CS 4920/5920 Applied Cryptography Spring 2020
HW 3

This HW assignment is due at the beginning of class on 3/31. Please explain how you reached your answers.

Problem 1.

a. Develop a set of tables similar to *Table 5.1* in the textbook for GF(5).
b. Determine if the follow are reducible over GF(2), i.e., coefficients mod 2.
   i) $x^3 + 1$
   ii) $x^3 + x^2 + 1$
   iii) $x^4 + 1$

Problem 2.

a. Develop a set of tables similar to Table 5.3 for GF(4) with $m(x) = x^2 + x + 1$.
b. Develop a table similar to *Table 5.5* in the textbook for GF(2^4) with $m(x) = x^4 + x + 1$.

Problem 3.

a. Investigate Simplified AES (S-AES) based on GF(2^4). What is the block length and the structure of the state array? Express them in bits.
b. What is the modulus/prime polynomial used for the GF(2^4) operations in S-AES?
c. Show that the matrix given in the following, with entries in GF(2^4), is the inverse of the matrix used in the MixColumns step of S-AES.

$$\begin{pmatrix} x^3+1 & x \\ x & x^3+1 \end{pmatrix}$$

Problem 4.

Let's implement AES using a computer.

a. Identify the programming language and the software program you use for this problem. Upload your codes on cloud, e.g., OneDrive, so that they are publicly accessible and include the link to the codes for this problem.
b. Attach a part of your code/implementation that corresponds to the MixColumns computation in printed copy. Include comments and describe the variables/functions (for example, the MixColumns matrix [02 03 01 01; 01 02 03 01; …] that you defined).
c. Perform Key Expansion using the Key {0f1571c947d9e8591cb7add6af7f6798} and construct a table like Table 6.3 in the textbook. Have the table the same structure/format as Table 6.3 and include the entry values. Only the table outcome is needed for this part.
d. Perform AES on Plaintext {0123456789abcdeffedcba9876543210} using the key in the previous part and construct a table like Table 6.4. Have the table the same structure/format as Table 6.4 and include the entry values.

Problem 5.

Let's study the Avalanche Effect in AES. This problem builds on the previous problem.

a. Explain the Avalanche Effect and why it is an attractive feature.
b. Given the Plaintext *P*= {8123456789abcdeffedcba9876543210} as the baseline, generate three more plaintexts which are different from *P* by one bit and perform AES on them using the key {0f1571c947d9e8591cb7add6af7f6798}. To compare each of the new plaintexts and *P*, construct three tables which are like Table 6.5 in the textbook. Have the table the same structure/format as Table 6.5 and include the entry values. (If you have not used your own implementation from the previous problem, identify what you used for this problem.)