Stream Cipher

March 5, 2023

Assignment 2

Name: [Your name]
Student Number: [XXXXXXXXX]

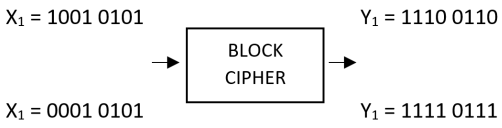
Due date: 15 March 2023, 23:59 (GMT+3:30)
In this assignment, you will answer questions related to Stream Cipher.

- By turning in this assignment, I declare that all of this is my own work.
- This is an individual assignment. Please mention your name and student number in submission. You have to hand in a **SINGLE** document (PDF) with your answers and your source code (if any). **Also, be aware that any form of plagiarism will not be condoned.**
- Your code must be written in C, Java, Python, or Golang, although we encourage you to use Python for simplicity.
- Pose your questions on the Telegram group so that your fellow students can also read them.
- **Explain and motivate all your answers!**

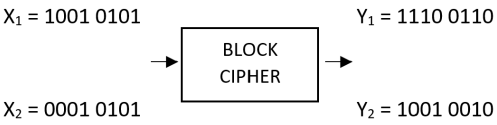
Avalanche effect (10 points)

Explain which of the sequence below, satisfies the avalanche effect. write your reasons.

- Item 1:

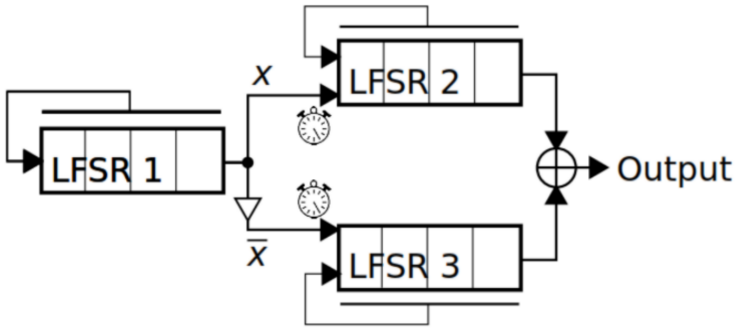


- Item 2:



LFSR, Alternate steps (20 points)

with given assumptions, Write outputs for 4 clocks (0 to 3)



LFSR1 = 1 0 1 0 $F1(x) = X^4 + X^2 + 1$

LFSR2 = 1 1 0 1 $F2(x) = X^4 + X^3 + 1$

LFSR3 = 1 0 0 0 $F3(x) = X^4 + X^3 + X$

Linear Feedback Shift Register (30 points)

Consider two stream ciphers constructed based on three LFSR. for constructing the first stream cipher, 3 LFSR are given to the g1 function, and the function's output, have considered as an output bit of the stream cipher. as the first stream cipher, the second one has been constructed exactly the same but with the use of the g2 function.

- g1 (x0, x1, x2) = x0x1x2 + x0 + x1x2 + x1
- g2 (x0, x1, x2) = x0 + x1x2 + x1

Assume that a user uses one of the above algorithms, but you don't know which one. Provide a method for algorithm recognition by observing the execution key sequence generated by the user.

Linear Feedback Shift Register (20 points)

We will now analyze a pseudorandom number sequence generated by an LFSR characterized by (c2=1,c1=0,c0=1)

- What is the sequence generated from the initialization vector (s2=1,s1=0,s0=0) ?
- What is the sequence generated from the initialization vector (s2=0,s1=1,s0=1) ?
- How are the two sequences related?

Golomb sequence (20 points)

Check the Golomb triple criterion for the sequence below.

- 101001101001111101