**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(28).
* 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(28) used in AES with the irreducible polynomial p(x) = x8+x4+x3+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(28). 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.
   1. (**10 pts**) You are expected to perform c(x) = a(x)×b(x) in GF(28) and return c(x) as bit string.

Answers on py file

* 1. (**10 pts**) You are expected to compute the multiplicative inverse of a(x) in GF(28) and return a-1(x).

Answers on py file

1. (**30 pts**) Consider the Geffe generator of three LFRSs (LFSR1, LFSR2, and LFSR3) with the following connection polynomials:

C1(x) = x14 + x5 + 1

C2(x) = x17 + x3 + 1

C3(x) = x11+ x2 + 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 LFSR1, LFSR2, and LFSR3?

1. (**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(x1, x2, x3) = x1x2 ⊕x1x3 ⊕ x2x3 ⊕ x1x2x3.

* 1. (**5 pts**) The lengths of LFSRs are 79, 85, and 97, respectively. Compute the linear complexity and the period of the output sequence.

Linear Complexity = (79x85) + (79x97) + (85x97) + (79x85x97)

Time Period = (279 -1)x(285 -1) + (279 -1)x(297 -1) + (285 -1)x(297 -1) + (279 -1)x(285 -1)x(297 -1)

* 1. (**15 pts**) Analyze the function F in terms of three criteria:
* Nonlinearity degree
* Balance
* Correlation

Is this a good combining function? Explain your answer.

Truth Table:

x1 x2 x3 F

0 0 0 0

0 0 1 0

0 1 0 0

0 1 1 1

1 0 0 0

1 0 1 1

1 1 0 1

1 1 1 0

Non-linearity degree:

Non-Balanced

Correlation 5/8

1. (**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.

AES for 128-bit key length consists of 10 rounds of processing. Since we don’t have ShiftRow and Mixcolumn layers we will only undergo one single-byte substitution and the addition of round key. Since, the decryption process for AES in the reverse on the encryption process we can XOR the block with round key and then do inverse byte substitution (all rounds use the same substitution box) in order to decrypt and obtain the plain text.

1. (**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: Ci = EK(Pi ⊕ Ci-1)

Decryption primitive: Pi = DK(Ci) ⊕ Ci-1

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

If one cipher text block is corrupted during the transmission only two blocks will be affected during the decryption. If Ci is corrupted, then in decryption block Pi and Pi+1 are corrupted and will be decrypted wrong. Since Pi+2 and onwards don’t depend on Ci they will be decrypted correctly.

**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.