Introduction to Cryptography, Fall 2021

Homework 2

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

Part 1: Written Problems

For this part, submit your answer to E3 with filename: “youid”.pdf

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)**

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

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

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

   a. $(x^2 + 7x + 9)(2x^3 + 9x^2 + 5) = 2x^5 + 23x^4 + 81x^3 + 86x^2 + 35x + 45$

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

   b. $2x^5 + 3x + 2 = (5x^3 + 4)(6x^2) + 4x^2 + 3x + 2$

   Ans: $4x^2 + 3x + 2$

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

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

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

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

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

   ⇨ $1 = x^3+x+1 - (x^2 + 1)(x)$

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

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

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

   So, $(x^3+x+1)^{-1} \bmod x^4+x+1 = x^2 + 1$

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

   a. $x^3 + x + 1$

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

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

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

3. **In the discussion of MixColumns and InvMixColumns in AES, it is stated that $b(y) = a^{-1}(y) \bmod (y^4 + 1)$, 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.**

We want to show that $c(x) = a(x)b(x) \bmod (x^4 + 1) = 1$

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 0E \\ 09 \\ 0D \\ 0B \end{bmatrix} = \begin{bmatrix} 01 \\ 00 \\ 00 \\ 00 \end{bmatrix}$$

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

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

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

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