

Sieci Komputerowe, ćwiczenie: Szyfrowanie – S-box

Tablice *S-box* (z ang. *Substitution box*) są kluczowym elementem wielu nowoczesnych szyfrów blokowych. Są to pewnego rodzaju 'czarne skrzynki' służące do zamiany znaków (czy bitów) danych wejściowych na inne w celu zamaskowania wzorców czy statystycznych właściwości tych danych. Na ogół są niezmiennie i bardzo starannie dobrane, aby wzmocnić dany szyfr.

Szyfr DES korzysta z 8 tablic S-box $S1 \dots S8$. Działają one tak, że każde 6 bitów danych wejściowych jest zamieniane na 4 bity danych wyjściowych. Z tych 6 bitów, pierwszy i ostatni (czyli 2 bity) to wiersz tablicy, a pozostałe (środkowe 4) to kolumna. Przykładowo, tablica $S1$ ma postać:

S1

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

Założmy, że kolejne 6 bitów danych wejściowych to 101011. Pierwsze i ostatnie bity to 1 i 1, czyli razem 11_2 lub 3_{10} . Środkowe 4 bity to 0101 czyli 5_{10} . Pamiętając, że kolumny i wiersze są numerowane od 0 zamiast od 1, to liczba odpowiadająca kolumnie 5 i rzędkowi 3 to 9. Zamieniamy więc 101011 na 1001.

Poniżej podane są tablice S-box dla szyfru DES. Napisz funkcje w C czy C++, której podaje się liczbę wejściową (opisane 6 bitów) i numer tablicy (od 1 do 8), a która zwraca 4-bitową liczbę wyjściową.

S1

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

S2

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

S3

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

S4

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

S5

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

S6

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

S7

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

S8

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