

CS 463/563: Cryptography for Cybersecurity
Spring 2024
Homework #3
Points: 20

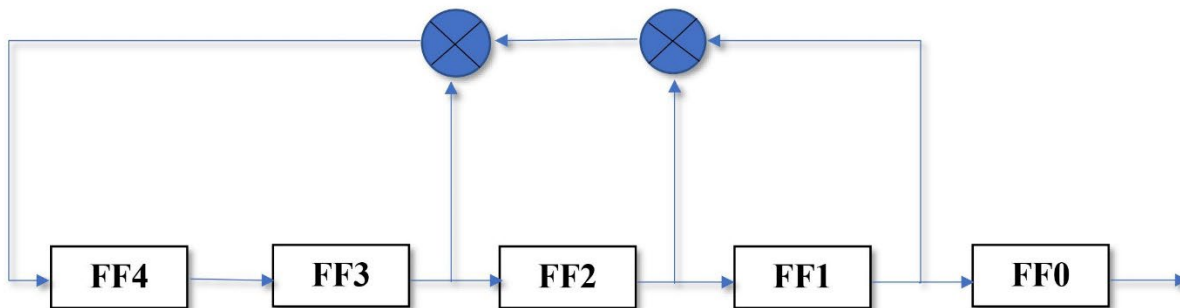
Question 1: [5 points]. Generate ten random numbers (**s1-s10**) using the linear congruently generator (page 35) using the seed (**s₀**) as **5**, and with the three parameters **a**, **b**, and **m** as **14**, **15**, and **21**, respectively.

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

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).

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.

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