

Homework #3

Due date: 07 November 2018

Notes:

- Computer programs and other soft material must be submitted through sucourse.
- Winzip your programs and add a readme.txt document to explain the programs and how to use them.
- Name your winzip file as “cs411_507_hw03_yourname.zip”

1. **(20 pts)** Consider an LFSR with connection polynomial $p(x) = 1+x^5+x^6$. What is the period of the LFSR bit stream when the initial state is $[1, 0, 0, 0, 0, 0]$. Print the first period of the sequence. Is this polynomial primitive?

(Hint: You can use LFSR() and FindPeriod(s) functions in the attached Python file)

2. (20 pts) Consider the following binary sequence:

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

Find the shortest LFSR that generates it using the Berlekamp-Massey algorithm.

(Hint: You can use BM() function in the attached Python file)

3. **(40 pts)** Consider the following ciphertext bit stream encrypted using a stream cipher. And you strongly suspect that an LFRS is used to generate the key stream:

[1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0,
0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0,
1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0,
1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0,
1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1,
1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1,
1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0,
1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0,
1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0,
1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0,
0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1,
0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1,
0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0,
1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0,
0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0,
1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1,
1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0,

0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1,
1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0]

Also, encrypted in the ciphertext you also know that there is a message to you from the instructor; and therefore the message starts with “Dear Student”. Find the plaintext. For this you need to find the connection polynomial of the LFSR first. Note that the ASCII encoding (seven bits for each ASCII character) is used.

(Hint: You can use `ASCII2bin()` and `bin2ASCII(RecPText)` functions (in the attached Python file) to make conversion between ASCII and binary)

4. **(10 pts)** Consider $GF(2^8)$ used in AES with the irreducible polynomial $p(x) = x^8 + x^4 + x^3 + x + 1$.
 - a. Perform the following multiplication in $GF(2^8)$:

$$(x^7 + x^6 + x^4 + x^2) \times (x^7 + x^3 + x^2 + x + 1) = ?$$
 - b. Show that the inverse of $(x^7 + x^6 + x^4 + x^2)$ in $GF(2^8)$ is $(x^7 + x^6 + x^2 + 1)$.
5. **(10 pts)** Consider a modified AES without ShiftRow and Mixcolumn layers. How hard is it to attack it? If you use “chosen plaintext attack” which plaintexts would you choose?