92	9D	38	F5
8	C4	A7	7E	3D	64	5D	19	73	CD	0C	13	EC	5F	97	44	17
9	46	EE	B8	14	DE	5E	0B	DB	60	81	4F	DC	22	28	90	88
A	C2	D3	AC	62	91	95	E4	79	E0	32	3A	0A	49	06	24	5C
B	6C	56	F4	EA	65	78	AE	08	E7	C8	37	6D	8D	B5	4E	A9
C	E8	DD	74	1F	4B	BD	8B	8A	BA	78	25	2E	1C	A6	B4	C6
D	61	35	57	B9	8C	C1	1D	9E	70	3E	B5	66	48	03	F6	0E
E	9B	1E	87	E9	CE	55	28	DF	E1	F8	98	11	69	D9	8E	94
F	41	99	2D	0F	BO	54	BB	16	8C	A1	89	0D	BF	E6	42	68

S-Box table 10



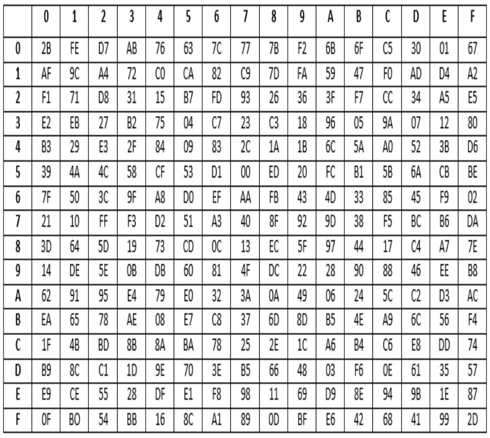
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	01	67	2B	FE	D7	AB	76	63	7C	77	7B	F2	6B	6F	C5	30
1	D4	A2	AF	9C	A4	72	C0	CA	82	C9	7D	FA	59	47	F0	AD
2	A5	E5	F1	71	D8	31	15	B7	FD	93	26	36	3F	F7	CC	34
3	12	80	E2	EB	27	B2	75	04	C7	23	C3	18	96	05	9A	07
4	3B	D6	B3	29	E3	2F	84	09	83	2C	1A	1B	6C	5A	A0	52
5	CB	BE	39	4A	4C	58	CF	53	D1	00	ED	20	FC	B1	5B	6A
6	F9	02	7F	50	3C	9F	A8	D0	EF	AA	FB	43	4D	33	85	45
7	B6	DA	21	10	FF	F3	D2	51	A3	40	8F	92	9D	38	F5	BC
8	A7	7E	3D	64	5D	19	73	CD	0C	13	EC	5F	97	44	17	C4
9	EE	B8	14	DE	5E	0B	DB	60	81	4F	DC	22	28	90	88	46
A	D3	AC	62	91	95	E4	79	E0	32	3A	0A	49	06	24	5C	C2
B	56	F4	EA	65	78	AE	08	E7	C8	37	6D	8D	B5	4E	A9	6C
C	DD	74	1F	4B	BD	8B	8A	BA	78	25	2E	1C	A6	B4	C6	E8
D	35	57	B9	8C	C1	1D	9E	70	3E	B5	66	48	03	F6	0E	61
E	1E	87	E9	CE	55	28	DF	E1	F8	98	11	69	D9	8E	94	9B
F	99	2D	0F	BO	54	BB	16	8C	A1	89	0D	BF	E6	42	68	41

S-Box table 11



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	67	2B	FE	D7	AB	76	63	7C	77	7B	F2	6B	6F	C5	30	01
1	A2	AF	9C	A4	72	C0	CA	82	C9	7D	FA	59	47	F0	AD	D4
2	E5	F1	71	D8	31	15	B7	FD	93	26	36	3F	F7	CC	34	A5
3	80	E2	EB	27	B2	75	04	C7	23	C3	18	96	05	9A	07	12
4	D6	B3	29	E3	2F	84	09	83	2C	1A	1B	6C	5A	A0	52	3B
5	BE	39	4A	4C	58	CF	53	D1	00	ED	20	FC	B1	5B	6A	CB
6	02	7F	50	3C	9F	A8	D0	EF	AA	FB	43	4D	33	85	45	F9
7	DA	21	10	FF	F3	D2	51	A3	40	8F	92	9D	38	F5	BC	B6
8	7E	3D	64	5D	19	73	CD	0C	13	EC	5F	97	44	17	C4	A7
9	B8	14	DE	5E	0B	DB	60	81	4F	DC	22	28	90	88	46	EE
A	AC	62	91	95	E4	79	E0	32	3A	0A	49	06	24	5C	C2	D3
B	F4	EA	65	78	AE	08	E7	C8	37	6D	8D	B5	4E	A9	6C	56
C	74	1F	4B	BD	8B	8A	BA	78	25	2E	1C	A6	B4	C6	E8	DD
D	57	B9	8C	C1	1D	9E	70	3E	B5	66	48	03	F6	0E	61	35
E	87	E9	CE	55	28	DF	E1	F8	98	11	69	D9	8E	94	9B	1E
F	2D	0F	BO	54	BB	16	8C	A1	89	0D	BF	E6	42	68	41	99

S-Box table 12



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2B	FE	D7	AB	76	63	7C	77	7B	F2	6B	6F	C5	30	01	67
1	AF	9C	A4	72	C0	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2
2	F1	71	D8	31	15	B7	FD	93	26	36	3F	F7	CC	34	A5	E5
3	E2	EB	27	B2	75	04	C7	23	C3	18	96	05	9A	07	12	80
4	B3	29	E3	2F	84	09	83	2C	1A	1B	6C	5A	A0	52	3B	D6
5	39	4A	4C	58	CF	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE
6	7F	50	3C	9F	A8	D0	EF	AA	FB	43	4D	33	85	45	F9	02
7	21	10	FF	F3	D2	51	A3	40	8F	92	9D	38	F5	BC	B6	DA
8	3D	64	5D	19	73	CD	0C	13	EC	5F	97	44	17	C4	A7	7E
9	14	DE	5E	0B	DB	60	81	4F	DC	22	28	90	88	46	EE	B8
A	62	91	95	E4	79	E0	32	3A	0A	49	06	24	5C	C2	D3	AC
B	EA	65	78	AE	08	E7	C8	37	6D	8D	B5	4E	A9	6C	56	F4
C	1F	4B	BD	8B	8A	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74
D	B9	8C	C1	1D	9E	70	3E	B5	66	48	03	F6	0E	61	35	57
E	E9	CE	55	28	DF	E1	F8	98	11	69	D9	8E	94	9B	1E	87
F	0F	BO	54	BB	16	8C	A1	89	0D	BF	E6	42	68	41	99	2D

S-Box Table 1 to Table 12 shows the output of the 12 S-Box that can be applied in various algorithms like DES, AES, and Blowfish etc for getting the nonlinear function and for getting more Avalanche Effect.

5. Conclusion

DES helps in encrypting data with lots of permutation and combination, providing better result and security. In DES 4X32 S-Box technique employed on combinational logic using techniques like X-OR operation, additive modulo raised the standards of S-Box for Data Encryption Standard (DES).

References

.

[1] Alani, M.M.," A DES96 - improved DES security",7th International Multi-Conference on Systems, Signals and Devices, Amman , 27-30 June 2010.

[2] Manikandan. G, Rajendiran.P, Chakarapani.K, Krishnan.G, Sundarganesh.G,"A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Advanced Information Technology, Jan 2012.

[3] Shah Kruti R., Bhavika Gambhava,"New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[4] Govind Prasad Arya, Aayushi Nautiyal, Ashish Pant, Shiv Singh, Tishi Handa,"A Cipher Design with Automatic Key Generation using the Combination of Substitution and Transposition Techniques and Basic Arithmetic and Logic Operations", The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 1, No. 1, March-April 2013.

[5] Duncan S. Wong, Hector Ho Fuentes and Agnes H. Chan,"The Performance Measurement of Cryptographic Primitives on Palm Devices", College of Computer Science, Northeastern University, Boston, MA 02115, USA.

[6] Adi Shamir Ronald Rivest and Len Adleman, "A method for obtaining digital signatures and public-key cryptosystem", Communications of the ACM, 21:120–126, 1978.

[7] Allam Mousa, "Data Encryption Performance Based on Blowfish", 47th International Symposium ELMAR-2005.08-1 0, June 2005.

[8] Israa Tahseen and Shatha Habeeb, "Proposal New Approach for Blowfish Algorithm by Using Random Key Generator", Journal of Madent Alelem College, Vol. 4, No. 1, pp. 1-10, 2012.

[9] SIMMONS, G.J.: 'Symmetric and asymmetric encryption', ACM Comput. Surveys, 1979, 11, pp. 305-330

[10] "Ms. Ramya G., Ms. Anita Madona M." "Enhancing DES and AES with 1024 Bits Key", International Research Journal of Engineering and Technology (IRJET), vol 2,issue 4, July2015, pp. 1008-1014.

[11] "Ms. Priya S, Ms. Anita Madona M" ,"Hybrid Data Encryption Standard", International Research Journal of Engineering and Technology (IRJET), vol 2,issue 4, July2015, pp.1024-1028.

[12] Guesmi, Ramzi, Mohamed Amine Ben Farah, Abdennaceur Kachouri, and Mounir Samet. "A novel design of Chaos based S-Boxes using genetic algorithm techniques", 2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA), 2014.

[13] Khan, Fadia Ali, et al. "A novel substitution box forencryption based on Lorenz equations." Circuits, System and Simulation (ICCSS), 2017 International Conference on. IEEE, 2017.

[14] Özkaynak, Fatih, Vedat Çelik, and Ahmet Bedri Özer. "A new S-box construction method based on the fractional-order chaotic Chen system." Signal, Image and Video Processing 11.4 (2017): 659-664.

[15] Bhowmik, Dipanjan, Avijit Datta, and Sharad Sinha. "A Novel Scheme for Analyzing Confusion Characteristics of Block Ciphers." Proceedings of the First International Conference on Intelligent Computing and Communication. Springer Singapore, 2017.

[16] Qureshi, A., and T. Shah. "S-box on subgroup of Galois field based on linear fractional transformation." Electronics Letters 53.9 (2017): 604-606.

[17] Cruz, Bryan F., et al. "Expanded 128-bit Data Encryption Standard." (2017).

[18] Paul, Varghese, and Amitabh Wahi. "Dynamic colour table: A novel S□box for cryptographic applications." International Journal of Communication Systems (2017).

[19] Biryukov, Alex, et al. "Topics and Research Directions for Symmetric Cryptography." Proceedings of Early Symmetric Crypto workshop, 2017. University of Luxembourg, 2017.

[20] Altaleb, Anas, et al. "An algorithm for the construction of substitution box for block ciphers based on projective general linear group." AIP Advances 7.3 (2017): 035116.

[21] S.V.Manikanthan and T.Padmapriya "Recent Trends In M2m Communications In 4g Networks And Evolution Towards 5g", International Journal of Pure and Applied Mathematics, ISSN NO:1314-3395, Vol-115, Issue -8, Sep 2017.

[22] S.V. Manikanthan,T.Padmapriya "An enhanced distributed evolved node-b architecture in 5G tele-communications network" International Journal of Engineering & Technology (UAE), Vol 7 Issues No (2.8) (2018) 248-254.March2018.