Homework #3

Due date: 25 November 2020, by 11:59 pm.

Notes:

- For Question 1, you can use a Python module for arithmetic in GF(2^8).
- For Question 2, you can use "**lfsrf.py**" provided to you earlier.
- You are expected to submit your answer document as well as two Python codes for Questions 1 and 2, respectively.
- Zip your programs and add a readme.txt document (if necessary) to explain the programs and how to use them.
- Name your winzip file as "cs411_507_hw03_yourname.zip"

1. (**20 pts**) Consider GF(2^8) used in AES with the irreducible polynomial $p(x) = x^8+x^4+x^3+x+1$. You are expected to query the server "cryptlygos.pythonanywhere.com/poly/<*your_id*>", which will send you two binary polynomials a(x) and b(x) in GF(2^8). Polynomials are expressed as bit strings of their coefficients. For example, p(x) is expressed as '100011011'. You can use the Python code "**Q1_student.py**" given in the assignment package to communicate with the server.

a. (**10 pts**) You are expected to perform $c(x) = a(x)\times b(x)$ in GF(2^8) and return c(x) as bit string.

b. (**10 pts**) You are expected to compute the multiplicative inverse of a(x) in GF(2^8) and return $a^{-1}(x)$.

2. (**30 pts**) Consider the Geffe generator of three LFRSs ($LFSR_1$, $LFSR_2$, and $LFSR_3$) with the following connection polynomials:

$C_1(x) = x^{14} + x^5 + 1$
$C_2(x) = x^{17} + x^3 + 1$
$C_3(x) = x^{11}+ x^2 + 1$

You also observed the following output sequence of the Geffe generator:

z = [0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1]

Can you find the initial states of $LFSR_1$, $LFSR_2$, and $LFSR_3$?

3. (**20 pts**) Consider the combining function given in the following table, that is used to combine the outputs of three **maximum-length** LFSR sequences:

$F(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3$.

a. (**5 pts**) The lengths of LFSRs are 79, 85, and 97, respectively. Compute the linear complexity and the period of the output sequence.

b. (**15 pts**) Analyze the function F in terms of three criteria:
   - Nonlinearity degree
   - Balance
   - Correlation

   Is this a good combining function? Explain your answer.

4. (**20 pts**) Consider a modified AES without ShiftRow and Mixcolumn layers, where the secret key length is 128-bit. Show that with moderate effort you can break it.

5. (**10 pts**) The cipher block chaining (CBC) mode has the property that it recovers from the errors (corruption, deletion, and insertion) in ciphertext blocks. Its encryption schemes are given as follows

Encryption primitive: $C_i = E_K(P_i \oplus C_{i-1})$
Decryption primitive: $P_i = D_K(C_i) \oplus C_{i-1}$

How many blocks decrypt incorrectly if the ciphertext block C_i is corrupted during transmission? Show which plaintext blocks are corrupted.

Exercise for Rainbow Tables (Non-credit question)

Consider ten digests in the attached file “**rainbow_table.py**”, each of which is the hash of a six-character password. Your mission is to find those passwords using the rainbow table given in the attached file “**rainbowtable.txt**”. Complete and submit the Python code in the file “**rainbow_table.py**” such that it finds and prints out the ten passwords corresponding to the digests.