Homework 1

Jackson Mowry

Wed Aug 20 11:06:37 2025

Contents

1 Finite Field Multiply Pseudocode

```
def ffMultiply(a, b):
    powers = [a]

    for i = 0; i < 7:
        powers.push(xtime(powers[i]))

    answer: u8 = 0
    for i = 0; i < 8:
        if b & (1 << i):
            answer ^= powers[i]

    return answer
```

2 MixColumns Pseudocode

```
def MixColumns(state):
    answer = state
    for col = 0; col < 4:
        # row 0
        answer(0, col) = ffMultiply(2, state(0, col)) ^
                         ffMultiply(3, state(1, col)) ^
                         state(2, col) ^
                         state(3, col)
        # row 1
        answer(1, col) = state(0, col) ^
                         ffMultiply(2, state(1, col)) ^
                         ffMultiply(3, state(2, col)) ^
                         state(3, col)
        # row 2
        answer(2, col) = state(0, col) ^
                         state(1, col) ^
                         ffMultiply(2, state(2, col)) ^
                         ffMultiply(3, state(3, col))
        # row 3
        answer(3, col) = ffMultiply(3, state(0, col)) ^
                         state(1, col) ^
                         state(2, col) ^
                         ffMultiply(2, state(3, col))

    return answer
```