Homework #3

Due date: 05 November 2015
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. (**10 pts**) Consider an LFSR with connection polynomial $p(x) = 1+x^2+x^3+x^5+x^6$. Show that p(x) is a primitive polynomial by demonstrating that the LFSR, whose connection polynomial is p(x), generates maximum length sequences (i.e., sequences with the maximum period 2^6-1).

The LFSR generates the following sequence with the period 63 if we start with the initial state 000001:

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

2. (**20 pts**) Consider the following binary sequence:
[1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0]

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

The length of the LFSR is 9
Its connection polynomial is $1 + x^3 + x^5 + x^6 + x^7 + x^8 + x^9$.

3. (**30 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:

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

Also, encrypted in the ciphertext you also know that there is a message to you from the instructor; and therefore the message ends with "Your Instructor". Find the plaintext and the connection polynomial of the LFSR. Note that the ASCII encoding (seven bits for each ASCII character) is used.

Hint: You can use the following Python function to convert a message in ASCII to binary:

```
def ASCII2bin(message):
    m_i = []
    mlen = len(msg)
    for i in range(0,mlen):
        ascii_no = ord(msg[i])
        print ascii_no
        ascii_bin = bin(ascii_no)
        print ascii_bin
        char_len = len(ascii_bin)
        if(char_len<9):
            for j in range(0,9-char_len):
                m_i.append(0)
        for j in range(2,char_len):
            m_i.append(int(ascii_bin[j]))
    return m_i
```

The connection polynomial: $x^{11} + x^8 + x^5 + x^2 + 1$.

Dear Student,

You just earned 30 points. Congratulations!

Your Instructor

4. (**20 pts**) Consider the combining function given in the following table, that is used to combine the outputs of four maximum-length LFSR sequences:

$F(x_1, x_2, x_3, x_4) = x_1 \oplus x_2 \oplus x_1x_3 \oplus x_1x_2x_4$.

   a. The lengths of LFSRs are 89, 97, 101, and 103, respectively. Compute the linear complexity and the period of the output sequence. (**10 pts**)

The linear complexity is
$89 + 97 + 89\times101 + 89\times97\times103 = 898374$
The period
$(2^{89}-1) + (2^{97}-1) + (2^{89}-1)\times(2^{101}-1) + (2^{89}-1)\times(2^{97}-1)\times(2^{103}-1)$.

   b. Is the function F nonlinear, balanced and correlation-free? Is this a good combining function? Explain your answer. (**10 pts**)

The function is nonlinear. (1 pts)

The truth table of F is as follows:

x_1	x_2	x_3	x_4	F
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	1
0	1	0	1	1
0	1	1	0	1
0	1	1	1	1
1	0	0	0	1
1	0	0	1	1
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	1
1	1	1	0	1
1	1	1	1	0

The function is balanced (4 pts).
But the output is correlated to x_1 and x_3
(F is correlated to x_3'). (6 pts)

5. (**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):

   $(x^7+ x^4+x^3+x^2+1) \times (x^7+x^5+ x^2+x) = ?$

   $x^7 + x^6 + x^4 + x^3 + x^2 + 1$

   b. Show that the inverse of $(x^7+ x^4+x^3+x^2+1)$ in GF(2^8) is $(x^7+ x^6+x^4+x^3+x^2)$.

   $(x^7+ x^4+x^3+x^2+1) \times (x^7+ x^6+x^4+x^3+x^2) \mod x^8+x^4+x^3+x+1 = 1.$

6. (**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?

In AES without ShiftRow and Mixcolumn layers, one byte in the plaintext affects only the corresponding byte in the ciphertext. Therefore, the encryption becomes 16 substitution ciphers where the block size is only 8. Then, in chosen plaintext attack the following plaintexts can be chosen:

$P_0 = [0, 0, \ldots, 0]$, $P_1 = [1, 1, \ldots, 1\}$, …, $P_{255} = [255, 255, \ldots, 255]$