

Hector Lopez

65-764-0379

Section 1

1.

MixColumns(state):

```
    for each column in the state matrix
        # matrix multiplication for this function defines addition as XOR and multiplication as ffMultiply

        the first item in the column is equal to the column matrix multiplied by the top row of the fixed matrix
        second item is equal to column matrix multiplied by the second row
        third " " " third row
        fourth " " " fourth row
    return state
```

2.

xtime(byte):

```
    do a left bitshift by one on byte to drop high bit
    if the high bit is one
        return byte ^ 0x1b
    else:
        return byte
```

uint8_t ffMultiply(uint8_t a,uint8_t b):

```
    answer = 0
    for right shift b
        and the bit that fell off with 1
        if it's equal to 1 then answer = answer ^ a
        a = xtime(a)
    return answer
```