Air Force Institute of Technology
Department of Electrical and Computer Engineering
Data Security(CSCE 544)
Homework #3
Due Date: 22-April-2019

You are able to place a probe at the output of a Linear Feedback Shift Register (LFSR) and observe the first 128 bits output.

Table 1: Input Table Format

	Bit							
Byte	1	2	3	4	5	6	7	8
0x0	0	1	0	0	1	1	1	0
0x1	0	0	1	0	1	1	1	1
0x2	0	0	1	0	1	0	0	0
0x3	1	1	0	0	0	0	1	0
0x4	0	0	0	0	1	1	1	1
0x5	1	1	0	1	0	1	0	1
0x6	1	0	0	1	1	0	1	1
0x7	1	0	1	1	0	1	0	0
0x8	1	0	0	1	1	1	0	0
0x9	0	1	0	1	1	1	1	0
0xA	0	1	0	1	0	0	0	1
0xB	1	0	0	0	0	1	0	0
0xC	0	0	0	1	1	1	1	1
0xD	1	0	1	0	1	0	1	1
0xE	0	0	1	1	0	1	1	1
0xF	0	1	1	0	1	0	0	1

Table 2: 128 Bits Output Vector Format

```
0 1 0 0 1 1 1 0 0 0 1 0 1 1 1 1 0 0 1 0 1 0 0 0 1 1 0 0 0 0 1 0 0 0 0 0 1 1 1 1 1 1 0 1 0 1 0 1
1 0 0 1 1 0 1 1 1 0 1 1 0 1 0 0 1 0 0 1 1 1 0 0 0 1 0 1 1 1 1 0 0 1 0 1 0 0 0 1 1 0 0 0 0 1 0 0
0 0 0 1 1 1 1 1 1 0 1 0 1 0 1 1 0 0 1 1 0 1 1 1 0 1 1 0 1 0 0 1
```

Encrypt the plaintext "*Hope this Helps!*" by XORing the output of the LFSR and the plaintext. Assume 8-bits ASCII encoding for the plaintext.

The output is shown below, in Hex:

```
06 40 58 a7 2f a1 f3 dd ef 7e 19 e1 73 db 44 48
```

Explain the differences between the two different types of LFSR implementation: internal feedback, external feedback.

An internal feedback implementation keeps the XOR gates between flip flops in the LFSR. Thus, the following input is the previous output.
An external feedback LFSR sends all of the XOR outputs back to the input bit of the LFSR. Thus, the input for the next stage is not always the previous output.

Determine the LFSR's output for the next two bytes.

The next two bytes are shown below, which is simply a continuation of the repeating sequence.

```
0 0 1 1 1 0 0 0
1 0 1 1 1 1 0 0
```

Determine the LFSR's degree of polynomial and initial value.

Based on the knowledge that the polynomial is a maximum length sequence, I know it is a 6-bit LFSR because the sequence repeated after 63 bits.

$$\begin{aligned}\text{Length } &= 2^m - 1\\ 63 &= 2^m - 1\\ 64 &= 2^m\\ m &= 6\end{aligned}$$

The initial value is shown below, and was determined by working backwards with the given output sequence. This is based on the assumption that the output is taken after clocking.

```
1 0 0 1 0 0
```

Determine the LFSR's characteristics polynomial.

The characteristic polynomial $P(x)$ is shown below:

$$P(x) = x^6 + x^5 + 1 \tag{1}$$