CS 463/563: Cryptography for Cybersecurity
Fall 2023
Homework #3
Points: 20

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. [Note: $s_{i+1} = (a*s_i + b) \bmod m$].

s0 = 5
a, b, m = 14, 15, 21

```
random_number_list = []

i = 0
while i < 10:
    s0 = (a * s0 + b) % m
    random_number_list.append(s0)
    i+=1

print(random_number_list)

# [1, 8, 1, 8, 1, 8, 1, 8, 1, 8]
```

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.

(The symbol represents XOR operation).

Period = 6

Work

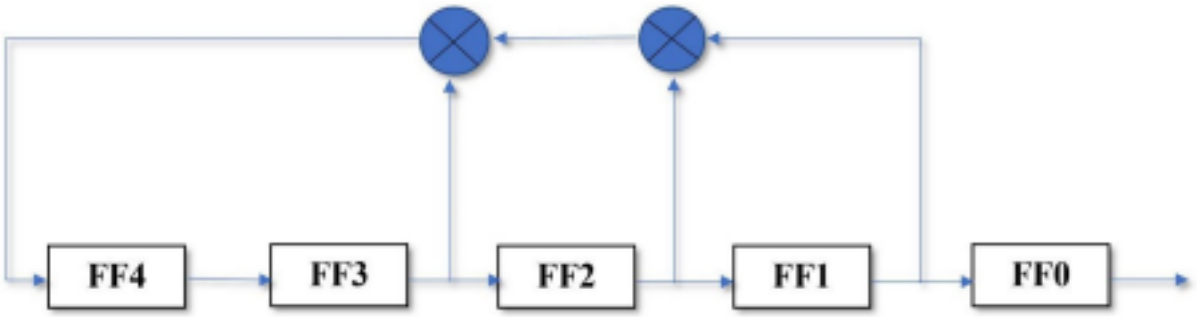
A3=IF(XOR(B2:F2) = TRUE, 1, 0), =B3= A2, etc.

F0	F1	F2	F3	F4
0	**0**	**1**	**1**	**1**
1	0	0	1	1
1	1	0	0	1
1	1	1	0	0
1	1	1	1	0

0	1	1	1	1
0	**0**	**1**	**1**	**1**
1	0	0	1	1
1	1	0	0	1
1	1	1	0	0
1	1	1	1	0
0	1	1	1	1
0	**0**	**1**	**1**	**1**
1	0	0	1	1
1	1	0	0	1
1	1	1	0	0
1	1	1	1	0
0	1	1	1	1
0	**0**	**1**	**1**	**1**
1	0	0	1	1
1	1	0	0	1
1	1	1	0	0
1	1	1	1	0
0	1	1	1	1
0	**0**	**1**	**1**	**1**
1	0	0	1	1
1	1	0	0	1
1	1	1	0	0
1	1	1	1	0
0	1	1	1	1

Hint: *Look for patterns in any of the columns or across the rows. Once a row repeats, everything that follows*

will repeat. Since there are 5 flipflops, you need to do it carefully. You could use Excel's XOR function to save time. In Excel, 0 is represented by FALSE and 1 by TRUE



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.

inputa = "D4C3B2A1"
binary = 11010100110000111011001010100001
Expanded_input = 01101101010011001011001010100001100101011000100 1

48_bit_key_hex = "F0D532A490C6"
48_bit_key_bin = 111100001101010100110010101001001001000011000110

XOR = 100111011001100110000000000001011101100110111111

S1 = 100111 = 0010
S2 = 011001 = 1101
S3 = 100110 = 1000
S4 = 000000 = 1101
S5 = 000001 = 0000
S6 = 011101 = 0101
S7 = 100110 = 1011
S8 = 111111 = 1110

0010 1101 1000 1101 0000 0101 1011 1110

Permutation = 11011001100111000000101111101110

32_bit_output_in_hexadecimal = D99C0BEE

What to submit? Submit a pdf file with your answers via Canvas. Show your work