

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:

0101011101101000011100100100000110010001101001011001000010000001000101011100000110100101100110
1101111011001000110010101110011001000000110100001011000010000001101010010110000100000010000101
101110011001000010000000110110001000000110001101101110110110110010100100000011011101110101011
1010000100000011000100110010101100110011011101100100110010100100000011000100110000100000011
0010001011000010000001100001011011100110010000100000011001100111110010000010000100110010101100
0110110000101110101011001101100101001000001101001011011100010000011000110110100001100001011100
100110011101100100100000011011101100110001000000110010001101001011100100110010101100011011010
0010100010110110011001110010110000100000011010010110111011001000110000100100000011101101100001
0111001100101110
Keystream Bits:

1001000111101011001000111101011001000111101011001000111101011001000111101011001000111101011001000
1111010110010001111010110010001111010110010001111010110010001111010110010001111010110010001111010
1100100011110101100100011110101100100011110101100100011110101100100011110101100100011110101100100
0111101011001000111101011001000111101011001000111101011001000111101011001000111101011001000111101
0110010001111010110010001111010110010001111010110010001111010110010001111010110010001111010110010
0011110101100100011110101100100011110101100100011110101100100011110101100100011110101100100011110
1011001000111101011001000111101011001000111101011001000111101011001000111101011001000111101011001
0001111010110010001111010110010001111010110010001111010110010001111010110010001111010110010001111
0101100100011110
Ciphertext Bits:

1100011010000011010110101111011000100011110001011110101101111001010110111100001001010100000101110
0010101101011001001000011100010110010110001011111111010011001111001100101000110111110010111111111
011100010110010100010001001100111010001001011011111101000011001000110111101100010100011011001111
11011011110010111100110101110101100001011000010001010110110101011010000011000111000000111110
01000110101110001100111011100011011101110101001001000001100101101101010101000101001000011110
010100010100101011010100100010001000110011100110001101110111101101000101010100000101000010
00101011111001000010110001100001000100010111110110001000111100010111111010011110001111011100011
00101010000001010000110111100100110101110010001000100010001111011011101100111110101111011101110
0010101000110000

Decrypted Ciphertext Bits:

010101110110100001111001001000001100100011010010110010000100000010001010111000001101001011100110
1101111011001000110010101110011001000000110100001011000010000001101010010110000100000010000101
1011100110010000100000001101100010000001100011011011101101101100101001000000110111101110101011
1010000100000011000100110010101100110011011101100100110010100100000011000100110000100000011
001000101100001000000110000101101110011001000010000001100110011111001000001000100110010101100
0110110000101110101011001101100100100000011010010110111000100000011000110110100001100001011100
10011001110110010010000001101111011001100010000001100100011010010111001001100101011000110111010
00110100010110111001100111001011000010000001100101101111011001000110000100100000011101101100001
0111001100101110

ASCII Text:

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

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)

```
Do you want to 1) encrypt / decrypt or 2) conduct cryptanalysis?: 2
Plaintext:

Princess Leia:

Ciphertext:

Y&A&p;UIm4yT0az03'IEm
IVKz$W{?JU'0A&+0ia+@U4U0Z'*@Av,@%PEiYAi}~u0! 0ba=0Up,SU+-Z-1i

Known Plaintext Bits:

01010000011001001101001011011001100011011001010111001101100110010000001001100011001010110010
11000010011101000001010
Ciphertext Bits:

10010100101001011110000011000001011100000011011010101011100111101101101001101001111111100110000
10101001101100001100001100100111011111111000010000011001100110010011101001001110010010110110100
001011110111010000100010101101000100101011101100011010011101001110111011001111110101111010
01010110110100110000000001111111001110000101010000011000011100001111110100011101111110101100
11000110000100101011010000001101101000110100010101111011010011100101101010001001000001010101
01010110000101010011100000101110100011000100000010010001001000110111101000100101010100
00100100000100010110011101101110111000001100111001111010111110011101011010011001000010001011
110100000111101101100010100010100000010011000111010010010101011101100011100000010110001010011
11011010001010110000000110110111001110101101010001101000000010101101110011110111010010000
0011001
Period:
15
Degree:
4
Suspected Keystream:

1100010011010111000100110101110001001101011100010011010111000100110101110001001101011100010
01101011110001001101011
Seed:
1100
```

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
```

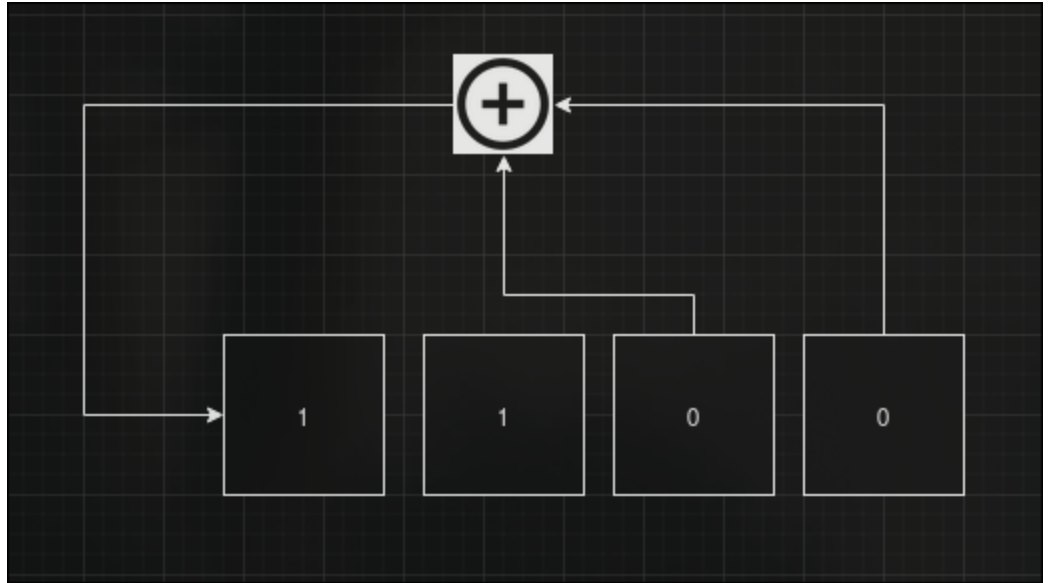
```
#   1 1
# 0
#
#
```

```
#
#   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)