1172/DCP1323 Introduction to Cryptography, Spring 2019 **Due: 2019/4/1 (Mon.)**

Homework 3

Instructor: Prof. Wen-Guey Tseng Scribe: Hung-Yu Chiu

Part 1: Written Problems

1. For polynomial arithmetic with coefficients in Z_{11} , perform the following calculations.
   a. $(x^2 + 2x + 9)(x^3 + 11x^2 + x + 7)$
   b. $(8x^2 + 3x + 2)(5x^2 + 6)$

2. Determine which of the following polynomials are reducible over GF(2).
   a. $x^2 + 1$
   b. $x^2 + x + 1$
   c. $x^4 + x + 1$

3. Determine the gcd of the following pairs of polynomials.
   $(x^4 + 8x^3 + 7x + 8)$ and $(2x^3 + 9x^2 + 10x + 1)$ over GF(11)

4. Develop a set of tables similar to Table 5.3 for GF(3) with $m(x) = x^2 + x + 1$.

5. In the discussion of MixColumns and InvMixColumns, it was stated that $b(x) = a^{-1}(x) \bmod (x^4 + 1)$, where $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$ and $b(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E.\}$ Show that this is true.

6. Given the plaintext {0F0E 0D0C 0B0A 0908 0706 0504 0302 0100} and the key {0202 0202 0202 0202 0202 0202 0202 0202}:

   a. Show the original contents of **State**, displayed as a 4 × 4 matrix.
   b. Show the value of **State** after initial AddRoundKey.
   c. Show the value of **State** after SubBytes.
   d. Show the value of **State** after ShiftRows.
   e. Show the value of **State** after MixColumns.

Part 2: Programming Problem

This programming problem is to use an AES library to encode messages in various modes and padding methods. The purpose is to get familiar with the parameter setting and function calls. You can use either OpenSSL or Crypto++. Please find the related library information and examples on the Internet.

I. Encrypt the message (in ASCII)

```
AES is efficient in both software and hardware.
```

by the key "1234567890123456" (ASCII) and the following specifications.

Mode	Initial Vector (IV)	Output format	Padding method (see Wiki Padding for details)
ECB		Hex	Zeros Padding
ECB		Hex	PKCS#7
CBC	0000 0000 0000 0000 (ASCII)	Hex	Zeros Padding
CBC	0000 0000 0000 0000 (ASCII)	Hex	PKCS#7

II. Test data: Plaintext = "Hello World!" by the above specification.

A. ECB, Zeros Padding → 2e98 68aa 6eae 7218 4b4a 8881 f3df b26b

B. ECB, PKCS Padding → 6f36 4e3f 45c8 7893 0e1d 88be 8458 3a32

C. CBC, Zeros Padding → ddc1 94e6 d0f1 85ae 03a0 4dd4 1504 35b4

D. CBC, PKCS Padding → 8fed aeca 2fe9 fa8a 9f35 0468 0258 e80c

III. Submission: you need to upload two files

A. ase-modes.cpp or aes-modes.c: the program of generating the answers.

B. Out.txt: 4 ciphertexts separated by empty lines.

IV. On-site test: Will announce the venue and schedule later. The problem is to use your programs to decrypt some ciphertexts on the spot.