分组密码作业

1. 验证 DES 中 S 盒的非线性性质。即证明 $S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$;

(1) $x_1 = 000000, x_2 = 000001$

(2) $x_1 = 111111, x_2 = 100000$

(3) $x_1 = 101010, x_2 = 010101$

	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	S_1
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	

2. 给定不可约多项式 $P(x) = x^4 + x + 1$。在 $GF(2^4)$上计算 $A(x) + B(x) \bmod P(x)$。

(1) $A(x) = x^2 + 1, B(x) = x^3 + x^2 + 1$

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

3. 给定不可约多项式 $P(x) = x^4 + x + 1$。在 $GF(2^4)$上计算 $A(x) \cdot B(x) \bmod P(x)$。

(1) $A(x) = x^2 + 1, B(x) = x^3 + x^2 + 1$

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

4. 若明文为 $M = (0000000000000000)_{16}$, 密钥为 $Key = (0000000000000000)_{16}$, 求经过 DES 加密操作 16 轮中第 1 轮处理后所得的结果。

5. 若明文为 $M = (1111111111111111)_{16}$, 密钥为 $Key = (1111111111111111)_{16}$, 求经过 DES 加密操作 16 轮中第 1 轮处理后所得的结果。

6. $W = (w_0, w_1, w_2, w_3)$ = (0x01000000, 0x00000000, 0x00000000, 0x00000000)为 128 比特的 AES 的输入。第一轮计算中使用的子密钥为 $W_0, W_1, W_2, W_3, \ldots, W_7$。

W_0 = (0x2B7E1516); W_1 = (0x28AED2A6); W_2 = (0xABF71588)

W_3 = (0x09CF4F3C); W_4 = (0xA0FAFE17); W_5 = (0x88542CB1)

W_6 = (0x23A33939); W_7 = (0x2A6C7605)

(1) 输入为 W, 子密钥为 $W_0, \ldots, W_7$。计算 AES 的第一轮输出结果;

(2) 输入和子密钥均为全 0 的情况下, 计算 AES 的第一轮输出结果;

(3) 只考虑一轮的情况下, 在输出中有多少比特位发生了变化?

7. 如果在 OFB 模式下执行加密操作, 加密不同数据时使用相同的 IV, 那么可以如何进行攻击?