LAB 5

* PART 1

* For this segment, we use the following GF(2⁴) example:

$A(x) = x^3 + x^2 + 1$ (rep as 1011) (int val = 13)
$B(x) = x^2 + x$ (rep as 0110) (int val = 6)
$P(x) = x^4 + x^3 + 1$ (rep as 10011)

ADDITION

$A(x) + B(x) =$

```
  1 0 1 1
⊕ 0 1 1 0
---------
  1 1 0 1
```

Bitwise XOR

$= x^3 + x + 1$ // (int val = 11) → tallies w/ table & math

MULTIPLICATION

* We use the method that given in the handout

$A(x) \cdot B(x) \bmod P(x)$

Powers	Operations	New Result	R
$x^0 \otimes B(x)$	—	$x^2 + x$	N
$x^1 \otimes B(x)$	$x \otimes (x^2 + x)$	$x^3 + x^2$	N
$x^2 \otimes B(x)$	$x \otimes (x^3 + x^2)$	1	Y
$x^3 \otimes B(x)$	$x \otimes (1)$	x	N

$x^4 + x^3$ IGNORE

```
  0 0 0 1 +
  1 0 0 1 +
---------
  1 0 0 0
```

$A(x) \otimes B(x) = (x^2 + x) + (1) + (x)$

```
  0 1 1 0
  1 0 0 0
  0 1 0 0
---------
  1 0 1 0
```

Bitwise XOR

$= x^2 + 1$ // (int val = 5) → tallies with table

* To further verify, I also use the method discussed in the lecture. (In this representation, LSB is highest power)

① $A(x) \cdot B(x) =$

```
  1 1 0 1   } AND
  0 1 1 0
---------
  1 1 0 1 0 } XOR.
1 1 0 1 0 0
-----------
1 0 1 1 1 0
```

② We then mod p:

```
          1 0
      -------
11001 | 1 0 1 1 1 0
        1 1 0 0 1
      -----------
          1 1 1 0 0
          1 1 0 0 1
        -----------
              1 0 1
```

Hence, ans = 101 = $x^2 + 1$ //

(INT) ADDITION TABLE(2⁴) → available in the code :)
:)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

(INT) MULTIPLICATION TABLE(2⁴) → available in the code

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	4	6	8	10	12	14	9	11	13	15	1	3	5	7
3	3	6	5	12	15	10	9	1	2	7	4	13	14	11	8
4	4	8	12	9	13	1	5	11	15	3	7	2	6	10	14
5	5	10	15	13	8	7	2	3	6	9	12	14	11	4	1
6	6	12	10	1	7	13	11	2	4	14	8	3	5	15	9
7	7	14	9	5	2	11	12	10	13	4	3	15	8	1	6
8	8	9	1	11	3	2	10	15	7	6	14	4	12	13	5
9	9	11	2	15	6	4	13	7	14	12	5	8	1	3	10
10	10	13	7	3	9	14	4	6	12	11	1	5	15	8	2
11	11	15	4	7	12	8	3	14	5	1	10	9	2	6	13
12	12	1	13	2	14	3	15	4	8	5	9	6	10	7	11
13	13	3	14	6	11	5	8	12	1	15	2	10	7	9	4
14	14	5	11	10	4	15	1	13	3	8	6	7	9	2	12
15	15	7	8	14	1	9	6	5	10	2	13	11	4	12	3

#PART 2

INVERSE MUL

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

$P(x) = x^4 + x^1 + 1$

(These are long-div workings)
LSB is highest power

	Remainder (q)	Quotient (a)	y
①	x^4+x^1+1		$x(x^2+1)+1$
②	x^2+1	x^2+1	x
③	x	x	1
④	1	x	0

① → ②

```
      101
  101 | 1001
       101
       ---
       010
```

② → ③

```
       10
  10 | 101
       10
       --
        1
```

③ → ④

```
       10
   1 | 10
       1
       -
       0
```

$$\therefore y = x(x^2+1)+1$$
$$= x^3 + x + 1 \;//$$

AES Table Generated (Anvil in code)

```
############ The following is submission for part 2 ############

----- The S-Box AES Table --------
0x63 0x7c 0x77 0x7b 0xf2 0x6b 0x6f 0xc5 0x30 0x1  0x67 0x2b 0xfe 0xd7 0xab 0x76
0xca 0x82 0xc9 0x7d 0xfa 0x59 0x47 0xf0 0xad 0xd4 0xa2 0xaf 0x9c 0xa4 0x72 0xc0
0xb7 0xfd 0x93 0x26 0x36 0x3f 0xf7 0xcc 0x34 0xa5 0xe5 0xf1 0x71 0xd8 0x31 0x15
0x4  0xc7 0x23 0xc3 0x18 0x96 0x5  0x9a 0x7  0x12 0x80 0xe2 0xeb 0x27 0xb2 0x75
0x9  0x83 0x2c 0x1a 0x1b 0x6e 0x5a 0xa0 0x52 0x3b 0xd6 0xb3 0x29 0xe3 0x2f 0x84
0x53 0xd1 0x0  0xed 0x20 0xfc 0xb1 0x5b 0x6a 0xcb 0xbe 0x39 0x4a 0x4c 0x58 0xcf
0xd0 0xef 0xaa 0xfb 0x43 0x4d 0x33 0x85 0x45 0xf9 0x2  0x7f 0x50 0x3c 0x9f 0xa8
0x51 0xa3 0x40 0x8f 0x92 0x9d 0x38 0xf5 0xbc 0xb6 0xda 0x21 0x10 0xff 0xf3 0xd2
0xcd 0xc  0x13 0xec 0x5f 0x97 0x44 0x17 0xc4 0xa7 0x7e 0x3d 0x64 0x5d 0x19 0x73
0x60 0x81 0x4f 0xdc 0x22 0x2a 0x90 0x88 0x46 0xee 0xb8 0x14 0xde 0x5e 0xb  0xdb
0xe0 0x32 0x3a 0xa  0x49 0x6  0x24 0x5c 0xc2 0xd3 0xac 0x62 0x91 0x95 0xe4 0x79
0xe7 0xc8 0x37 0x6d 0x8d 0xd5 0x4e 0xa9 0x6c 0x56 0xf4 0xea 0x65 0x7a 0xae 0x8
0xba 0x78 0x25 0x2e 0x1c 0xa6 0xb4 0xc6 0xe8 0xdd 0x74 0x1f 0x4b 0xbd 0x8b 0x8a
0x70 0x3e 0xb5 0x66 0x48 0x3  0xf6 0xe  0x61 0x35 0x57 0xb9 0x86 0xc1 0x1d 0x9e
0xe1 0xf8 0x98 0x11 0x69 0xd9 0x8e 0x94 0x9b 0x1e 0x87 0xe9 0xce 0x55 0x28 0xdf
0x8c 0xa1 0x89 0xd  0xbf 0xe6 0x42 0x68 0x41 0x99 0x2d 0xf  0xb0 0x54 0xbb 0x16
(venv) ironwalrus@flyingwalrus-ironclad:~/PycharmProjects/FCS Labs/Lab 5$
```