Lab 05 - Stream Ciphers and Linear Feedback Shift Registers

Part 01

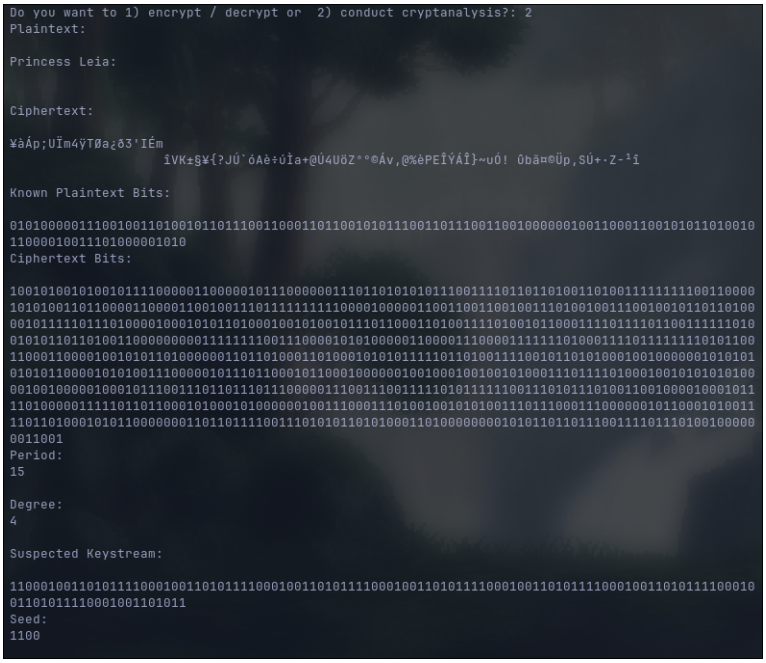
1. Encrypted message from part01_plainText.txt by using a 4-bit LFSR with the seed "1001" with the first and last bit XORd with each other.
   (10 points)

```
Do you want to 1) encrypt / decrypt or  2) conduct cryptanalysis?: 1
Enter starting values: 1001
Plaintext Bits:

01010111011010000111100100100000011001000110100101100100001000000100010101110000001101001011100110
11011110110010001100101011100110010000000110100001011000010000000011010100101100001000000110000101
10111001100100001000000011011000100000011000110110111101101101011001010010000000110111101110101011
10100001000000110001001100101011001100110111101110010011001010010000000110001001011000010000000011
00100010110000100000011000010110111001100100001000000011001100111111001000000010000100110010101100
01101100001011101010111001101100101001000000110100101101110001000000110001101101000011000010111100
10011001110110010100100000011011110110011000100000011001000110100101110010011001010110001101111010
00110100101101110011001110010110000010000000101100101101111011001000110000100100000011101110110000 1
0111001100101110
Keystream Bits:

10010001111010110010001111010110010001111010110010001111010110010001111010110010001111010110011001000
11110101100100011110101100100011110101100100011110101100100011110101100100011110101100100011110 10
11001000111101011001000111101011001000111101011001000111101011001000111101011001000111101011001 00
01111010110010001111010110010001111010110010001111010110010001111010110010001111010110010001111 01
01100100011110101100100011110101100100011110101100100011110101100100011110101100100011110101100 10
00111101011001000111101011001000111101011001000111101011001000111101011001000111101011001000111 10
10110010001111010110010001111010110010001111010110010001111010110010001111010110010001111010110 01
00011110101100100011110101100100011110101100100011110101100100011110101100100011110101100100011 11
0101100100011110
Ciphertext Bits:

11000110100000011010110101111011000100011110001011110101101111001010110111100001001010100000101110
00101011010110010010000111000101100101100010111111110100110011110011001101000110111100101111111 1
01110001011001010001000100110011101000100101101111111010000110010001101111011000101000110110011 11
11011011110010111110011010111010110110000101100001000101011011101010110100000110001110000000111 10
01000110101110001100111011100011011101111010100100100000111001011011010110101000101010010000011 10
01010001010010101101010010100100010100011001110011000110111001111101101000101010101000001010000 10
00101011111001000010110001100001000100010111110110001000111100010111111101001111000111110111000 11
00101010000000101000011101111001001101010111001000100001000100011110110111011001111101101111101 10
0010101000110000

Decrypted Ciphertext Bits:

01010111011010000111100100100000011001000110100101100100001000000100010101110000001101001011100110
11011110110010001100101011100110010000000110100001011000010000000011010100101100001000000110000101
10111001100100001000000011011000100000011000110110111101101101011001010010000000110111101110101011
10100001000000110001001100101011001100110111101110010011001010010000000110001001011000010000000011
00100010110000100000011000010110111001100100001000000011001100111111001000000010000100110010101100
01101100001011101010111001101100101001000000110100101101110001000000110001101101000011000010111100
10011001110110010100100000011011110110011000100000011001000110100101110010011001010110001101111010
00110100101101110011001110010110000010000000101100101101111011001000110000100100000011101110110000 1
0111001100101110

ASCII Text:

Why did Episodes 4, 5, and 6 come out before 1, 2, and 3? Because in charge of directing, Yoda wa
s.
```

-

Part 02

1. XOR the known plaintext with the first X bits of the ciphertext, where X is the number of bits in the known plaintext
   (5 points)
   -



2. Calculate the period by showing the number of bits that are repeated in the keystream
   (5 points)
   - period = 15 (110001001101011)

3. Calculate the degree (Show your work step by step)
   (5 points)
   - period = 15 (110001001101011) repeating
   - degree = log_2(15 + 1) = 4

4. Calculate the seed by pasting your keystream into a spreadsheet and tracing it back to the initial starting values
   (10 points)
   - seed = 1100

   # 0 0 (1 1) -> 0
   # 0 0 0 1 -> 1
   # 1 0 0 0 -> 0
   # 0 1 0 0 0
   # 0 0 1 0 1
   # 1 0 0 1 1
   # 1 1 0 0 0
   # 0 1 1 0 1
   # 1 0 1 1 0
   # 0 1 0 1 1
   # 1 0 1 0 1
   # 1 1 0 1 1

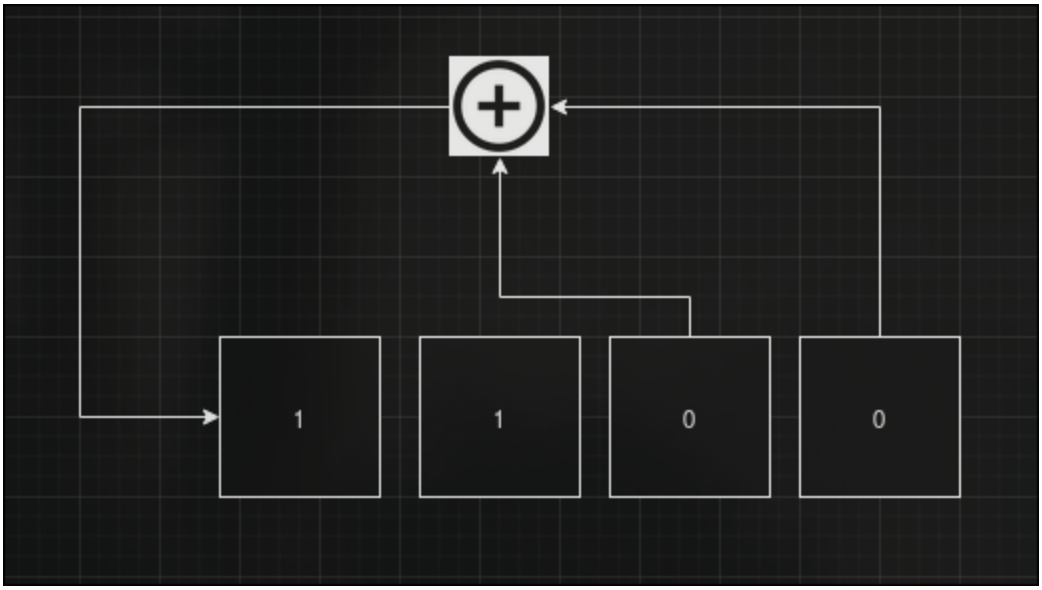
```
#     1   1   0      1
#         1   1      0
#             1      0

# seed = 1100
```

5. Use the spreadsheet from step 4 to find the LFSR configuration and show your work for each step.
   (10 points)

```
# Base
# 0   0   1   1
# 0   0   0   1
# 1   0   0   0
# 0   1   0   0


#         1   1
# 0
#
#

#
#         0   1
# 1
#

#
#
#         0   0
# 0
```

   And so on

6. Draw a diagram of the LFSR configuration you identified in step 5
   (10 points)

- 

7. Translate the plaintext into ASCII
   (15 points)
   - Princess Leia:
     Why, you stuck up, half-witted, scruffy-looking nerf-herder.

     Han Solo:
     Who's scruffy-looking?

8. Upload your code to canvas as "Lab5_part01_02.py". A TA will run your program and make sure it can decrypt the ciphertext. Double check that it runs without any issues before uploading it. Be sure to have both lines in the cycle() to demonstrate the part01 bits and the part02 bits.
   (30 points)