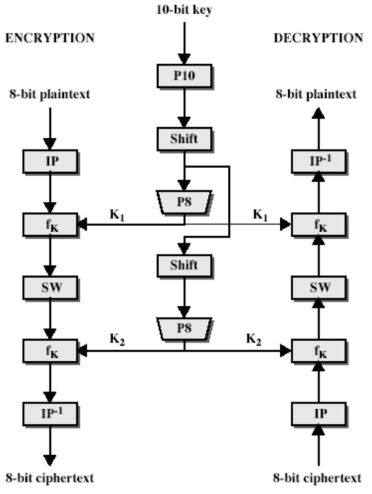
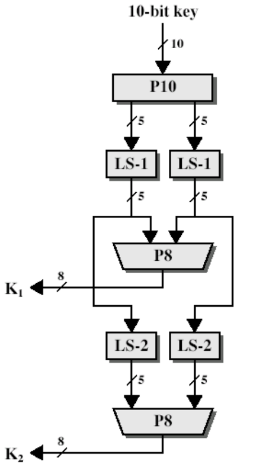
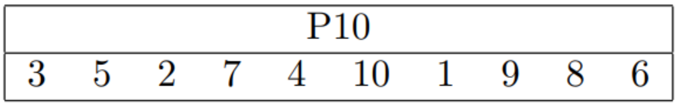


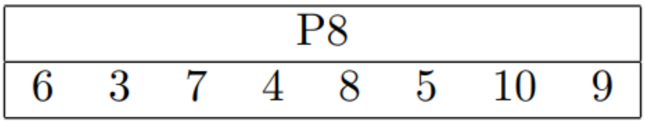
Simplified DES Scheme



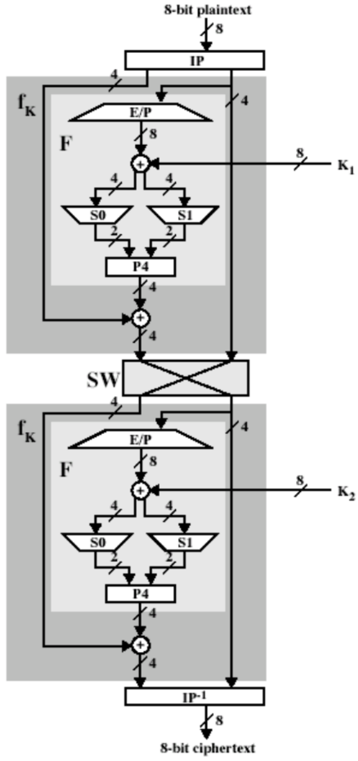
Key Generation for Simplified DES



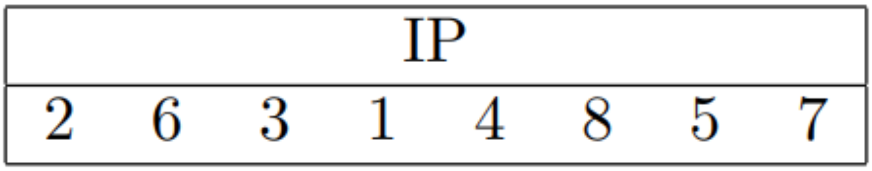
P10									
3	5	2	7	4	10	1	9	8	6



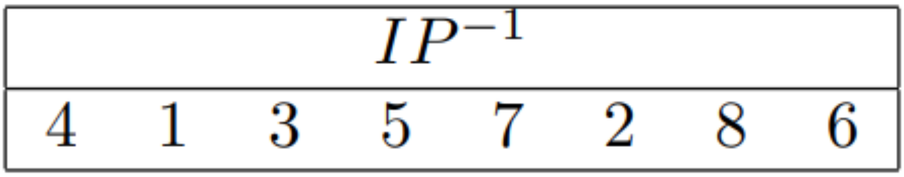
P8							
6	3	7	4	8	5	10	9



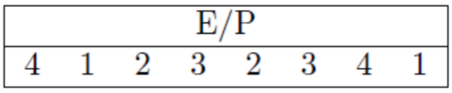
Simplified DES Encryption Detail



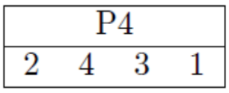
IP							
2	6	3	1	4	8	5	7



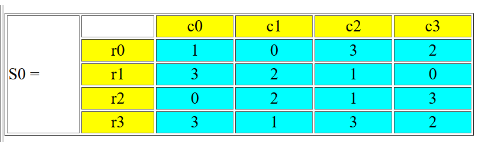
IP^{-1}							
4	1	3	5	7	2	8	6



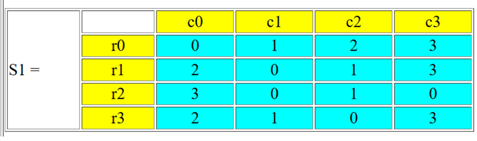
E/P							
4	1	2	3	2	3	4	1



P4			
2	4	3	1



S0 =		c0	c1	c2	c3
	r0	1	0	3	2
	r1	3	2	1	0
	r2	0	2	1	3
	r3	3	1	3	2



S1 =		c0	c1	c2	c3
	r0	0	1	2	3
	r1	2	0	1	3
	r2	3	0	1	0
	r3	2	1	0	3

S-DES Encryption Steps:

1. Key Generation:
   - A 10-bit key is used to generate two 8-bit subkeys: **K1** and **K2**.
2. Initial Permutation (IP):
   - Apply a fixed permutation to the 8-bit plaintext.
3. Round 1 (using K1):
   - Split the 8 bits into Left (L) and Right (R).
   - Apply the **Function F** with K1 on R, and XOR the result with L.
   - Swap the halves.
4. Round 2 (using K2):
   - Apply **Function F** with K2.
   - XOR with the other half (from swap step).
   - No swap after this round.
5. Inverse Initial Permutation (IP^{-1}):
   - Apply the inverse of the initial permutation to get ciphertext.

S-DES Decryption Steps:

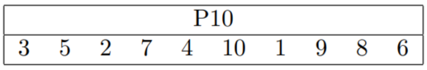
1. Use same key to generate K1 and K2.
2. Initial Permutation (IP):
   - Same as in encryption.
3. Round 1 (using K2):
   - Same as encryption but **K2 is used first**.
4. Round 2 (using K1):
   - Same structure, now use **K1**.
5. Inverse Initial Permutation (IP^{-1}):
   - Same as in encryption to get the original plaintext.

Key Difference:

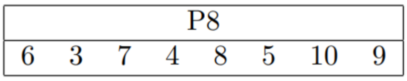
Step	Encryption	Decryption
Round 1 Key	K1	K2
Round 2 Key	K2	K1

Let the plaintext be the string 0010 1000. Let the 10 bit key be 1100011110.

⟵ Sol ⟶



P10									
3	5	2	7	4	10	1	9	8	6



P8							
6	3	7	4	8	5	10	9

1. Key generation :-

K : 11000 11110

$P10(K)$: 00110 01111

$\text{shift}(P10(K))$:- 01100 11110 → left shift by 1

$P8(\text{shift}(P10(K)))$:- 1110 1001 → this is K_1

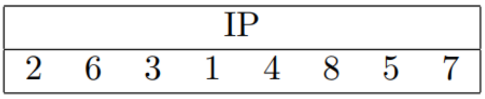
$\text{shift}^2(P10(K))$:- 10001 11011 → left shift by 2

$P8(\text{shift}^2(P10(K)))$:- 1010 0111 → this is K_2

So we have the two keys

$K_1 = \{1110\ 1001\}$, $K_2 = \{1010\ 0111\}$

2. Initial Permutation



IP							
2	6	3	1	4	8	5	7

plain message (P) :- 0010 1000

IP (P) :- 0010 0010

3. Round 1

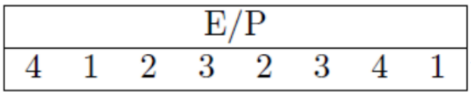
$L = 0010$ $R = 0010$

$f_{K_1} = (L \oplus f(R, K_1), R)$

this Function to XOR ⟵

$= 0010 \oplus f(0010, 1110\ 1001), 0010$

↳ we need to expand to perform XOR



E/P							
4	1	2	3	2	3	4	1

$E/P(R) = 0001\ 0100$

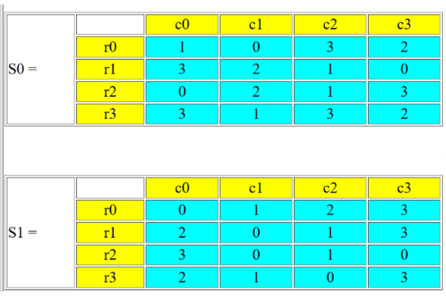
$K_1 = 1110\ 1001$

$E/P(R) \oplus K_1 = 1111\ 1101$

11 → 3 11 → 3

11 → 3 10 → 2

2 0



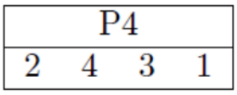
S0 =

	c0	c1	c2	c3
r0	1	0	3	2
r1	3	2	1	0
r2	0	2	1	3
r3	3	1	3	2

S1 =

	c0	c1	c2	c3
r0	0	1	2	3
r1	2	0	1	3
r2	3	0	1	0
r3	2	1	0	3

$S\,Box(E/P(R) \oplus K_1) = 1000 \xrightarrow{P_4} 0001$



P4			
2	4	3	1

then the Result of F = 0001

then we calculate $f_{K_1} = (0010 \oplus 0001, 0010)$

$f_{K_1} = (0011, 0010)$

now we have $L = 0011$, $R = 0010$

then we perform Swap so $R = 0011$, $L = 0010$

4. Round 2

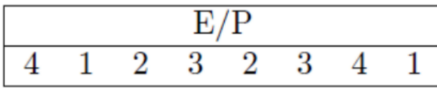
$L = 0010 \quad R = 0011$

$$f_{K_2}(L, R) = (L \oplus f(R, K_2), R)$$

well perform XOR

$$f_{K_2} = (0010 \oplus f(0011, 10100111), 0011)$$

↳ we will expand



E/P							
4	1	2	3	2	3	4	1

$E/P(R) = 10010110$

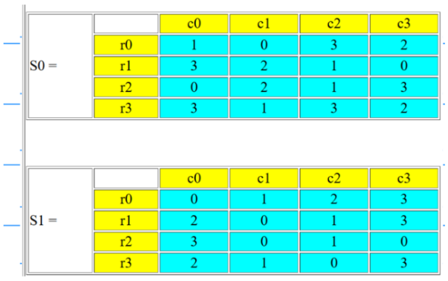
$K_2 = 10100111$

$$E/P(R) \oplus K_2 = \boxed{0011}\boxed{0001}$$

$01 \rightarrow 1 \qquad 01 \rightarrow 1$

$01 \rightarrow 1 \qquad 00 \rightarrow 0$

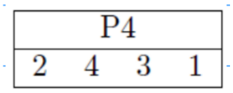
$2 \qquad 2$



S0 =		c0	c1	c2	c3
	r0	1	0	3	2
	r1	3	2	1	0
	r2	0	2	1	3
	r3	3	1	3	2

S1 =		c0	c1	c2	c3
	r0	0	1	2	3
	r1	2	0	1	3
	r2	3	0	1	0
	r3	2	1	0	3

$$SBox(E/P(R \oplus K_2)) = 10\ 10 \xrightarrow{P4} 0011$$



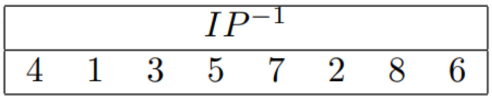
P4			
2	4	3	1

the the result of F is 0011

So we calculate $f_{K_2} = (0010 \oplus 0011, 0011)$

$= (0001, 0011)$

5. Inverse Initial permutation



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

we have 00010011

apply IP^{-1} 10001010

So the final result (Cipher) is 10001010

Let the cipher be 1000 1010. Let the 10 bit key be 1100011110.

← Sol →

1. Key generation:

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9

K: 11000 11110

P10(K): 00110 01111

shift(p10(K)): 01100 11110 → left shift by 1

P8(shift(p10(K))): 1110 1001 → this is K_1

shift^2(p10(K)): 10001 11011 → left shift by 2

P8(shift^2(p10(K))): 1010 0111 → this is K_2

So we have the two keys

$K_1 = \{1110\ 1001\}$, $K_2 = \{1010\ 0111\}$

2. Initial Permutation

IP							
2	6	3	1	4	8	5	7

C = 1000 1010

IP(c) = 00010011

3. Round 1 → Here we will use K_2

L = 0001   R = 0011

$F_{K_2}(L,R) = (L \oplus F(R,K_2), R)$

Perform XOR

$= (0001 \oplus F(0011, 1010\ 0111), 0011)$

we will expand

E/P							
4	1	2	3	2	3	4	1

S0 =

	c0	c1	c2	c3
r0	1	0	3	2
r1	3	2	1	0
r2	0	2	1	3
r3	3	1	3	2

S1 =

	c0	c1	c2	c3
r0	0	1	2	3
r1	2	0	1	3
r2	3	0	1	0
r3	2	1	0	3

E/P(R) = 10010110

K_2 = 10100111

E/P(R) ⊕ K_2 = 0011 0001

01 → 1   01 → 1

01 → 1   00 → 0

2   2

P4			
2	4	3	1

$\text{SBox}(E/P(R) \oplus K_2) = 1010 \xrightarrow{P_4} 0011$

So the Result of F is 0011

now we calculate $F_{K_2} = (0001 \oplus 0011, 0011)$

$F_{K_2} = (0010, 0011)$

now we have L= 0010, R=0011 → so we will swap

So R=0010, L=0011

4. Round 2 ⟶ Here we will use K_1

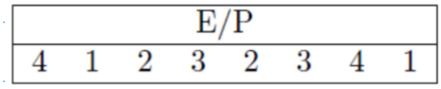
L = 0011 , R = 0010

$f_{K_1}(L, R) = (L \oplus f(R, K_1), R)$

Perform XOR

$= (0011 \oplus f(0010, 11101001), 0010)$

↳ we will expand

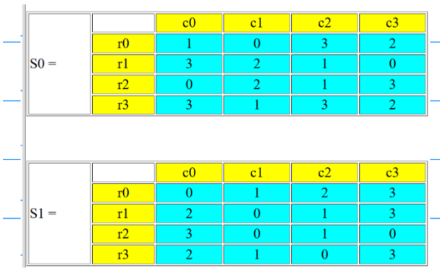


E/P							
4	1	2	3	2	3	4	1

$E/P(R) = 00010100$

$K_1 = 11101001$

$E/P(R) \oplus K_1 = 1111\ 1101$



S0 =		c0	c1	c2	c3
	r0	1	0	3	2
	r1	3	2	1	0
	r2	0	2	1	3
	r3	3	1	3	2

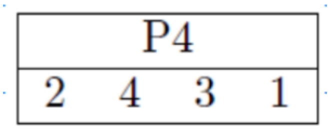
S1 =		c0	c1	c2	c3
	r0	0	1	2	3
	r1	2	0	1	3
	r2	3	0	1	0
	r3	2	1	0	3

11 → 3 11 → 3

11 → 3 10 → 2

2 0

$SBox(E/P(R) \oplus K_1) = 1000 \xrightarrow{P_4} 0001$



P4			
2	4	3	1

So we have F = 0001

then we calculate

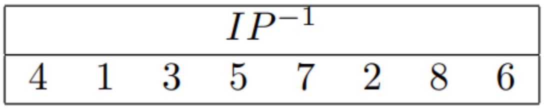
$f_{K_1} = (0011 \oplus 0001, 0010)$

$f_{K_1} = (0010, 0010)$

5. Inverse Initial Permutation:

we have 00100010

apply IP^{-1} 00101000



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

So the final result (plaintext) is 00101000

Thank You

Prepared by: Yahya Ashraf Afifi