S-DES

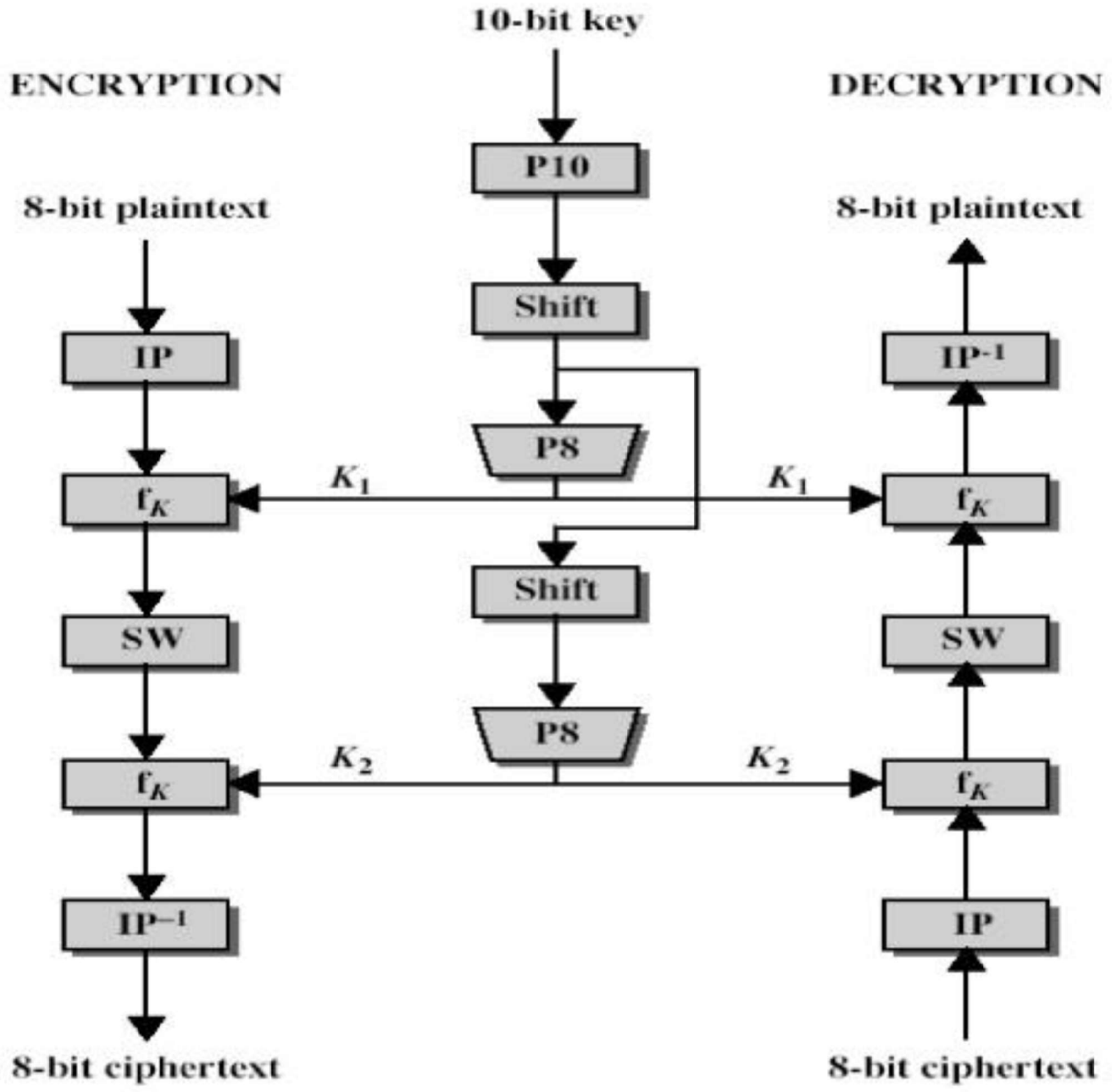
- **The S-DES encryption algorithm takes an *8-bit block of plaintext* and a *10-bit key* as input and produces an 8-bit block of ciphertext as output.**
- **S-DES depends on the use of a 10-bit key shared between sender and receiver. From this key, *two 8-bit subkeys* are produced for use in particular stages of the encryption and decryption algorithm.**
- **The S-DES decryption algorithm takes an *8-bit block of ciphertext* and the same *10-bit key* used to produce that ciphertext as input and produces the original *8-bit block of plaintext*.**

S-DES

The encryption algorithm involves five functions:

- ***Initial permutation (IP).***
- **A complex *function labeled* f_K :which involves both permutation and substitution operations and depends on a key input.**
- **A simple permutation function that switches *(SW)* the two halves of the data.**
- **The function f_K again.**
- **Finally a permutation function that is the inverse of the initial permutation *(*IP^{-1}*).***

S-DES


10-bit key
ENCRYPTION
DECRYPTION
P10
8-bit plaintext
8-bit plaintext
Shift
IP
IP-1
P8
K1
K1
fK
fK
Shift
SW
SW
P8
K2
K2
fK
fK
IP–1
IP
8-bit ciphertext
8-bit ciphertext

S-DES

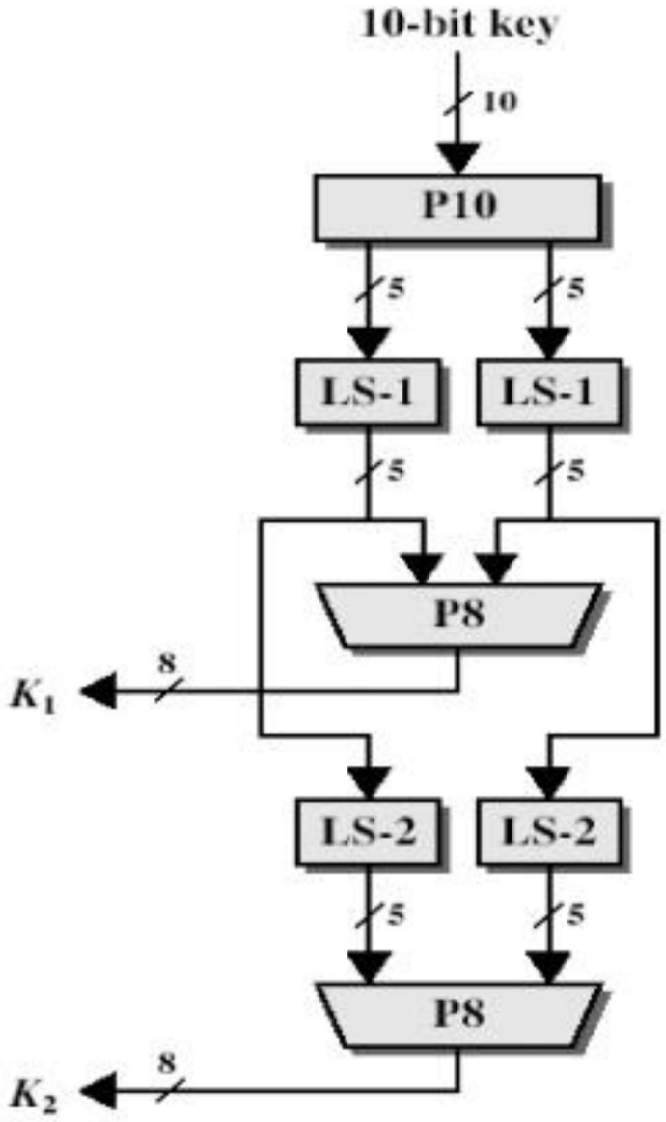
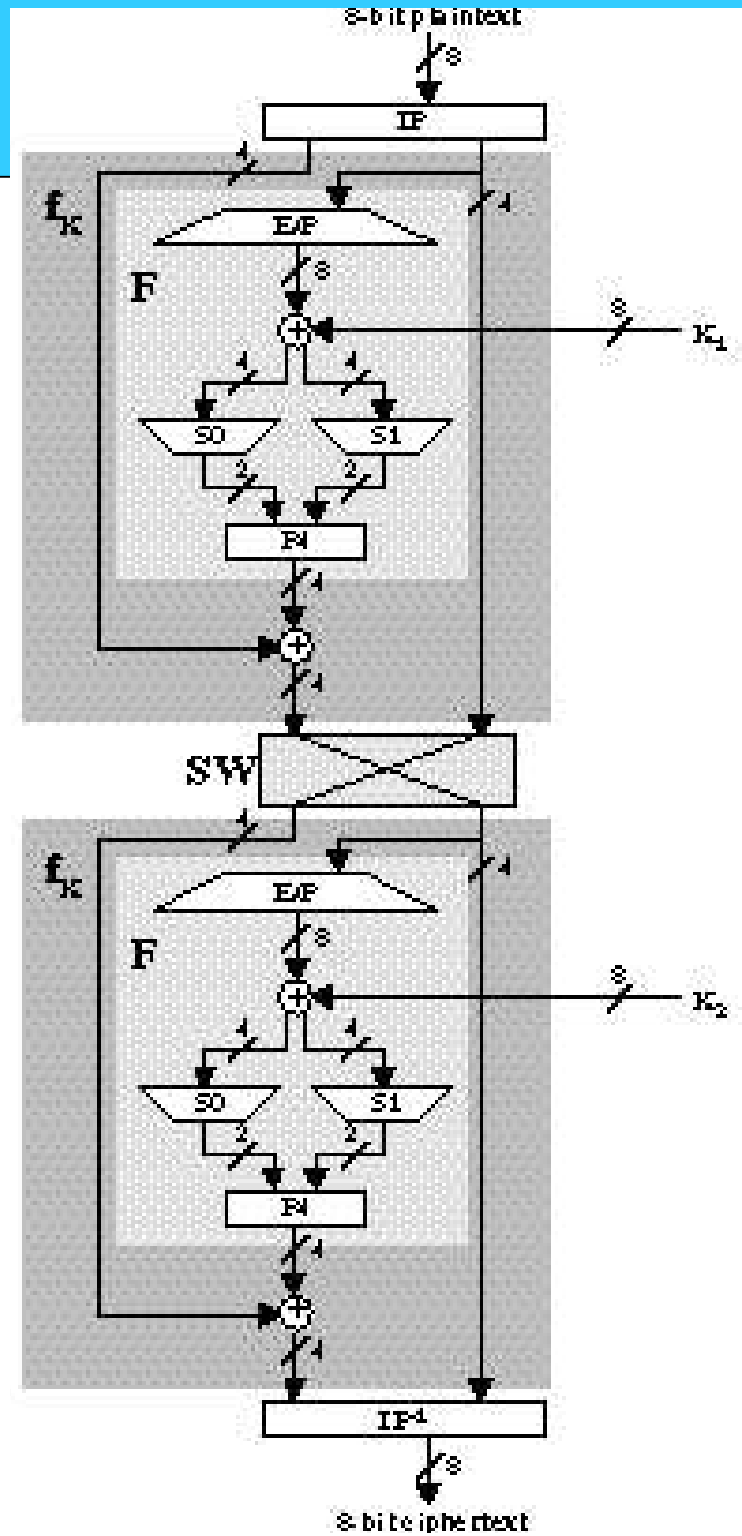


Figure: key generation for S-DES

S-DES


8-bit plaintext
8
IP
4
4
f_K
E/P
F
8
8
K_1
4
4
S0
S1
2
2
P4
4
4
SW
4
f_K
E/P
F
8
8
K_2
4
4
S0
S1
2
2
P4
4
4
IP^{-1}
8
8 bit ciphertext

S-DES

$$\text{Ciphertext} = IP^{-1} \circ f_{K2} \circ SW \circ f_{K1} \circ IP$$

$$\text{Ciphertext} = IP^{-1}(f_{K2}(SW(f_{K1}(IP(\text{plaintext})))))$$

$$K_1 = \text{P8}\left(\text{Shift}\left(\text{P10}(\text{key})\right)\right)$$

$$K_2 = \text{P8}\left(\text{Shift}\left(\text{Shift}\left(\text{P10}(\text{key})\right)\right)\right)$$

$$\text{plaintext} = IP^{-1}\left(f_{K_1}\left(SW\left(f_{K_2}\left(IP(\text{ciphertext})\right)\right)\right)\right)$$

S-DES: Key Computation

P10									
3	5	2	7	4	10	1	9	8	6

Shift 1 (LS-1): Divide input to equal halves and perform a circular left shift (LS-1), or rotation, separately on the first five bits and the second five bits

P8							
6	3	7	4	8	5	10	9

Shift 2 (LS-2): We then go back to the pair of 5-bit strings produced by the two LS-1 functions and perform a circular left shift of 2 bit positions on each string

S-DES Encryption

IP							
2	6	3	1	4	8	5	7

IP^{-1}							
4	1	3	5	7	2	8	6

S-DES

- The most complex component of S-DES is the function f_K, which consists of a combination of permutation and substitution functions.
- The functions can be expressed as follows: Let L and R be the leftmost 4 bits and rightmost 4 bits of the 8-bit input to f_K

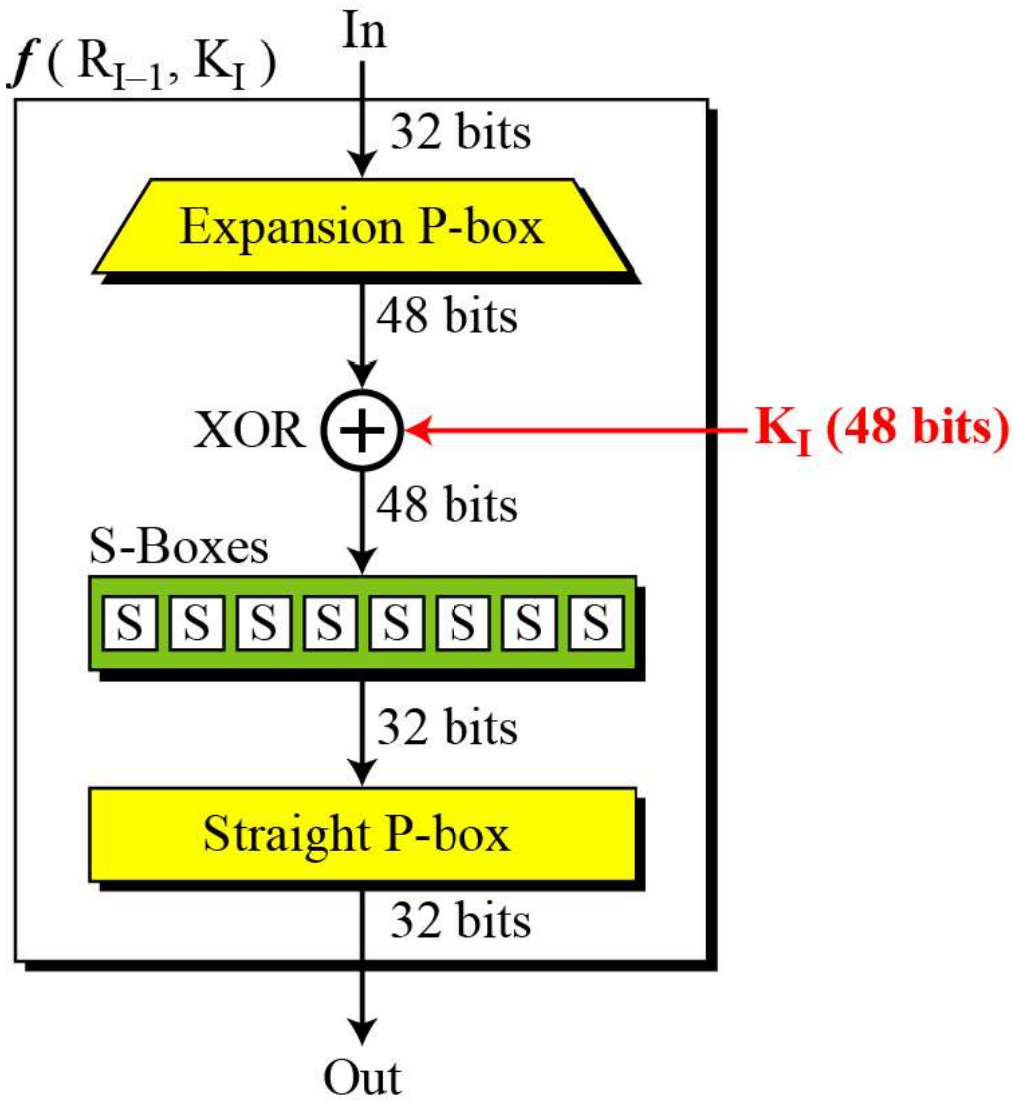
$$f_K(L, R) = (L \oplus F(R, SK), R)$$

where SK is a subkey and xor is the bit-by-bit exclusive-OR function. The F(R,SK) will execute in similar manner as for DES.

S-DES

E/P							
4	1	2	3	2	3	4	1

P4			
2	4	3	1



S-DES

The first and fourth input bits are treated as a 2-bit number that specify a row of the S-box, and the second and third input bits specify a column of the S-box.

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

S-DES

- The Switch Function the function f_K only alters the leftmost 4 bits of the input. The switch function (SW) interchanges the left and right 4 bits so that the second instance of f_K operates on a different 4 bits.
- In this second instance, the E/P, S0, S1, and P4 functions are the same. The key input is K2.

Key Generation

Key Generation

Key (10-bit):	1	0	1	0	0	0	0	0	1	0	Input
P10:	1	0	0	0	0	0	1	1	0	0	
Shift (1-Bit):	0	0	0	0	1	1	1	0	0	0	
Key -1 P8:	1	0	1	0	0	1	0	0			
Shift (2-Bit):	0	0	1	0	0	0	0	0	1	1	
Key -2 P8:	0	1	0	0	0	0	1	1			

K_1= P8 (Shift_1(P10(Key)))

K_2= P8(Shift_2(Shift_1(P10(Key))))

P10:	3	5	2	7	4	10	1	9	8	6

P8:	6	3	7	4	8	5	10	9

Encryption

Encryption

Plaintext :	0	1	1	1	0	0	1	0

IP :	1	0	1	0	1	0	0	1

$$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$$

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

IP :	2	6	3	1	4	8	5	7

IP^{-1} :	4	1	3	5	7	2	8	6

Encryption

Plaintext :	0	1	1	1	0	0	1	0
IP :	1	0	1	0	1	0	0	1

1	1	0	0
0	0	1	1

$$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$$

$$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)),\ R)$$

IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6
E/P :	4	1	2	3	2	3	4	1

Encryption

Plaintext :	0	1	1	1	0	0	1	0
IP :	1	0	1	0	1	0	0	1

$1 \oplus 1 = 0$	$1 \oplus 0 = 1$	$0 \oplus 1 = 1$	$0 \oplus 0 = 0$
$0 \oplus 0 = 0$	$0 \oplus 1 = 1$	$1 \oplus 0 = 1$	$1 \oplus 0 = 1$

$$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$$

$$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)),\ R)$$

IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6
E/P :	4	1	2	3	2	3	4	1

Encryption

Plaintext :	0	1	1	1	0	0	1	0
IP :	1	0	1	0	1	0	0	1

S-Box I	$1 \oplus 1 = 0$	$1 \oplus 0 = 1$	$0 \oplus 1 = 1$	$0 \oplus 0 = 0$
S-Box II	$0 \oplus 0 = 0$	$0 \oplus 1 = 1$	$1 \oplus 0 = 1$	$1 \oplus 0 = 1$
	Row	Column	Column	Row

$F(R, k_i) = 10\ 11$

P4 : 0111

$F_{k_1}(L, R) = (1010 \oplus 0111, 1001) = (1101\ 1001)$

SW : 1001 1101

$$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$$

$$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)),\ R)$$

P4:

2	4	3	1

S_0 :

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1 :

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

Encryption

Plaintext :	0	1	1	1	0	0	1	0
SW :	1	0	0	1	1	1	0	1

$$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$$

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6

Encryption

Plaintext :	0	1	1	1	0	0	1	0
SW :	1	0	0	1	1	1	0	1

1	1	1	0
1	0	1	1

$$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$$

$$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)),\ R)$$

IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6
E/P :	4	1	2	3	2	3	4	1

Encryption

Plaintext :	0	1	1	1	0	0	1	0
SW :	1	0	0	1	1	1	0	1

$1 \oplus 0 = 1$ | $1 \oplus 1 = 0$ | $1 \oplus 0 = 1$ | $0 \oplus 0 = 0$

$1 \oplus 0 = 1$ | $0 \oplus 0 = 0$ | $1 \oplus 1 = 0$ | $1 \oplus 1 = 0$

$$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$$

$$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)),\ R)$$

IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6
E/P :	4	1	2	3	2	3	4	1

Encryption

Plaintext :	0	1	1	1	0	0	1	0
SW :	1	0	0	1	1	1	0	1

S-Box I	$1 \oplus 0 = 1$	$1 \oplus 1 = 0$	$1 \oplus 0 = 1$	$0 \oplus 0 = 0$
S-Box II	$1 \oplus 0 = 1$	$0 \oplus 0 = 0$	$1 \oplus 1 = 0$	$1 \oplus 1 = 0$
	Row	Column	Column	Row

$F(R, k_i) = 10\ 11$

P4 : 0111

$F_{k_2}(L, R) = (1001 \oplus 0111, 1101) = (1110\ 1101)$

$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$

$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)), R)$

P4:

2	4	3	1

S_0 :

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1 :

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

Encryption

Plaintext :	0	1	1	1	0	0	1	0
SW :	1	0	0	1	1	1	0	1

S-Box I	$1 \oplus 0 = 1$	$1 \oplus 1 = 0$	$1 \oplus 0 = 1$	$0 \oplus 0 = 0$
S-Box II	$1 \oplus 0 = 1$	$0 \oplus 0 = 0$	$1 \oplus 1 = 0$	$1 \oplus 1 = 0$
	Row	Column	Column	Row

$F(R, k_i) = 10\ 11$

P4 : 0111

$F_{k_2}(L, R) = (1001 \oplus 0111, 1101) = (1110\ 1101)$

IP^{-1} : 01110111

$$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$$

IP^{-1} :	4	1	3	5	7	2	8	6

Encryption

Plaintext :	0	1	1	1	0	0	1	0
SW :	1	0	0	1	1	1	0	1

S-Box I	$1 \oplus 0 = 1$	$1 \oplus 1 = 0$	$1 \oplus 0 = 1$	$0 \oplus 0 = 0$
S-Box II	$1 \oplus 0 = 1$	$0 \oplus 0 = 0$	$1 \oplus 1 = 0$	$1 \oplus 1 = 0$
	Row	Column	Column	Row

$F(R, k_i) = 10\ 11$

P4 : 0111

Ciphertext

$F_{k_2}(L, R) = (1001 \oplus 0111, 1101) = (1110\ 1101)$

IP^{-1} : 0111 0111

$$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$$

IP^{-1} :	4	1	3	5	7	2	8	6

Decryption

Decryption

Ciphertext :	0	1	1	1	0	1	1	1
IP :	1	1	1	0	1	1	0	1

$$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$$

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6

Decryption

Ciphertext :	0	1	1	1	0	1	1	1
IP :	1	1	1	0	1	1	0	1

1	1	1	0
1	0	1	1

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

$$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)),\ R)$$

IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6
E/P :	4	1	2	3	2	3	4	1

Decryption

Ciphertext :	0	1	1	1	0	1	1	1
IP :	1	1	1	0	1	1	0	1

$1 \oplus 0 = 1$	$1 \oplus 1 = 0$	$1 \oplus 0 = 1$	$0 \oplus 0 = 0$
$1 \oplus 0 = 1$	$0 \oplus 0 = 0$	$1 \oplus 1 = 0$	$1 \oplus 1 = 0$

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

$$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)),\ R)$$

IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6
E/P :	4	1	2	3	2	3	4	1

Decryption

Ciphertext :	0	1	1	1	0	1	1	1
IP :	1	1	1	0	1	1	0	1

S-Box I	$1 \oplus 0 = 1$	$1 \oplus 1 = 0$	$1 \oplus 0 = 1$	$0 \oplus 0 = 0$
S-Box II	$1 \oplus 0 = 1$	$0 \oplus 0 = 0$	$1 \oplus 1 = 0$	$1 \oplus 1 = 0$
	Row	Column	Column	Row

$F(R, k_i) = 10\ 11$ P4 : 0111

$F_{k_1}(L, R) = (1110 \oplus 0111, 1101) = (1001\ 1101)$ SW : 1101 1001

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

$$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)),\ R)$$

P4:

2	4	3	1

S_0 :

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1 :

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

Decryption

Ciphertext :	0	1	1	1	0	1	1	1
SW :	1	1	0	1	1	0	0	1

$$Ciphertext = IP^{-1}(F_{k2}(SW(F_{k1}(IP(Plaintext)))))$$

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6

Decryption

Ciphertext :	0	1	1	1	0	1	1	1
SW :	1	1	0	1	1	0	0	1

1	1	0	0
0	0	1	1

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

$$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)),\ R)$$

IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6
E/P :	4	1	2	3	2	3	4	1

Decryption

Ciphertext :	0	1	1	1	0	1	1	1
SW :	1	1	0	1	1	0	0	1

$1 \oplus 1 = 0$	$1 \oplus 0 = 1$	$0 \oplus 1 = 1$	$0 \oplus 0 = 0$
$0 \oplus 0 = 0$	$0 \oplus 1 = 1$	$1 \oplus 0 = 1$	$1 \oplus 0 = 1$

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

$$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)),\ R)$$

IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6
E/P :	4	1	2	3	2	3	4	1

Decryption

Ciphertext :	0	1	1	1	0	1	1	1

SW :	1	1	0	1	1	0	0	1

S-Box I	$1 \oplus 1 = 0$	$1 \oplus 0 = 1$	$0 \oplus 1 = 1$	$0 \oplus 0 = 0$
S-Box II	$0 \oplus 0 = 0$	$0 \oplus 1 = 1$	$1 \oplus 0 = 1$	$1 \oplus 0 = 1$
	Row	Column	Column	Row

$$F(R, k_i) = 10\ 11$$

P4 :	0111

$$F_{k_2}(L, R) = (1101 \oplus 0111, 1001) = (\mathbf{1010}\ 1001)$$

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

$$F_{k_i}(L, R) = (L \oplus P4(F(R, k_i)), R)$$

P4:	2	4	3	1

S_0 :

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1 :

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

Decryption

Ciphertext :	0	1	1	1	0	1	1	1
SW :	1	1	0	1	1	0	0	1

S-Box I	$1 \oplus 1 = 0$	$1 \oplus 0 = 1$	$0 \oplus 1 = 1$	$0 \oplus 0 = 0$
S-Box II	$0 \oplus 0 = 0$	$0 \oplus 1 = 1$	$1 \oplus 0 = 1$	$1 \oplus 0 = 1$
	Row	Column	Column	Row

$F(R, k_i) = 10\ 11$ P4 : 0111

$F_{k_2}(L, R) = (1101 \oplus 0111, 1001) = (1010\ 1001)$ IP^{-1} : 0111 0010

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

IP^{-1} :	4	1	3	5	7	2	8	6

Decryption

Ciphertext :	0	1	1	1	0	1	1	1
SW :	1	1	0	1	1	0	0	1

S-Box I	$1 \oplus 1 = 0$	$1 \oplus 0 = 1$	$0 \oplus 1 = 1$	$0 \oplus 0 = 0$
S-Box II	$0 \oplus 0 = 0$	$0 \oplus 1 = 1$	$1 \oplus 0 = 1$	$1 \oplus 0 = 1$
	Row	Column	Column	Row

$F(R, k_i) = 10\ 11$

P4 : 0111

Plaintext

$F_{k_2}(L, R) = (1101 \oplus 0111, 1001) = (1010\ 1001)$

IP^{-1} : 0111 0010

$$Plaintext = IP^{-1}(F_{k1}(SW(F_{k2}(IP(Ciphertext)))))$$

IP^{-1} :	4	1	3	5	7	2	8	6

Examples

Plaintext :	1	1	0	1	0	1	0	1

Key (10-bit):	0	1	1	1	0	1	0	0	0	1

Examples

Plaintext :	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	
Key (10-bit):	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**1**
Ciphertext :	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**1**	

Thank You.