ECE 404 Homework #4

Ranjan Behl

Due: **TUESDAY** 2/23/2021 at 5:59PM

In this homework, you will get a deeper understanding of finite fields of the form $GF(2^n)$ and the Advanced Encryption Standard (AES).

Theory Problems

1. Determine the following in GF(13), please show your work:
   (a) $(7x^4 + 3x^3 + x^2 + 10) - (9x^4 + 6x^3 + 7x^2 + 8x + 2)$
   (b) $(7x^3 + 2x + 9) \times (2x^3 + x^2 + 8x + 7)$
   (c) $\frac{12x^5+4x^4+36x^3+12x^2+x}{3x^3+4x^2+3}$
2. For the finite field $GF(2^3)$, calculate the following for the modulus polynomial $x^3 + x + 1$, please show your work:
   (a) $(x^2 + x + 1) \times (x + 1)$
   (b) $(x + 1) - (x^2 + x + 1)$
   (c) $\frac{x^2+x+1}{x^2+1}$

Programming Problem

Write a script in Python or Perl to implement the AES algorithm with a 256-bit key size.
The following points may aid you in your implementation and are worth noting:

1. Each round of AES involves four steps:
   (a) Single-byte based substitution
   (b) Row-wise permutation
   (c) Column-wise mixing
   (d) Addition of the round key
2. **The order in which these four steps are executed is different for encryption and decryption. The last round for encryption does not involve the 'Mix columns' step. Similarly, the last round for decryption does not involve the 'Inverse mix columns' step.**
3. As you know, AES has variable key-length, and the number of rounds of processing depend upon the key-length. The lecture assumes a 128-bit key length and all subsequent explanation is based upon that assumption. But the key provided to you is 256 bits long, hence, there will be a slight variation in how you generate the *key schedule*. The following explanation will be helpful in that regard:

Theory Problems

1. Determine the following in GF(13), please show your work:
   (a) $(7x^4 + 3x^3 + x^2 + 10) - (9x^4 + 6x^3 + 7x^2 + 8x + 2)$
   (b) $(7x^3 + 2x + 9) \times (2x^3 + x^2 + 8x + 7)$
   (c) $\frac{12x^5+4x^4+36x^3+12x^2+x}{3x^3+4x^2+3}$
2. For the finite field $GF(2^3)$, calculate the following for the modulus polynomial $x^3 + x + 1$, please show your work:
   (a) $(x^2 + x + 1) \times (x + 1)$
   (b) $(x + 1) - (x^2 + x + 1)$
   (c) $\frac{x^2+x+1}{x^2+1}$

1) GF(13)

additive inverse:

0	1	2	3	4	5	6	7	8	9	10	11	12
0	12	11	10	9	8	7	6	5	4	3	2	1

(a) $(7x^4 + 3x^3 + x^2 + 10) - (9x^4 + 6x^3 + 7x^2 + 8x + 2)$

$= (7x^4 + 3x^3 + x^2 + 10) + (4x^4 + 7x^3 + 6x^2 + 5x + 11)$

$= 11x^4 + 10x^3 + 7x^2 + 5x + 21$

$= \boxed{11x^4 + 10x^3 + 7x^2 + 5x + 8}$

$21 \bmod 13 = 8$

(b) $(7x^3 + 2x + 9) \times (2x^3 + x^2 + 8x + 7)$

$= 14x^6 + 7x^5 + 56x^4 + 49x^3 + 4x^4 + 2x^3 + 16x^2 + 14x + 18x^3 + 9x^2 + 72x + 63$

$= 14x^6 + 7x^5 + 60x^4 + 69x^3 + 25x^2 + 86x + 63$

$14 \bmod 13 = 1$

$60 \bmod 13 = 8$

$69 \bmod 13 = 4$

$25 \bmod 13 = 12$

$86 \bmod 13 = 8$

$63 \bmod 13 = 11$

$= \boxed{x^6 + 7x^5 + 8x^4 + 4x^3 + 12x^2 + 8x + 11}$

(c) $\dfrac{12x^5+4x^4+36x^3+12x^2+x}{3x^3+4x^2+3}$

MI of 3 is 9

$(3 \cdot 9) \bmod 13 = 27 \bmod 13 = 1$ ✓

$\frac{12}{3} \Rightarrow 12 \cdot 9 = 108 \qquad 108 \bmod 13 = 4$

$$\frac{12x^5 + 4x^4 + 36x^3 + 12x^2 + x}{3x^3 + 4x^2 + 3}$$

$$= 4x^2 + \frac{12x^5 - 12x^5 + 4x^4 - 16x^4 + 36x^3 + 12x^2 - 12x^2 + x}{3x^3 + 4x^2 + 3}$$

$-16 = -2 \cdot 13 + 10$

$36 = 36 \bmod 13 = 10$

$14 = 14 \bmod 13 = 1$

$$= 4x^2 + \frac{x^4 + 10x^3 + x}{3x^3 + 4x^2 + 3} \qquad \frac{1}{3} = 1 \cdot 9 = 9$$

$$= 4x^2 + 9x + \frac{x^4 - 27x^4 + 10x^3 - 36x^3 + x - 27x}{3x^3 + 4x^2 + 3}$$

$-27 = -3(13) + 12$

$-36 = -3(13) + 3$

$= 4x^2 + 9x + \dfrac{x^4 + 12x^4 + 10x^3 + 3x^3 + 7x + 12x}{3x^3 + 4x^2 + 3}$

$= 4x^2 + 9x + \dfrac{13x^4 + 13x^3 + 13x}{3x^3 + 4x^2 + 3} = 0$

$= \boxed{4x^2 + 9x}$

2) (a) $(x^2 + x + 1) \times (x + 1)$, GF(8)

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

$= x^3 + 1$

now $x^3 + 1 \bmod x^3 + x + 1 \Rightarrow \boxed{x}$

1001

1011

$$\begin{array}{r|l} & 1 \\ 1011 & 1001 \\ & 1011 \\ \hline & 0010 \end{array}$$

$\rightarrow x$

(b) $(x+1)-(x^2+x+1)$

$= -x^2$

$\Rightarrow -x^2 \mod x^3+x+1 \Rightarrow \boxed{x^2}$

```
   11
1011 0100
     1011
     ----
     1111
     1011
     ----
     0100
     ----
      x^2
```

(c) $\dfrac{x^2+x+1}{x^2+1}$

$(x^2+x+1)/(x^2+1) = (x^2+x+1)\cdot(x^2+1)^{-1}$

$(x^2+1)^{-1} = ?$

$x^2+1 = 101 \Rightarrow (x^2+1)^{-1} = 010$

So $(x^2+x+1)\cdot(x) = x^3+x^2+x$

$\Rightarrow \underbrace{x^3 + x^2 + x}_{1110} \mod \underbrace{x^3 + x + 1}_{1011} \Rightarrow \boxed{x^2 + 1}$

$$
\begin{array}{r|l}
1011 & 1110 \\
 & 1011 \\
\hline
 & 0101
\end{array}
$$

$\rightarrow x^2 + 1$