1172/DCP1323 Introduction to Cryptography, Spring 2019
Due: 2019/3/25 (Mon.)

Homework 3

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. $(8x^2 + 3x + 2)(5x^2 + 6)$
   Answer.
   a. $(x^2 + 2x + 9)(x^3 + 11x^2 + x + 7)$
   $= x^5 + 11x^4 + x^3 + 7x^2 + 2x^4 + 22x^3 + 2x^2 + 14x + 9x^3 + 99x^2 + 9x + 63$
   $= x^5 + 13x^4 + 32x^3 + 108x^2 + 23x + 63$
   $= x^5 + 2x^4 + 10x^3 + 9x^2 + x + 8$
   b. $(8x^2 + 3x + 2)(5x^2 + 6)$
   $= 40x^4 + 48x^2 + 15x^3 + 18x + 10x^2 + 12$
   $= 40x^4 + 15x^3 + 58x^2 + 18x + 12$
   $= 7x^4 + 4x^3 + 3x^2 + 7x + 1$

2. Determine which of the following polynomials are reducible over GF(2).
   a. $x^2 + 1$
   b. $x^2 + x + 1$
   c. $x^4 + x + 1$
   Answer.
   a. reducible, since $(x^2 + 1) = (x^2 + 2x + 1) = (x + 1)^2$
   (in GF(2) $2 = 0$. therefore, $x^2 + 1 = x^2 + 2x + 1$)
   b. irreducible, because there is no linear factor of the form x or $(x + 1)$
   c. irreducible, because there is no linear factor of the form x , $(x + 1)$,
   $x^2, (x^2 + x), (x^2 + 1)$ *or* $(x^2 + x + 1)$

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)
   Answer.
   $x^4 + 8x^3 + 7x + 8 = (6x + 10)(2x^3 + 9x^2 + 10x + 1) + (4x^2 + 9)$
   $2x^3 + 9x^2 + 10x + 1 = (6x + 5)(4x^2 + 9) + 0$
   So, $gcd[(x^4 + 8x^3 + 7x + 8),\ (2x^3 + 9x^2 + 10x + 1)] = 4x^2 + 9$

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

Answer.

+	00 (0)	01 (1)	10 (x)	11 (x+1)
00	0	1	x	x+1
01	1	0	x+1	x
10	x	x+1	0	1
11	x+1	x	1	0

*	00 (0)	01 (1)	10 (x)	11 (x+1)
00	0	0	0	0
01	0	1	x	x+1
10	0	x	x+1	1
11	0	x+1	1	x

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.

Answer.

Show that $\mathrm{d(x) = a(x)b(x) \ \ mod}(x^4+1) = 1$

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

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

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

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

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

6. Given the plaintext {0F0E0D0C0B0A09080706050403020100} and the key

{02020202020202020202020202020202}:

a. Show the original contents of **State**, displayed as a 4 x 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.

Answer.

a. Original state

0F	0B	07	03
0E	0A	06	02
0D	09	05	01
0C	08	04	00

b. After AddRoundKey

0D	09	05	01
0C	08	04	00
0F	0B	07	03
0E	0A	06	02

c. After SubBytes

D7	01	6B	7C
FE	30	F2	63
76	2B	C5	7B
AB	67	6F	77

d. After ShiftRows

D7	01	6B	7C
30	F2	63	FE
C5	7B	76	2B
77	AB	67	6F

e. After MixColumns

57	DF	62	A5
94	D8	50	89
EF	E3	4D	65
79	C7	66	8F