

Question 1: [5 points]. Generate ten random numbers (s1-s10) using the linear congruently generator (page 35)

using the seed (s 0) as 5, and with the three parameters a, b, and m as 14, 15, and 21, respectively.

seed = 5 a = 14, b = 15, m = 21

$s_0 = (a * s_i + b) \bmod m$

$s_1 = (14 * 5 + 15) \bmod 21 = 85 \bmod 21 = 1$

$s_2 = (14 * 1 + 15) \bmod 21 = 29 \bmod 21 = 8$

$s_3 = (14 * 8 + 15) \bmod 21 = 127 \bmod 21 = 1$

$s_4 = (14 * 1 + 15) \bmod 21 = 29 \bmod 21 = 8$

$s_5 = (14 * 8 + 15) \bmod 21 = 127 \bmod 21 = 1$

The random number is 1 and 8 because it keeps repeated.

Question 2: [5 points] For a Linear Feedback Shift Register (LFSR) with m=5 and the flip-flops set to 00111

(FF4=FF3=0, FF2=FF1=FF0=1), show the output of the first 30 bits and determine the length of the period.

Clock = 30

Clk	FF4	FF3	FF2	FF1	FF0
0	0	0	1	1	1
1	1	0	0	1	1
2	1	1	0	0	1
3	0	1	1	0	0
4	0	0	1	1	0
5	1	0	0	1	1
6	1	1	0	0	1
7	0	1	1	0	0
8	0	0	1	1	0
9	1	0	0	1	1
10	1	1	0	0	1
11	0	1	1	0	0
12	0	0	1	1	0
13	1	0	0	1	1
14	1	1	0	0	1

15	0	1	1	0	0
16	0	0	1	1	0
17	1	0	0	1	1
18	1	1	0	0	1
19	0	1	1	0	0
20	0	0	1	1	0
21	1	0	0	1	1
22	1	1	0	0	1
23	0	1	1	0	0
24	0	0	1	1	0
25	1	0	0	1	1
26	1	1	0	0	1
27	0	1	1	0	0
28	0	0	1	1	0
29	1	0	0	1	1
30	1	1	0	0	1

The cycle length is 7 = **011001100**

30 bits = 011001100110011001100110011001

Question 3: [10 points]. Let us consider the f-Function (Fig. 3.8, sec. 3.3.2) used in the DES algorithm.

Suppose input to this function is the 32-bit input expressed in hexadecimal as “D4C3B2A1”, determine the 32-bit output of the function expressed in hexadecimal representation. The 48-bit key to the function is “F0D532A490C6” in hexadecimal

Convert input D4C3B2A1 to binary

D4C3B2A1 = 1101 0100 1100 0011 1011 0010 1010 0001

Expansion of each bit

111010 101001 011000 000111 110110 100101 010100 000011

Convert key F0D532A490C6 to binary

F0D532A490C6 = 1111 0000 1101 0101 0011 0010 1010 0100 1001 0000 1100 0110

Step 3.

Input = 1110 1010 1001 0110 0000 0111 1101 1010 0101 0101 0000 0011

XOR

Output = 1111 0000 1101 0101 0011 0010 1010 0100 1001 0000 1100 0110

= 0001 1010 0100 0011 0011 0101 0111 1110 1100 0101 1100 0101

S1 = 000110 s2=100100 s3=001100 s4=110101 s5=011111 s6=101100 s7=010111
s8=000101

S-box s1 = 0001 S-box s5 = 0110

S-box s2 = 0111 S-box s6 = 1100

S-box s3 = 1111 S-box s7 = 1111

S-box s4 = 1101 S-box s8 = 1110

Permutation table

1 0	2 0	3 0	4 1	5 0	6 1	7 1	8 1
9 1	10 1	11 1	12 1	13 1	14 1	15 0	16 1
17 0	18 1	19 1	20 0	21 1	22 1	23 0	24 0
25 1	26 1	27 1	28 1	29 1	30 1	31 1	32 0

Permutation matrix table

1	1	0	1	1	1	1	0
0	0	0	1	0	1	1	1
0	1	0	1	0	1	0	1
1	1	1	1	1	1	1	1

32-bit output

1101 1110 0001 0111 0101 0101 1111 1111 = **DE1755FF**