Introduction to Cryptography, Fall 2021

Homework 2

Due: 5pm, 10/19/2021 (Wed)

Part 1: Written Problems

1. For polynomial arithmetic with specified coefficient fields, perform the following calculation:

   a. $(x^2 + 7x + 9)(2x^3 + 9x^2 + 5)$ over GF(11)

   $2x^5 + x^4 + 4x^3 + 9x^2 + 2x + 1$

   b. $(2x^5 + 3x + 2) \bmod (5x^3 + 4)$ over GF(7)

   $4x^3 + 3x + 2$

   c. gcd $(x^4 + 8x^3 + 7x + 8, 2x^3 + 9x^2 + 10x + 1)$ over GF(11)

   $x^4 + 8x^3 + 7x + 8 = (6x + 10)(2x^3 + 9x^2 + 10x + 1) + (4x^2 + 9)$

   $2x^3 + 9x^2 + 10x + 1 = (6x + 5)(4x^2 + 9) + 0$

   So, $gcd[(x^4 + 8x^3 + 7x + 8), (2x^3 + 9x^2 + 10x + 1)] = 4x^2 + 9$

   d. $(x^3 + x + 1)^{-1} \bmod x^4 + x + 1$ over GF(2)

   $1 = x^3 + x + 1 - (x^2 + 1)(x)$

   $= (x^2 + 1)(x^3 + x + 1) + (x)(x^4 + x + 1)$

   $(x^2 + 1)(x^3 + x + 1) \equiv 1 \pmod{x^4 + x + 1}$

   So, $(x^3 + x + 1)$-1 mod $x^4 + x + 1 = x^2 + 1$

2. Determine which of the following polynomials are reducible over GF(2).

   a. $x^3 + x + 1$

   irreducible, because there is no linear factor of the form x or (x+1)

   b. $x^4 + x^2 + x + 1$

   reducible, since $x^4 + x^3 + x + 1 = (x + 1)(x^3 + x^2 + 1)$

3. In the discussion of MixColumns and InvMixColumns in AES, it is 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.

Show that d(x) = a(x)b(x) mod(x^4 + 1) = 1

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0\ a_3\ a_2\ a_1 \\ a_1\ a_0\ a_3\ a_2 \\ a_2\ a_1\ a_0\ a_3 \\ a_3\ a_2\ a_1\ a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \begin{bmatrix} 0E \\ 09 \\ 0D \\ 0B \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

({0E} · {02} $\oplus$ {09} · {03} $\oplus$ {0D} · {01} $\oplus$ {0B} · {01}) = {01}

({0E} · {01} $\oplus$ {09} · {02} $\oplus$ {0D} · {03} $\oplus$ {0B} · {01}) = {00}

({0E} · {01} $\oplus$ {09} · {01} $\oplus$ {0D} · {02} $\oplus$ {0B} · {03}) = {00}

({0E} · {03} $\oplus$ {09} · {01} $\oplus$ {0D} · {01} $\oplus$ {0B} · {02}) = {00}