分组密码作业

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

(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	

解：(1) $S_1(x_1) = 14 = (1110)_2$，$S_1(x_2) = 0 = (0000)_2$，所以，$S_1(x_1) \oplus S_1(x_2) = (1110)_2$；
$x_1 \oplus x_2 = (000001)$, 所以，$S_1(x_1 \oplus x_2) = 0 = (0000)_2$；因此，$S_1(x_1)\cdot S_1(x_2) \neq S_1(x_1 \oplus x_2)$。
(2) $S_1(x_1) = 13 = (1101)_2$，$S_1(x_2) = 4 = (0100)_2$，所以，$S_1(x_1) \oplus S_1(x_2) = (1001)_2$；
$x_1 \oplus x_2 = (011111)$, 所以，$S_1(x_1 \oplus x_2) = 8 = (1000)_2$；因此，$S_1(x_1)\cdot S_1(x_2) \neq S_1(x_1 \oplus x_2)$。
(3) $S_1(x_1) = 6 = (1110)_2$，$S_1(x_2) = 12 = (1100)_2$，所以，$S_1(x_1) \oplus S_1(x_2) = (1010)_2$；
$x_1 \oplus x_2 = (111111)$, 所以，$S_1(x_1 \oplus x_2) = 13 = (1101)_2$；因此，$S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$。

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) $A(x) = x^2 + 1, B(x) = x + 1$。

解：

(1) $A(x)+B(x) = x^3+2x^2+2 = x^3 \bmod P(x)$。

(2) $A(x)+B(x) = x^2+x+2 = x^2 + x \bmod P(x)$。

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

解：

(1) $A(x)\cdot B(x) = (x^2 + 1)\cdot(x^3 + x^2 + 1) = x^5 + x^4 + x^3 + 2x^2 + 1$

$= x^5 + x^4 + x^3 + 2x^2 + 1$

$= x^3 + x^2 \mod P(x)$。

(2) $A(\mathrm{x})\cdot B(\mathrm{x}) = (x^2 + 1)\cdot(x + 1)$

$= x^3 + x^2 + x + 1 \bmod P(x)$。

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。

解：
根据 DES 算法的流程进行推导：
输入为 $M = (0000000000000000)_{16}$，密钥为 $Key = (0000000000000000)_{16}$。
(1)经过 *IP* 置换得到：$L_0=(0000\ 0000)_{16}$, $R_0=(0000\ 0000)_{16}$;
(2)第一轮密钥 K1 生成：

a. Key 经过 PC-1 得到 C0=D0=$(0000\ 000)_{16}$;
b. 左移位得到：C0=D0=$(0000\ 000)_{16;}$
c. 经过 PC-2 得到 $K_1=(0000\ 0000\ 0000)_{16}$

(3)$L_1=R_0=(0000\ 0000)_{16}$,;
(4)R_0 经过 *E* 盒扩展置换得到 $R'_0 = (0000\ 0000\ 0000)_{16;}$
(5)R_0 与 K_1 异或得到 $R'_0 = (0000\ 0000\ 0000)_{16}$
(6)经过 *S* 盒代替得到 $R'_0 = (EFA7\ 2C4D)_{16}$
(7)经过 P 盒置换得到 $R'_0 =(D8D8\ DBBC)_{16}$
因此，$L_1=(0000\ 0000)_{16}$, $R_1=(D8D8\ DBBC)_{16}$。

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。
解：
根据 DES 算法的流程进行推导：
输入为 $M = (1111\ 1111\ 1111\ 1111)_{16}$，密钥为 $Key = (1111\ 1111\ 1111\ 1111)_{16}$。
(1)经过 *IP* 置换得到：$L_0=(00FF\ 00FF)_{16}$, $R_0=(0000\ 0000)_{16}$;
(2)第一轮密钥 K1 生成：

a. Key 经过 PC-1 得到 C0=D0=$(0000\ 00F)_{16}$;
b. 左移位得到：C0=D0=$(0000\ 01E)_{16;}$
c. 经过 PC-2 得到 $K_1=(1000\ 8844\ 0040)_{16}$

(3)$L_1=R_0=(0000\ 0000)_{16}$,;
(4)R_0 经过 *E* 盒扩展置换得到 $R'_0 = (0000\ 0000\ 0000)_{16;}$
(5)R_0 与 K_1 异或得到 $R'_0 = (1000\ 8844\ 0040)_{16}$;
(6)经过 *S* 盒代替得到 $R'_0 = (DF00\ 5CDD)_{16;}$
(7)经过 *P* 盒置换得到 $R_1 = R'_0 =(7A63\ C8C4)_{16;}$
因此，$L_1=(00FF\ 00FF)_{16}$, $R_1=(7A63\ C8C4)_{16}$。

6. $W = (w_0, w_1, w_2, w_3)$ = (0x0001000000, 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, …, 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, …, 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?

解：(1)

① 输入为$\begin{pmatrix}01 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\end{pmatrix}$

②轮密钥加：$\begin{pmatrix}01 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\end{pmatrix}\oplus\begin{pmatrix}2B & 28 & AB & 09\\ 7E & AE & F7 & CF\\ 15 & D2 & 15 & 4F\\ 16 & A6 & 88 & 3C\end{pmatrix}=\begin{pmatrix}2A & 28 & AB & 09\\ 7E & AE & F7 & CF\\ 15 & D2 & 15 & 4F\\ 16 & A6 & 88 & 3C\end{pmatrix}$

③字节代换$\begin{pmatrix}E5 & 34 & 62 & 01\\ F3 & E4 & 68 & 8A\\ 59 & B5 & 59 & 84\\ 47 & 24 & C4 & E8\end{pmatrix}$

④行移位$\begin{pmatrix}E5 & 34 & 62 & 01\\ E4 & 68 & 8A & F3\\ 59 & 84 & 59 & B5\\ EB & 47 & 24 & C4\end{pmatrix}$

⑤列混淆$\begin{pmatrix}02 & 03 & 01 & 01\\ 01 & 02 & 03 & 01\\ 01 & 01 & 02 & 03\\ 03 & 01 & 01 & 02\end{pmatrix}\oplus\begin{pmatrix}E5 & 34 & 62 & 01\\ E4 & 68 & 8A & F3\\ 59 & 84 & 59 & B5\\ EB & 47 & 24 & C4\end{pmatrix}=\begin{pmatrix}54 & 13 & 3C & 7D\\ 36 & 34 & A2 & FC\\ 95 & 86 & 36 & D4\\ 44 & 3E & 3D & D6\end{pmatrix}$

⑥轮密钥加$\begin{pmatrix}54 & 13 & 3C & 7D\\ 36 & 34 & A2 & FC\\ 95 & 86 & 36 & D4\\ 44 & 3E & 3D & D6\end{pmatrix}\oplus\begin{pmatrix}A0 & 88 & 23 & 2A\\ FA & 54 & A3 & 6C\\ FE & 2C & 39 & 76\\ 17 & B1 & 39 & 05\end{pmatrix}=\begin{pmatrix}F4 & 9B & 1F & 57\\ CC & 60 & 01 & 90\\ 6B & AA & 0F & A2\\ 53 & 8F & 04 & D3\end{pmatrix}$

因此，结果为$(\text{F4CC 6B53 9660 AA8F 1F01 0F04 5790 02D3})_{16}$。

(2)

① 输入和子密钥均为$\begin{pmatrix}00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\end{pmatrix}$

②轮密钥加：$\begin{pmatrix}00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\end{pmatrix}\oplus\begin{pmatrix}00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\end{pmatrix}=\begin{pmatrix}00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\\ 00 & 00 & 00 & 00\end{pmatrix}$

③字节代换$\begin{pmatrix}63 & 63 & 63 & 63\\ 63 & 63 & 63 & 63\\ 63 & 63 & 63 & 63\\ 63 & 63 & 63 & 63\end{pmatrix}$

④行移位$\begin{pmatrix}63 & 63 & 63 & 63\\63 & 63 & 63 & 63\\63 & 63 & 63 & 63\\63 & 63 & 63 & 63\end{pmatrix}$

⑤列混淆$\begin{pmatrix}63 & 63 & 63 & 63\\63 & 63 & 63 & 63\\63 & 63 & 63 & 63\\63 & 63 & 63 & 63\end{pmatrix}$

⑥轮密钥加$\begin{pmatrix}63 & 63 & 63 & 63\\63 & 63 & 63 & 63\\63 & 63 & 63 & 63\\63 & 63 & 63 & 63\end{pmatrix}\oplus\begin{pmatrix}00 & 00 & 00 & 00\\00 & 00 & 00 & 00\\00 & 00 & 00 & 00\\00 & 00 & 00 & 00\end{pmatrix}=\begin{pmatrix}63 & 63 & 63 & 63\\63 & 63 & 63 & 63\\63 & 63 & 63 & 63\\63 & 63 & 63 & 63\end{pmatrix}$

因此，结果为$(6363\ 6363\ 6363\ 6363\ 6363\ 6363\ 6363\ 6363)_{16}$。

(3)

显然，当输入为 W, 子密钥为 $W_0, \ldots, W_7$ 时，AES 第一轮的输出结果与输入相比改变了 61 位。 当输入和子密钥全为 0 的情况下，AES 第一轮的输出结果与输入相比改变了 64 位。

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?

解：利用已知明文攻击。若明文 m 的明文块 x_i 对应的密文是 y_i，那么，将 x_i 与对应的 y_i 进行异或可得到 IV 经过加密得到的结果 E_{IV}。若 m 的其它明文块 x_j 使用相同 IV 进行加密得到的密文为 y_j，那么，明文 x_j 可由 E_{IV} 和 y_j 异或得到。

下图为 OFB 模式流程图。