Szyfrowanie S-DES

155445 % 25 = 20
20 + 1 = 21

Generowanie kluczy

Nr	Tekst jawny	Klucz
21	0101 0100	1011010010

1. Tabela P10

Numer	1	2	3	4	5	6	7	8	9	10
Wejście	1	0	1	1	0	1	0	0	1	0

Numer	3	5	2	7	4	10	1	9	8	6
Wyjście	1	0	0	0	1	0	1	1	0	1

2. Podział na klucze 5-bitowe

l = 10001
r = 01101

3. Przesunięcie i połączenie pierwszego klucza

l = 00011
r = 11010

w = 0001111010

4. Tabela P8 pierwszego klucza

Pomijamy 1 i 2.

Numer	3	4	5	6	7	8	9	10
Wejście	0	1	1	1	1	0	1	0

Numer	6	3	7	4	8	5	10	9
Wyjście	1	0	1	1	0	1	0	1

Nasz klucz to:
K1 = **10110101**

5. Stworzenie drugiego klucza

Drugi klucz będzie pochodzić z przesunięcia i połączenia dla pierwszego klucza, czyli:
k = 0001111010

6. Przesunięcia drugiego klucza

Najpierw trzeba podzielić klucz na dwie połowy, a następnie przesunąć w lewo o 2:
l = 00011
r = 11010

Przesunięcia:
l = 01100
r = 01011

Po połączeniu otrzymujemy:
w = 0110001011

7. Tabela P8 drugiego klucza

Pomijamy 1 i 2.

Numer	3	4	5	6	7	8	9	10
Wejście	1	0	0	0	1	0	1	1

Numer	6	3	7	4	8	5	10	9
Wyjście	0	1	1	0	0	0	1	1

Nasz klucz to:
K2 = **01100011**

C1 = E(K, M) i dekodowanie

Nr	Tekst jawny	Klucz
21	0101 0100	1011010010

1. Tabela IP-8

Numer	1	2	3	4	5	6	7	8
Wejście	0	1	0	1	0	1	0	0

Numer	2	6	3	1	4	8	5	7
Wyjście	1	1	0	0	1	0	0	0

Wynik:
11001000

2. Tabela EP

Krokiem pośrednim jest podzielenie na słowa 4-bitowe:
l = 1100
r = 1000

Wybieramy r

r	1	0	0	0				
Numer	1	2	3	4	5	6	7	8

Numer	4	1	2	3	2	3	4	1
Wyjście	0	1	0	0	0	0	0	1

Rozszerzone słowo:
ew = 01000001

3. XOR z K1

ew = 01000001
K1 = **10110101**

XOR1 = **11110100**

4. S-0 i S-1

l = 1111
r = 0100

S-0

Cols/Rows	0	1	2	3
0	01	00	11	10
1	11	10	01	00
2	00	10	01	11
3	11	01	11	10

S-1

Cols/Rows	0	1	2	3
0	00	01	10	11
1	10	00	01	11
2	11	00	01	00
3	10	01	00	11

Dla S-0:
wiersz -> 11 -> 3
kolumna -> 11 -> 3

S-0 = 10

Dla S-1:
wiersz -> 00 -> 0
kolumna -> 10 -> 2

S-1 = 10

Połączenie S-0 i S-1:
1010

5. Tabela P-4

Numer	1	2	3	4
Wejście	1	0	1	0

Numer	2	4	3	1
Wyjście	0	0	1	1

Wyjście:
p4 = 0011

6. XOR

Lewe bity z kroku **1:**
l = 1100

XOR:

p4 = 0011
l = 1100

XOR = 1111

Prawe bity z kroku 1:
r = 1000

Połączenie XOR z r:
11111000

7. Zamiana

Musimy zamienić obydwie połówki ze sobą:
11111000 -> 10001111

8. Tabela EP

Po podzieleniu na dwie części:
l = 1000
r = 1111

r	1	1	1	1				
Numer	1	2	3	4	5	6	7	8

Numer	4	1	2	3	2	3	4	1
Wyjście	1	1	1	1	1	1	1	1

Rozszerzone słowo:
ew = 11111111

9. XOR z K2

K2 = **01100011**
ew = 11111111

XOR = 10011100

10. S-0 i S-1

l = 1001
r = 1100

S-0

Cols/Rows	0	1	2	3
0	01	00	11	10
1	11	10	01	00
2	00	10	01	11
3	11	01	11	10

S-1

Cols/Rows	0	1	2	3
0	00	01	10	11
1	10	00	01	11
2	11	00	01	00
3	10	01	00	11

Dla S-0:
wiersz -> 11 -> 3
kolumna -> 00 -> 0

S-0 = 11

Dla S-1:
wiersz -> 10 -> 2
kolumna -> 10 -> 2

S-1 = 01

Połączenie S-0 i S-1:
1101

11. Tabela P-4

Nr	1	2	3	4
Wejście	1	1	0	1

Nr	2	4	3	1
Wyjście	1	1	0	1

Wyjście:
p4 = 1101

12. XOR

p4 = 1101
l = 1000

XOR = 0101

r = 1111

Połączenie XOR z r:
01011111

13. Tabela IP-1

Numer	1	2	3	4	5	6	7	8
Wejście	0	1	0	1	1	1	1	1

Numer	4	1	3	5	7	2	8	6
Wyjście	1	0	0	1	1	1	1	1

Wynik:
1001111

14. Dekodowanie

0	0	0	0	A
0	0	0	1	B
0	0	1	0	C
0	0	1	1	D
0	1	0	0	E
0	1	0	1	F
0	1	1	0	G
0	1	1	1	H
1	0	0	0	I
1	0	0	1	J
1	0	1	0	K
1	0	1	1	L
1	1	0	0	M
1	1	0	1	N
1	1	1	0	O
1	1	1	1	P

1001111

1001 -> J
1111 -> P

C2 = E(K, not(M))

Na podstawie zadania nr 1:
K1 = **10110101**
K2 = **10100001**

not(M) -> 01010100 -> 10101011

Nr	Tekst jawny	Klucz
21	10101011	1011010010

1. Tabela IP-8

Numer	1	2	3	4	5	6	7	8
Wejście	1	0	1	0	1	0	1	1

Numer	2	6	3	1	4	8	5	7
Wyjście	0	0	1	1	0	1	1	1

Wynik:
00110111

2. Tabela EP

Krokiem pośrednim jest podzielenie na słowa 4-bitowe:
l = 0011
r = 0111

Wybieramy r

r	0	1	1	1				
Numer	1	2	3	4	5	6	7	8

Numer	4	1	2	3	2	3	4	1
Wyjście	1	0	1	1	1	1	1	0

Rozszerzone słowo:
ew = 10111110

3. XOR z K1

ew = 10111110
K1 = **10110101**

XOR1 = **00001011**

4. S-0 i S-1

l = 0000
r = 1011

S-0

Cols/Rows	0	1	2	3
0	01	00	11	10
1	11	10	01	00
2	00	10	01	11
3	11	01	11	10

S-1

Cols/Rows	0	1	2	3
0	00	01	10	11
1	10	00	01	11
2	11	00	01	00
3	10	01	00	11

Dla S-0:
wiersz -> 00 -> 0
kolumna -> 00 -> 0

S-0 = 01

Dla S-1:
wiersz ->11 -> 3
kolumna -> 01 -> 1

S-1 = 01

Połączenie S-0 i S-1:
0101

5. Tabela P-4

Numer	1	2	3	4
Wejście	0	1	0	1

Numer	2	4	3	1
Wyjście	1	1	0	0

Wyjście:
p4 = 1100

6. XOR

Lewe bity z kroku **1:**
l = 0011

XOR:
p4 = 1100
l = 0011

XOR = 1111

Prawe bity z kroku 1:
r = 0111

Połączenie XOR z r:
11110111

7. Zamiana

Musimy zamienić obydwie połówki ze sobą:
11110111 -> 01111111

8. Tabela EP

Po podzieleniu na dwie części:
l = 0111
r = 1111

r	1	1	1	1				
Numer	1	2	3	4	5	6	7	8

Numer	4	1	2	3	2	3	4	1
Wyjście	1	1	1	1	1	1	1	1

Rozszerzone słowo:
ew = 11111111

9. XOR z K2

K2 = **01100011**
ew = 11111111

XOR = 10011100

10. S-0 i S-1

l = 1001
r = 1100

S-0

Cols/Rows	0	1	2	3
0	01	00	11	10
1	11	10	01	00
2	00	10	01	11
3	11	01	11	10

S-1

Cols/Rows	0	1	2	3
0	00	01	10	11
1	10	00	01	11
2	11	00	01	00
3	10	01	00	11

Dla S-0:
wiersz -> 11 -> 3
kolumna -> 00 -> 0

S-0 = 11

Dla S-1:
wiersz -> 10 -> 2
kolumna -> 10 -> 2

S-1 = 01

Połączenie S-0 i S-1:
1101

11. Tabela P-4

Nr	1	2	3	4
Wejście	1	1	0	1

Nr	2	4	3	1
Wyjście	1	1	0	1

Wyjście:
p4 = 1101

XOR

p4 = 1101
l = 0111

XOR = 1010

r = 1111

Połączenie XOR z r:
10101111

12. Tabela IP-1

Numer	1	2	3	4	5	6	7	8
Wejście	1	0	1	0	1	1	1	1

Numer	4	1	3	5	7	2	8	6
Wyjście	0	1	1	1	1	0	1	1

Wynik:
01111011

Generowanie kluczy not(K)

Not(K) -> 1011010010 -> 0100101101

Nr	Tekst jawny	Klucz
21	01010100	0100101101

1. Tabela P10

Numer	1	2	3	4	5	6	7	8	9	10
Wejście	0	1	0	0	1	0	1	1	0	1

Numer	3	5	2	7	4	10	1	9	8	6
Wyjście	0	1	1	1	0	1	0	0	1	0

0111010010

2. Podział na klucze 5-bitowe

l = 01110
r = 10010

3. Przesunięcie i połączenie pierwszego klucza

l = 11100
r = 00101

w = 1110000101

4. Tabela P8 pierwszego klucza

Pomijamy 1 i 2.

Numer	3	4	5	6	7	8	9	10
Wejście	1	0	0	0	0	1	0	1

Numer	6	3	7	4	8	5	10	9
Wyjście	0	1	0	0	1	0	1	0

Nasz klucz to:
K1 = **01001010**

5. Stworzenie drugiego klucza

Drugi klucz będzie pochodzić z przesunięcia i połączenia dla pierwszego klucza, czyli:

k = 1110000101

6. Przesunięcia drugiego klucza

Najpierw trzeba podzielić klucz na dwie połowy, a następnie przesunąć w lewo o 2:
l = 11100
r = 00101

Przesunięcia:
l = 10011
r = 10100

Po połączeniu otrzymujemy:
w = 1001110100

7. Tabela P8 drugiego klucza

Pomijamy 1 i 2.

Numer	3	4	5	6	7	8	9	10
Wejście	0	1	1	1	0	1	0	0

Numer	6	3	7	4	8	5	10	9
Wyjście	1	0	0	1	1	1	0	0

Nasz klucz to:
K2 = **10011100**

C3 = E(not(K), not(M))

Not(K) -> 1011010010 -> 0100101101
Not(M) -> 01010100 -> 10101011
K1 = **01001010**
K2 = **10011100**

Nr	Tekst jawny	Klucz
21	10101011	0100101101

1. Tabela IP-8

Numer	1	2	3	4	5	6	7	8
Wejście	1	0	1	0	1	0	1	1

Numer	2	6	3	1	4	8	5	7
Wyjście	0	0	1	1	0	1	1	1

Wynik:
00110111

2. Tabela EP

Krokiem pośrednim jest podzielenie na słowa 4-bitowe:
l = 0011
r = 0111

Wybieramy r

r	0	1	1	1				
Numer	1	2	3	4	5	6	7	8

Numer	4	1	2	3	2	3	4	1

Wyjście	1	0	1	1	1	1	1	0

Rozszerzone słowo:
ew = 10111110

3. XOR z K1

K2 = **10011100**

ew = 10111110
K1 = **01001010**

XOR1 = **11110101**

4. S-0 i S-1

l = 1111
r = 0101

S-0

Cols/Rows	0	1	2	3
0	01	00	11	10
1	11	10	01	00
2	00	10	01	11
3	11	01	11	10

S-1

Cols/Rows	0	1	2	3
0	00	01	10	11
1	10	00	01	11
2	11	00	01	00
3	10	01	00	11

Dla S-0:
wiersz -> 11 -> 3
kolumna -> 11 -> 3

S-0 = 10

Dla S-1:

wiersz -> 01 -> 1
kolumna -> 10 -> 2

S-1 = 01

Połączenie S-0 i S-1:
1001

5. Tabela P-4

Numer	1	2	3	4
Wejście	1	0	0	1

Numer	2	4	3	1
Wyjście	0	1	0	1

Wyjście:
p4 = 0101

6. XOR

Lewe bity z kroku **2:**
l = 0011

XOR:
p4 = 0011
l = 0011

XOR = 0000

Prawe bity z kroku b:
r = 0111

Połączenie XOR z r:
00000111

7. Zamiana

Musimy zamienić obydwie połówki ze sobą:
00000111 -> 01110000

8. Tabela EP

Po podzieleniu na dwie części:
l = 0111
r = 0000

r	0	0	0	0				
Numer	1	2	3	4	5	6	7	8

Numer	4	1	2	3	2	3	4	1
Wyjście	0	0	0	0	0	0	0	0

Rozszerzone słowo:
ew = 00000000

9. XOR z K2

K2 = **10011100**
ew = 00000000

XOR = 00011100

10. S-0 i S-1

l = 0001
r = 1100

S-0

Cols/Rows	0	1	2	3
0	01	00	11	10
1	11	10	01	00
2	00	10	01	11
3	11	01	11	10

S-1

Cols/Rows	0	1	2	3
0	00	01	10	11
1	10	00	01	11
2	11	00	01	00
3	10	01	00	11

Dla S-0:
wiersz -> 01 -> 1
kolumna -> 00 -> 0

S-0 = 11

Dla S-1:
wiersz -> 10 -> 2
kolumna -> 10 -> 2

S-1 = 01

Połączenie S-0 i S-1:
1101

11. Tabela P-4

Nr	1	2	3	4
Wejście	1	1	0	1

Nr	2	4	3	1
Wyjście	1	1	0	1

Wyjście:
p4 = 1101

12. XOR

l = 0111
r = 0000

p4 = 1101
l = 0111

XOR = 1010

r = 0000

Połączenie XOR z r:
10100000

13. Tabela IP-1

Numer	1	2	3	4	5	6	7	8
Wejście	1	0	1	0	0	0	0	0

Numer	4	1	3	5	7	2	8	6
Wyjście	0	1	1	0	0	0	0	0

Wynik:
01100000