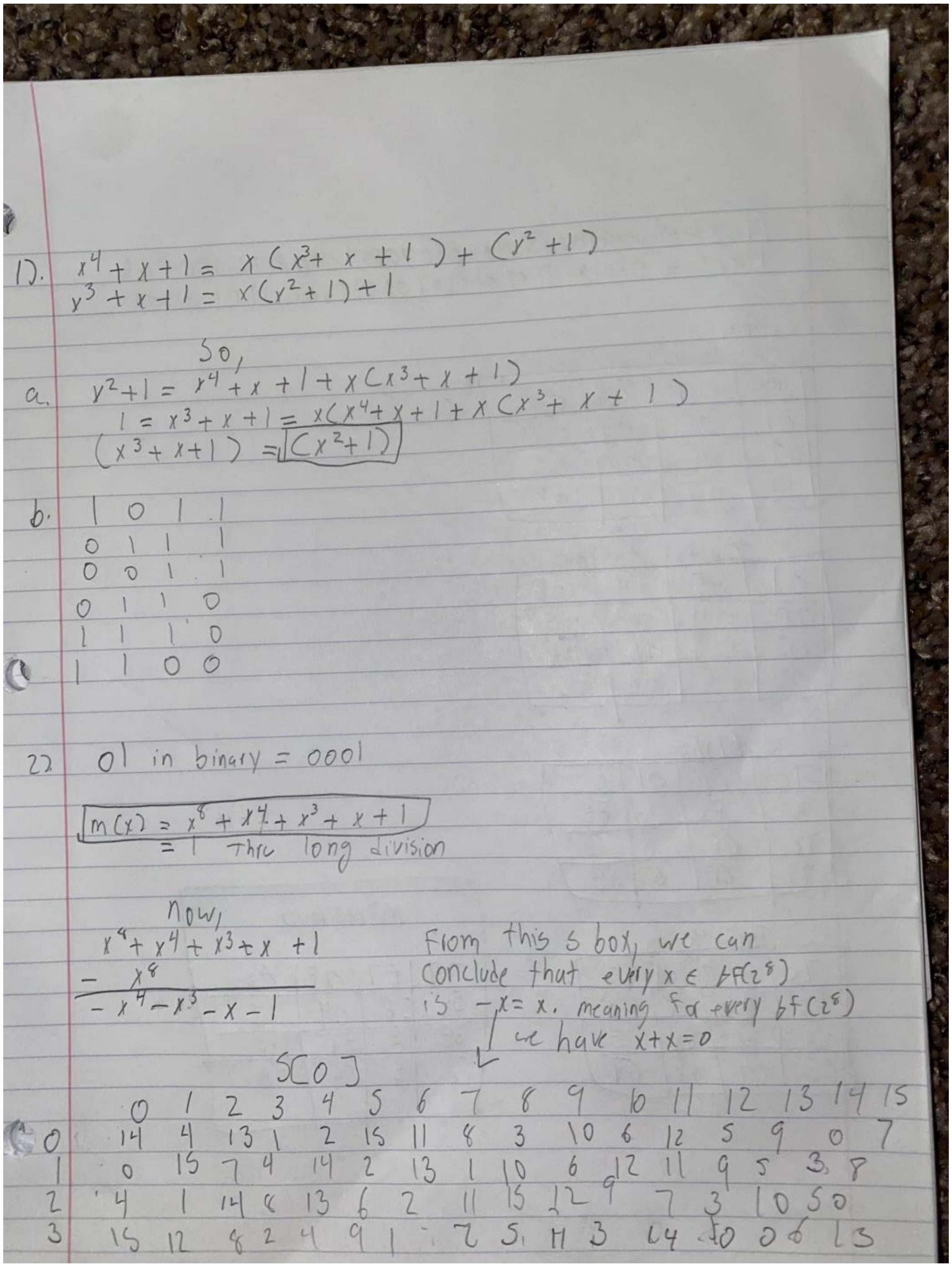
Issa Odeh

M3 Homework



1). $x^4+x+1 = x(x^3+x+1)+(x^2+1)$

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

So,

a. $x^2+1 = x^4+x+1+x(x^3+x+1)$

$1 = x^3+x+1 = x(x^4+x+1+x(x^3+x+1)$

$(x^3+x+1) = \boxed{(x^2+1)}$

b. 1 0 1 1

0 1 1 1

0 0 1 1

0 1 1 0

1 1 1 0

1 1 0 0

2) 01 in binary = 0001

$\boxed{m(x) = x^8+x^4+x^3+x+1}$

= 1 thru long division

now,

$x^4+x^4+x^3+x+1$

$-\ x^8$

$-x^4-x^3-x-1$

From this s box, we can conclude that every $x \in GF(2^8)$ is $-x = x$. meaning for every $GF(2^8)$ we have $x+x=0$

S[0]

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

3. plaintext=000102030405060708090A0B0C0D0E0f
Key = 01010101 01 01 01 0101 01 010101 01 01 01 01

a). orginal

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

Initial AddRound Key

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

SubBytes

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

Shift Rows

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

Mixed Rows

74	E7	0F	A2
55	E6	04	22
3E	2E	B8	8C
F6	15	58	0B