GF 256

Martin Kozeny
MATH 4530: Intro Cryptography
Spring 2011 University of New Orleans

March 3, 2011

1 Adding

For adding, I tried to evaluate these examples with shown results in table 1.

Table 1: Adding in GF 256

Left operand	Right operand	Expected result	Result
A1	D7	76	76
57	83	D4	D4
4B	C8	83	83
B2	E5	57	57
F1	10	E1	E1
D7	12	C5	C5
07	B9	BE	BE

2 Multiplying

For multiplying, I tried to evaluate these examples with shown results in table 2.

Table 2: Multiplying in GF 256

Left operand	Right operand	Expected result	Result
A1	D7	D0	D0
57	83	C1	C1
4B	C8	89	89
B2	E5	76	76
F1	10	89	89
D7	12	6A	6A
07	B9	2	2

3 Finding inverses

For finding inverses, I tried to evaluate these examples with shown results in table 3.

Table 3: Finding inverses in GF 256

Operand	Expected result	Result
7E	81	81
4B	4B	13
C6	E4	E4
B2	1F	1F
F1	23	23
D7	EA	EA
07	D1	D1

4 Conclusion

In conclusion it appears from provided test, that implemented algorithm works correctly.