Introduction to Cryptography, Spring 2021 **Due: 4/13/2021 (Tue.)**

Homework 3

Instructor: Prof. Wen-Guey Tseng

Part 1: Written Problems

1. For polynomial arithmetic with coefficients in Z_{11} , perform the following calculations.
   a. $(x^2 + 2x + 9)(2x^3 + 9x^2 + x + 7)$
   b. $(8x^2 + 3x + 2)(5x^2 + 4)$

2. Determine which of the following polynomials are reducible over GF(2).
   a. $x^2 + x + 1$
   b. $x^7 + x^5 + x^3 + x^2 + x + 1$

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. Compute $(x^2+2x+2)^{-1}$ mod x^4+2x^2+1, where the coefficients are over Z_3.

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

Part 2: Programming Problem

This programming problem is to use the AES library "Crypto++" to encode messages in various encryption and padding modes. The purpose is to get familiar with parameter settings and function calls. Please find the related library information and examples on the Internet.

I. Encrypt the following 33-byte message (in ASCII, quotes are not included.)

"AES is the block cipher standard."

by the key "1234567890ABCDEF" (ASCII) and the following specifications.

Mode	Initial Vector (IV)	Output format	Padding method (see Wiki Padding for details)
CFB	0000 0000 0000 0000 (ASCII)	Hex	- (no padding)
CBC	0000 0000 0000 0000 (ASCII)	Hex	Zeros Padding
CBC	9999 9999 9999 9999 (ASCII)	Hex	PKCS#7
ECB	-	Hex	PKCS#7

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

A. CFB, IV=0000 0000 0000 0000 → 36 db 74 5b 3b 6d a6 9a bf 5f eb 23

B. CBC, IV=0000 0000 0000 0000, Zeros Padding
→ 4c 85 5d 63 17 60 8f 8d d3 94 61 e5 bc c9 40 b8

C. ECB, PKCS padding → d5 23 32 6c 27 ee 0f 21 65 c7 69 6b 36 f2 68 8e

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 lines of ciphertexts.

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.