Data Encryption Standard

In 1974 - DES was proposed by IBM and it was published in the Fedral Register as a draft.

Criticised because of

(i) Small key length (56 - bits) ✓

(ii) Hidden design behind the internal structure.

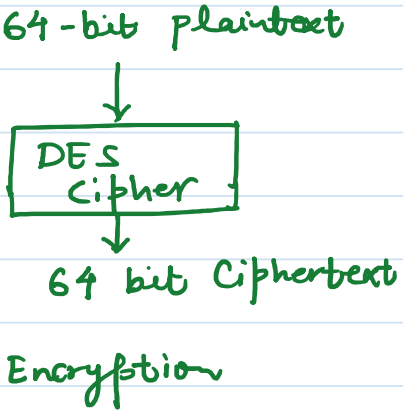
Final it was published in Fedral register 1977.

Was US std from 1977 - 1998.

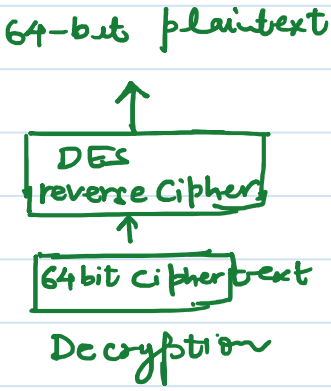
Most studied syn key block cipher.

In 1998, NIST issued a new standard 3 DES.

Overview

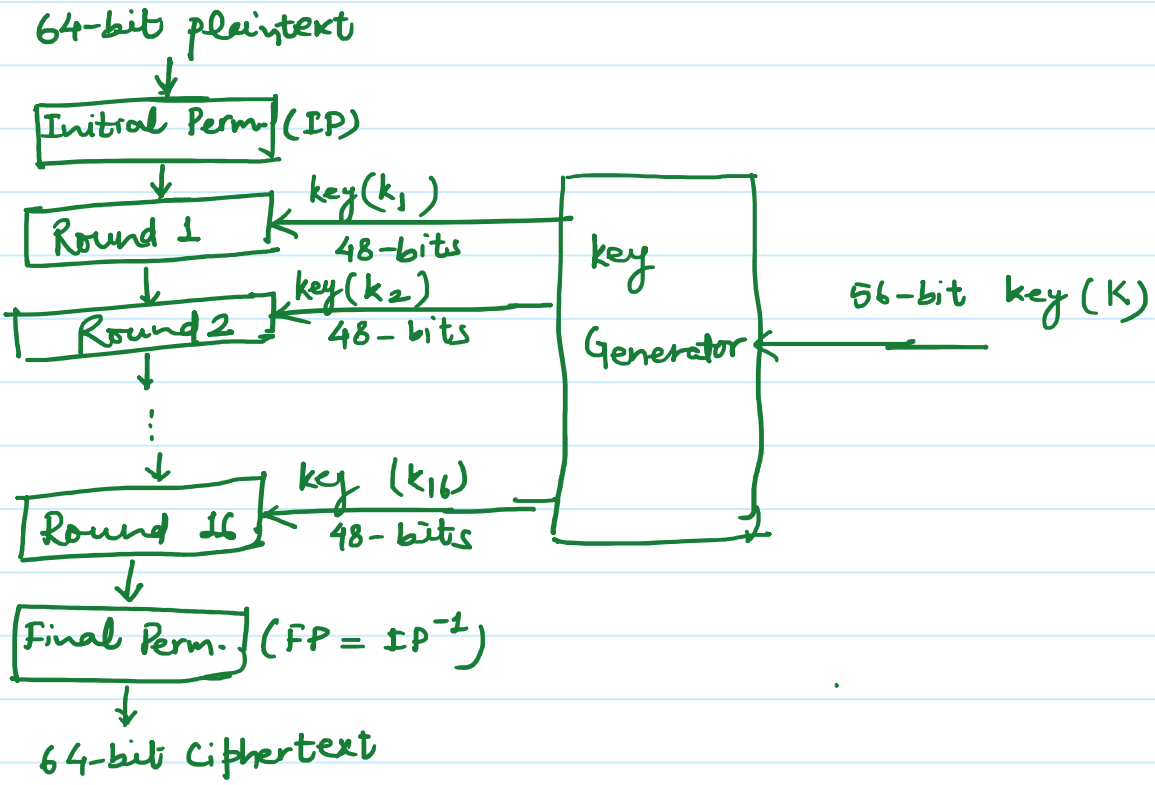


Encryption

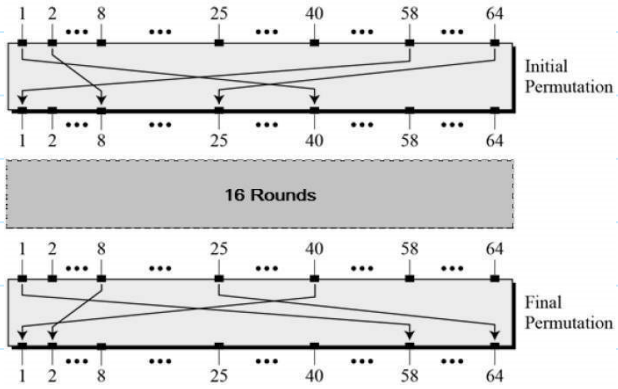


Decryption

DES Structure



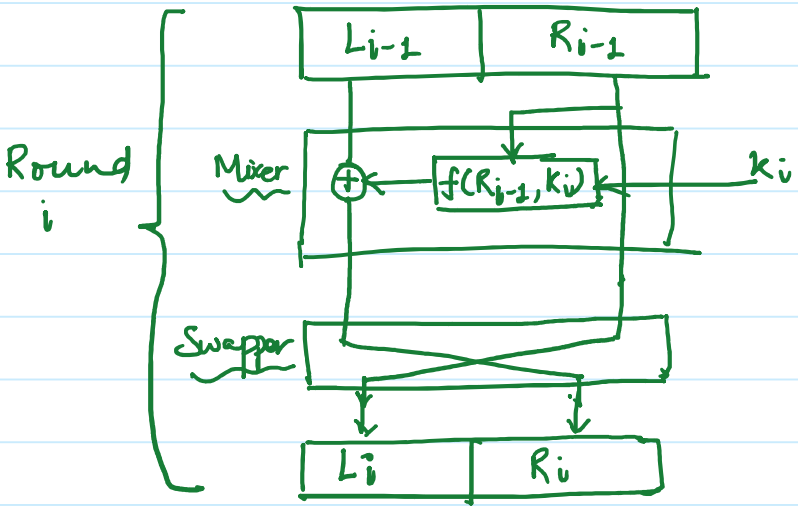
Initial and Final Permutations:



Initial Permutation	*Final Permutation*
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

IP & FP Tables.

Rounds in DES.

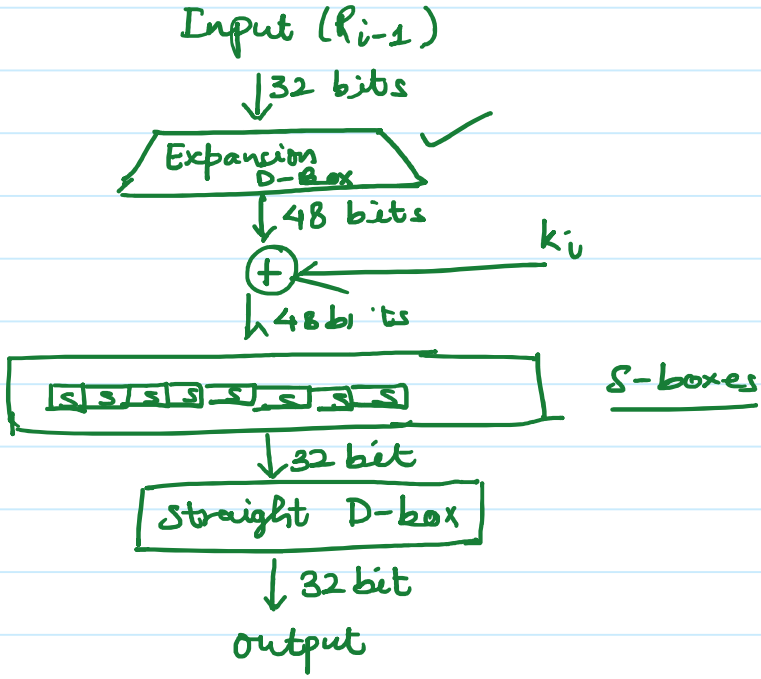


Mixer & swapper are invertible element

$f(R_{i-1}, k_i)$ Contains all non-invertible elements of DES.

Encryption

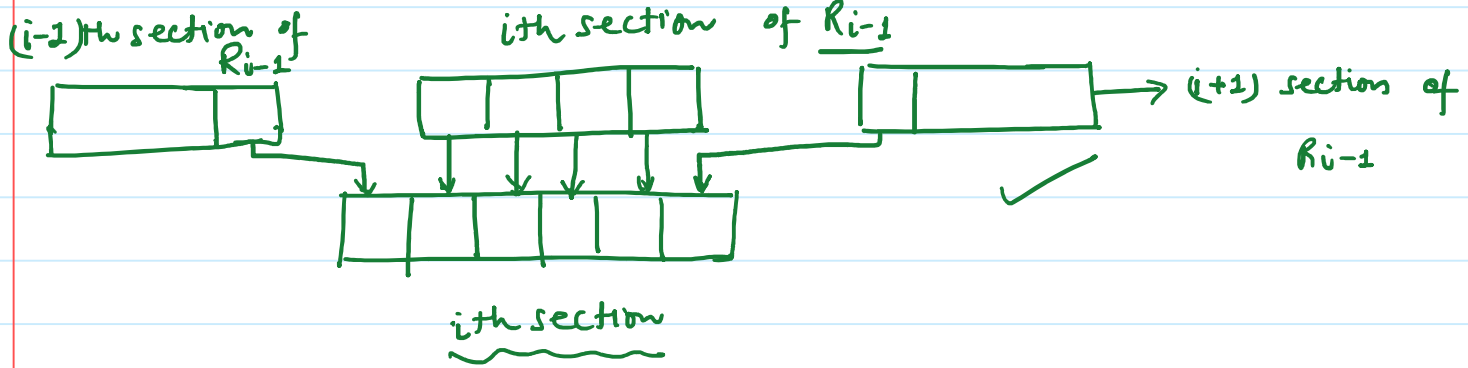
DES Function :



Expansion D-box in DES Function :

→ First R_{i-1} is divided into 8 4-bit sections.

→ Each 4 bit section then expanded to 6-bits using a predefined permutation table.



32	01	02	03	04	05
04	05	06	07	08	09
08	09	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	31	31	32	01

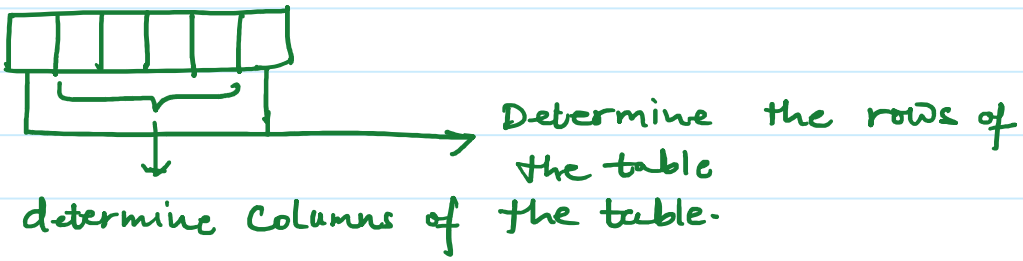
Expansion D-box table

S-Boxes in DES Function :

→ S-boxes creates confusion.

→ 8 - S-boxes, each with 6-bits of input & 4 bits of output

→ The substitution in each box follows a predefined rule based on a 4x16 table.



Example

Input 101101

Output 0010

Fifth S-box table →

S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Straight D-Box:

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Straight D-Box table.