International Journal of Pure and Applied Mathematics
Volume 118 No. 10 2018, 363-376
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v118i10.77
Special Issue

ijpam.eu

Mathematical Formulation of DES Algorithm.

V.P.BEENU[1]
[1]Department of Statistics,
Justice Basheer Ahmed Sayeed College For Women
Teynampet, Chennai-18
beenu.vinod1982@gmail.com

December 22, 2017

Abstract

Modern Technology like wireless network helps us to connect instantly with people anywhere and at any time. Security of Wireless network is the main challenge faced by todays world. It is where cryptography play a vital role to provide security to the wireless network. Numerous encryption calculations are accessible to secure the information. This paper deals with ordinarily utilized symmetric encryption calculation which is DES Algorithm. Test results are given to illustrate the execution of this calculation.

AMS Subject Classification: ...

Key Words and Phrases: DES, Feistel function, Permutation, Key schedule

1 INTRODUCTION

Cryptography is an art of conveying messages in coded form which is understood only by the intended recipient. The recipient in turn decodes to read the message. The transfer of data through public network with security issues can be protected with cryptography. There are several standard symmetric and asymmetric algorithms which are highly secured and time tested.

2 TYPES OF CRYPTOGRAPHY

Cryptography is mainly divided into two types.

1. Symmetric algorithm
2. Asymmetric algorithm

Symmetric Algorithm.
In this type a single key which is kept secret among the sender and the recipient is used so that no unauthorized person can use the data, which is to be transferred.
Asymmetric Algorithm.
In this type a public key and private key are used where public is known to everyone whereas the private key is only known to the recipient of the message. This encryption is considered more secure when compared with symmetric algorithm. When speed is compared symmetric algorithm works faster.

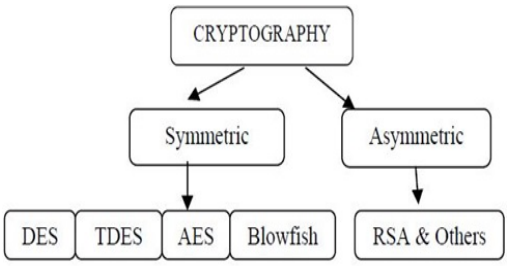

Figure 1:

3 PROPOSED WORK

3.1 DATA ENCRYPTION STANDARD

The DES has the following steps involved.

a) 64 bit plain text is taken as input and initial permutation is done on the input by re-arranging the bits to get the permuted input.

b) The next step involves 16 rounds of the same function along with permutation and substitution.

c) The 16^th output contains 64 bits as a result of function of input plain text and key.

d) The output of left and right side are swapped producing the preoutis.

e) e. The preoutis have gone through IP, i.e Opposite of initial permutation to produce 64 bit cipher text.

SINGLE ROUND DES

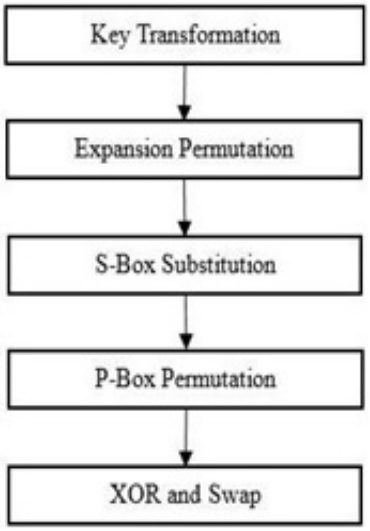

Figure 2:

3.2 DES-Feistel function

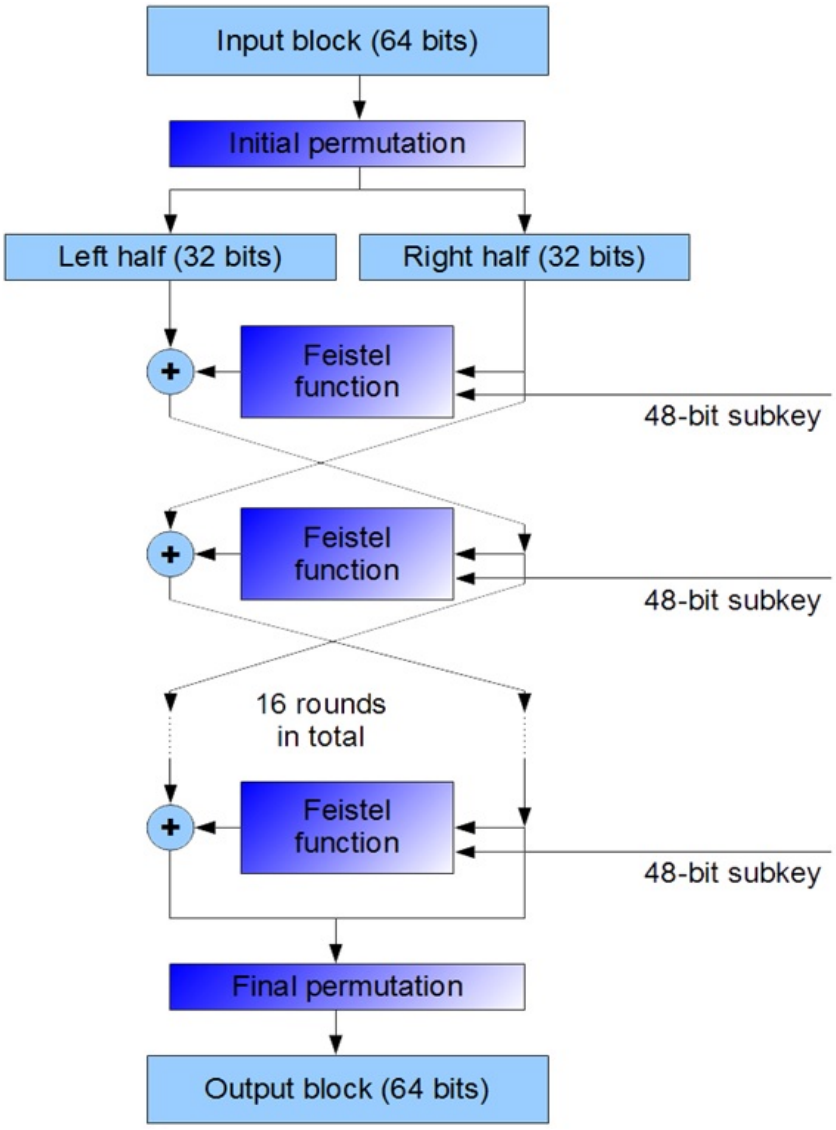

Figure 3:

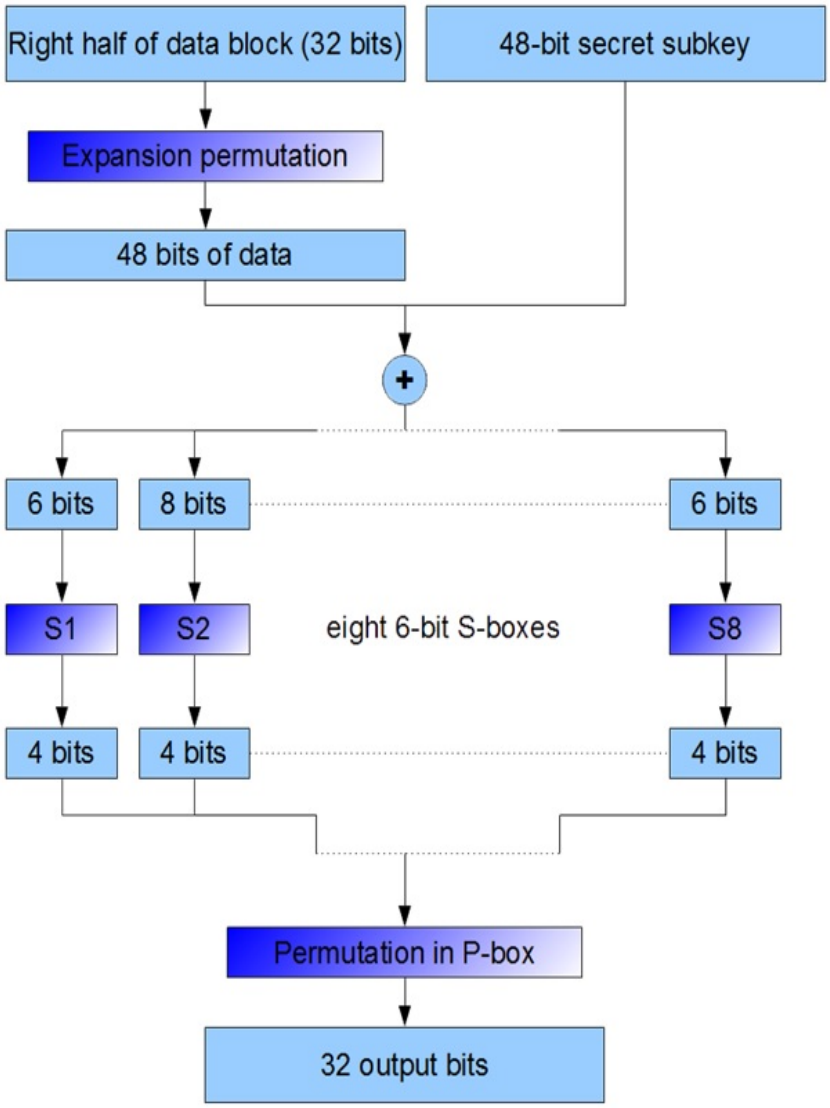
Right half of data block (32 bits)
48-bit secret subkey
Expansion permutation
48 bits of data
+
6 bits
8 bits
6 bits
S1
S2
eight 6-bit S-boxes
S8
4 bits
4 bits
4 bits
Permutation in P-box
32 output bits

Figure 4:

3.3 DES - key schedule

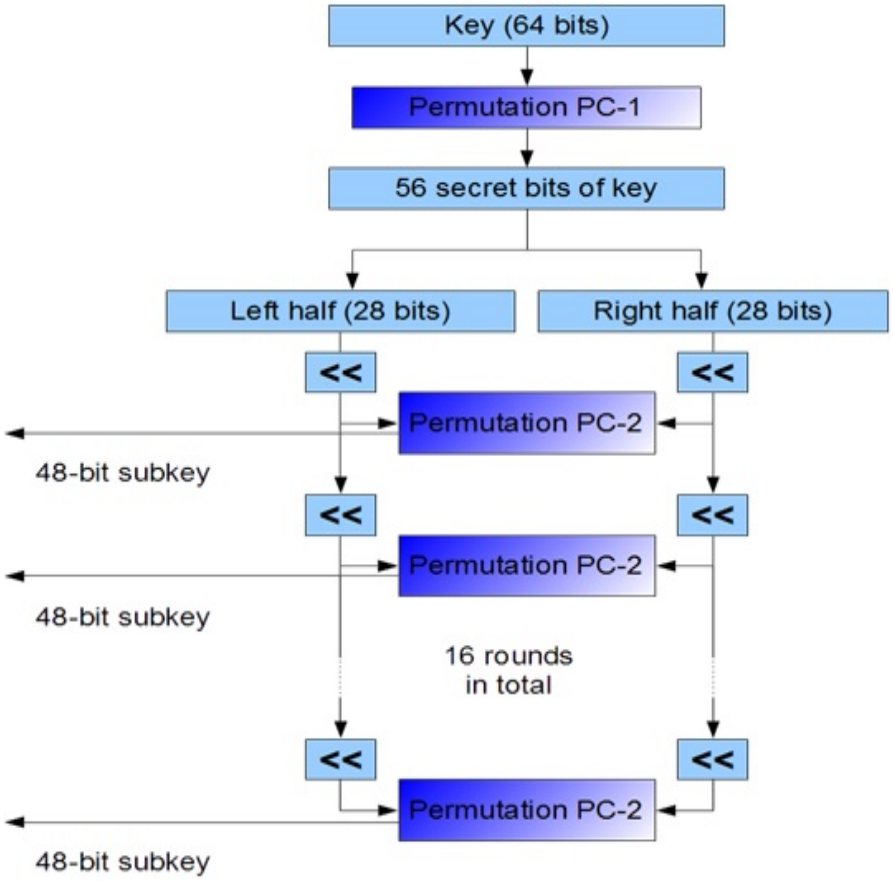

Figure 5:

3.3 MATHEMATICAL PROCEDURE

1. The presentation of permutations are in the table form only to understand easily. The data which are input are vectors and are not matrices.

2. The tables of permutation are read row by row from left to right and from top to bottom.

3. The bits which are permuted are read as follows.

   - The resultant first output is the bit from the input block whose position taken from the first row and the first column of the table.
   - The resultant second output is the bit from the input block whose position is taken from the first row and the second column of the table.
   - The resultant last output is the bit from the input block whose position is taken from the first row and the last column of the table.

3.4 Initial Permutation

It is done on every block of input data in the beginning stage of encryption.

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

3.5 Permutation Key PC-1

From 64-bit key only 56 bits are selected. The key is then divided as left half and right half. Bit shifting is done on every part. (Every eight bit can be used for parity control which is excluded from encryption.

Left half						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
Right half						
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

3.6 Permutation Expansion

Every round feistel function is initiated by expansion. The right half of data is expanded form 32 to 48 bits.

32	1	2	3	4	5	4	5
6	7	8	9	8	9	10	11
12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21
22	23	24	25	24	25	26	27
28	29	28	29	30	31	32	1

3.7 Binary Shifting

The 48 bits are rotated left by one or 2 bits.

No. of cycle	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Amount of bits	1	1	2	2	2	2	2	2	1	2	2	2	2	2	1	16

3.8 Permutation Key PC-2

From the 56 bit subkey which is output of a given round of feistel function, only 48 bit subkey are selected.

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

3.9 S-Blocks

- 48 bit input is divided into 6 bit input of 8 blocks.
- From each 6 bit the first and the last bit is taken as a row value and the remaining 4 bits are taken as a column value.
- The resultant S- box value is a 4 bit output. For eg, for a 6 bit input 001110 the row value is 0(00) and the column value is 7(0111) and the resultant S1 box is 8 whose 4 bit output is 1000.

S_1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	1	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

3.10 Permutation P

The output block of 32 bit from S -box undergo P-Permutation

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

3.11 Final Permutation

This is done for every block of data which is the inverse of IP.

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

For example we take“8989898989898989” as a plain text and encrypt with DES key as “ 5E32BD0EA6P3D792”. The result would be a cipher text. If the cipher text is decrypted with the same DES key the result is the original plain text.

Consider the message “MATHEMATICS MAKES LIFE SIMPLE AND EASY” which is a plain text with 33 bits (66 hexa decimal digits) long. This message is not 64 bit so it must be padded with some extra bits at the tail end for the encryption. Once the message encrypted has been decrypted, extra bits are removed and the original message is obtained.

There are many ways of padding to add extra bits. It is sufficient to add zeros at the end so that we get multiple of 8 bytes or 16 hexa decimal digits or 64 bits as the total message.

4 Conclusion

In this paper we have explained mathematical procedure for DES algorithm and have also given examples for the same. The major concern in DES algorithm security is about 2 areas such as nature of algorithm and key size. It is clear that DES can be broken using 2^{55} encryptions. However, today most applications use either 3DES with two keys or 3DES with three keys. These two multiple DES versions make DES resistant to brute- force attacks.

References

[1] A William Stallings, Network Security Essentials (Applications and Standards), Pearson Education, 2004.

[2] Atul Kahate, Cryptography and Network Security, Tata Mc Graw-Hill Companies, 2008.

[3] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha, Performance Evaluation of Symmetric Cryptography Algorithms, International Journal of Electronics and CommunicationTechnology, Vol- (2)3,2011.

[4] Pratap Chandra Mandal, Superiority of Blowfish Algorithm, International Journal of Advanced Research in Computers Science and Software Engineering, Vol(2)9, 2012.

[5] Mitali, Vijay Kumar and Arvind Sharma, A Survey on Various Cryptography Technique, International Journal Of Emerging Trends & Technology in Computer Science, Vol-(3)4, 2014

[6] Daemen, J., and Rijmen,V., Rijndael: The Advanced Encryption Standard, Dr. Dobb's Journal, 2001.

[7] R.L.Rivest, A.Shamir, and L.Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communication of the ACM, Vol(21) 2, 1978.

[8] E.Thambiraja, G.Ramesh, R.Umarani, A survey on various most common encryption techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Vol-(2) 7, 2012.

[9] Monika Agrawal, Pradeep Mishra, A Comparative Survey of Symmetric Key Encryption Techniques, International Journal of Computer Science and communication.....

[10] Vikrant M. Adki, Prof.ShubhanandS.Hatkar, A Survey on Cryptography Techniques

[11] Simar Preet Singh, and Raman Maini, Comparison of Data Encryption Algorithms, International Journal of Computer Science and Communication

[12] Anoop MS, Tata Elxsi Ltd, India, Public Key Cryptography, Applications Algorithms and Mathematical Explanations