作业03.

1. $a(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ $\quad b(x) = b_3x^3 + b_2x^2 + b_1x + b_0$.

$$a(x) * c(x) \equiv \{03\}\cdot a_3x^6 + (\{03\}\cdot a_2 + \{01\}\cdot a_3)x^5 + (\{03\}\cdot a_1 + \{01\}\cdot a_2 + \{01\}\cdot a_3)x^4$$
$$+ (\{03\}\cdot a_0 + \{01\}\cdot a_1 + \{01\}\cdot a_2 + \{02\}\cdot a_3)x^3 + (\{01\}\cdot a_0 + \{01\}\cdot a_1 + \{02\}\cdot a_2)x^2$$
$$+ (\{01\}\cdot a_0 + \{02\}\cdot a_1)x + \{02\}\cdot a_0.$$
$$\equiv (\{03\}\cdot a_0 + \{01\}\cdot a_1 + \{01\}\cdot a_2 + \{02\}\cdot a_3)x^3 + (\{01\}\cdot a_0 + \{01\}\cdot a_1 + \{02\}\cdot a_2 + \{03\}\cdot a_3)x^2$$
$$+ (\{01\}\cdot a_0 + \{02\}\cdot a_1 + \{03\}\cdot a_2 + \{01\}\cdot a_3)x + (\{02\}\cdot a_0 + \{03\}\cdot a_1 + \{01\}\cdot a_2 + \{01\}\cdot a_3).$$
$$(\bmod\ x^4+1)$$

即 $b_0 = \{02\}\cdot a_0 + \{03\}\cdot a_1 + \{01\}\cdot a_2 + \{01\}\cdot a_3$

$b_1 = \{01\}\cdot a_0 + \{02\}\cdot a_1 + \{03\}\cdot a_2 + \{01\}\cdot a_3$

$b_2 = \{01\}\cdot a_0 + \{01\}\cdot a_1 + \{02\}\cdot a_2 + \{03\}\cdot a_3$

$b_3 = \{03\}\cdot a_0 + \{01\}\cdot a_1 + \{01\}\cdot a_2 + \{02\}\cdot a_3$

$$\Longleftrightarrow \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

∴得证.

No.

Date / /

2. 0x87：10000111.

$0x87 \times 0x05 = (0x87 \times 0x04) \oplus 0x87$

$= [(0x87 \times 0x02) \times 0x02] \oplus 0x87.$

$0x87 \times 0x02$：最高位1. 左移1位为 00001110

与 ~~与A~~ $\oplus$ 1b] 即 $00001110 \oplus 00011011 = 00010101$

~~=4163~~.

$00010101 \times 0x02$：最高位0，左移1位为 $00101010 = 0x2A$.

原式 $= 0x2A \oplus 0x87 = 00101010 \oplus 10000111$

$= 10101101$

$= 0xAD$.

3. $0x37 = 00110111$ 多项式表示为 $a(x) = x^5+x^4+x^2+x+1$.

$m(x) = x^8+x^4+x^3+x+1$

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

$a(x) = (x^4+1)\cdot(x+1) + x^2$

$x^4+1 = x^2 \cdot x^2 + 1$

则 $1 = (x^4+1) - x^2 \cdot x^2$

$= (x^4+1) - x^2\cdot[a(x) - (x^4+1)(x+1)]$

$= \cancel{x^2 \cdot a(x} (x^3+x^2+1)(x^4+1) + x^2\cdot a(x)$

$\cancel{= [m(x) - (x^3+x^2+x)\cdot a(x)]\cdot x - x^2 \cdot a(x)} = (x^3+x^2+1)\cdot[m(x) - (x^3+x^2+x)\cdot a(x)] + x^2\cdot a(x)$

$\cancel{= x\cdot m(x) - (x^4+x^3+x^2+x^2)\cdot a(x)}$

$\cancel{= x+1}$ $= (x^3+x^2+1)\cdot m(x) + (x^6+x)\cdot a(x)$

即 $\cancel{x\cdot m(x) + (x^4+x^3)\cdot a(x)}$ $(x^3+x^2+1)\cdot m(x) + (x^6+x)\cdot a(x) = 1$.

$x^6+x$ 写为 ~~00100~~ 01000010 即 0x42.

则 0x37 逆元为 0x42.

4. SM4算法结构：改进的Feistel结构（非平衡）.

加密：1. 每个分组128 bit，密钥128 bit.

2. 输入：4个32bit字 $(X_0, X_1, X_2, X_3)$.

3. 迭代（32轮）：$X_{i+4} = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i)$.

其中 $rk_i$ 为第 $i$ 轮密钥.

4. 输出：$(X_{35}, X_{34}, X_{33}, X_{32})$.

解密：过程同加密，需逆序使用密钥 $(rk_i)$.

轮函数T：1. 非线性变换 $\tau$：由4个并行S盒构成（相同S盒）.

设输入为 $A=(a_0, a_1, a_2, a_3)$.

输出为 $B=(b_0, b_1, b_2, b_3)$.

则 $B=\tau(A)=(Sbox(a_0), Sbox(a_1), Sbox(a_2), Sbox(a_3))$.

$a_i, b_i$ 皆为8bit（1 Byte）.

2. 线性变换L（函数）：输入为B. 输出为C.

则 $C = L(B)$

$= B \oplus (B <<< 2) \oplus (B <<< 10) \oplus (B <<< 18) \oplus (B <<< 24)$.

密钥编排：1. 128bit 加密密钥 $MK=(MK_0, MK_1, MK_2, MK_3)$.

2. $(K_0, K_1, K_2, K_3)=(MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3)$.

其中 $FK_i$ $(0 \le i \le 3)$ 为系统参数.

3. $rk_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i)$

其中 $CK_i$ 为固定参数.

↳ $T'$：1. $\tau$ 同T函数

2. 线性变换 $L'$：$L'(B)= B \oplus (B <<< 13) \oplus (B <<< 23)$