

I utilized the scripts shown below to accomplish both tasks. The associated text outputs are attached as well.

Shrinking Generator

```
1 def lfsr(state, taps):
2     """
3     state - current state, initialized to IV
4     taps - tap indices
5
6     """
7     sum = 0
8     for tap in taps:
9         sum += int(state[tap]) # Sum taps
10    if sum % 2 == 0.0:
11        sum = 0
12    else:
13        sum = 1
14
15    # Final register contains output bit:
16    output = state[-1]
17
18    # Move sum to first register, shift all others over
19    state = str(sum) + state[:-1]
20
21    return output, state
22
23
24 def main():
25     # Define variables, and define IV/taps for each LFSR:
26     outputs_A = []
27     states_A, states_S = [], []
28     IV_A = '010101'
29     IV_S = '11100'
30
31     # Taps are indexed from left to right:
32     taps_A = (0, 5)
33     taps_S = (1, 4)
34
35     # Clock both LFSRs from their IV:
36     outBit_A, stateOut = lfsr(IV_A, taps_A)
37     states_A.append(stateOut)
38
39     outBit_S, stateOut = lfsr(IV_S, taps_S)
40     states_S.append(stateOut)
41
42     # Check if first bit is counted:
43     if outBit_S == '1':
44         outputs_A.append(outBit_A)
45
46     while len(outputs_A) < 100:
47         # Run S-LFSR:
48         outBit_S, stateOut_S = lfsr(states_S[-1], taps_S)
49         states_S.append(stateOut_S)
50
51         # Run A-LFSR
52         outBit_A, stateOut_A = lfsr(states_A[-1], taps_A)
```

Air Force Institute of Technology
Department of Electrical and Computer Engineering
Cryptography and Data Security (CSCE-544) Midterm Exam

April 29, 2019

Name: Micah Hayden

Page 2 of 4

```
states_A.append(stateOut_A)

53
    if outBit_S == '1':
55        outputs_A.append( outBit_A )

57
# Output vector to file:
59 outFile = open("ShrinkingGen_Output.txt", "w")
outFile.write("[" + ", ".join( outputs_A ) + "]" )
61 outFile.close()

63
if __name__ == "__main__":
65     main()
```

ShrinkingGenerator.py

```
1 [1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0,
    0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0,
    1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0,
    1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1]
```

ShrinkingGen_Output.txt

Feistel Network

The below python script was utilized to perform the Feistel network function.

```
1 def getLeft( input ):
2     """
3     Left input is the lower order nibble of the input byte:
4     """
5     return input & 15
6
7
8 def getRight( input ):
9     """
10    Right input is the upper order nibble of the input byte:
11    """
12    # Right shift by 4 will return desired bits by removing the lower order bits
13    return input >> 4
14
15
16 def buildByte(right , left):
17     """
18     This function multiplies the right by 16 to return it to its higher order position
19     """
20     right = right * 16
21     return right + left
22
23
24 def Feistel(inByte):
25     """
26     inByte - input data
27     outByte - taken from the final round; left/right outputs are the would-be left/
28     right inputs to the next round.
29     """
30     # S Boxes for each round:
31     S = [ [5, 2, 15, 10, 6, 13, 7, 4, 14, 0, 1, 3, 12, 8, 9, 11], \
32           [15, 5, 13, 11, 0, 12, 4, 8, 14, 10, 9, 2, 6, 1, 7, 3], \
33           [7, 1, 2, 12, 0, 5, 9, 8, 14, 13, 15, 4, 10, 11, 3, 6] ]
34
35     # Round Keys:
36     keys = [15, 5, 9]
37
38     # Pull nibbles from input byte:
39     left , right = getLeft(inByte), getRight(inByte)
40
41     for round in range(3):
42         # xor right and round key:
43         fOut = keys[round] ^ right
44
45         # substitute the output of the fOut with the round's S-Box
46         sOut = S[round][fOut]
47
48         # Set next round's inputs:
49         rightOut = left ^ sOut
50         leftOut = right
51
52         # Reset inputs to next state:
53         left = leftOut
54         right = rightOut
```

Air Force Institute of Technology
Department of Electrical and Computer Engineering
Cryptography and Data Security (CSCE-544) Midterm Exam

April 29, 2019

Name: Micah Hayden

Page 4 of 4

```
53     right = rightOut
55
56 # Build output:
57 outByte = buildByte(right, left)
58 return outByte
59
60 def main():
61     # print( lfsr('100100', (5, 0), 128) )
62     bytes = [0xFA, 0xB1, 0x39, 0x45]
63     outputs = []
64     for byte in bytes:
65         outputs.append( hex( Feistel( byte ) ) )
66
67 # Print outputs:
68 print(outputs)
69
70 # Write outputs to file keeping array syntax:
71 outFile = open("FeistelOut.txt", "w")
72 outFile.write("[" + ",".join(outputs) + "]")
73 outFile.close()
74
75 print("Done!")
76
77 """ Function testing:
78 # Used to test getLeft, getRight, and buildByte
79 for byte in bytes:
80     left = getLeft(byte)
81     right = getRight(byte)
82     print( "Left: " + str( getLeft(byte) ) )
83     print( "Right: " + str( getRight(byte) ) )
84     print( "Original: " + hex( buildByte(right, left) ) )
85 """
86
87 if __name__ == "__main__":
88     main()
```

Feistel.py

```
1 [0x96, 0x16, 0xc, 0xff]
```

FeistelOut.txt