1.证明AES的列混合操作等价于矩阵乘法

$b(x) = a(x) \cdot c(x)$

$= (a_3x^3 + a_2x^2 + a_1x^1 + a_0) \cdot (03x^3 + 01x^2 + 01x + 02)$

$= 03a_3x^2 + 03a_2x^1 + 03a_1 + 03a_0x^3$

$+01a_3x^1 + 01a_2 + 01a_1x^3 + 01a_0x^2$

$+01a_3 + 01a_2x3 + 01a_1x^2 + 01a_0x^1$

$+02a_3x^3 + 02a_2x^2 + 02a_1x^1 + 02a_0$

故得

$b_0 = 02a_0 \oplus 03a_1 \oplus 01a_2 \oplus 01a_3$

$b_1 = 01a_0 \oplus 02a_1 \oplus 03a_2 \oplus 01a_3$

$b_2 = 01a_0 \oplus 01a_1 \oplus 02a_2 \oplus 03a_3$

$b_3 = 03a_0 \oplus 01a_1 \oplus 01a_2 \oplus 02a_3$

即

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

2.快速计算法，计算0x87乘以0x05模$m(x) = x^8 + x^4 + x^3 + x + 1$的值

$10000111 \otimes 00000101 = 10000111 \otimes (0100 \oplus 0001) = (10000111 \otimes 0010 \otimes 0010) \oplus 1000$

$= ((00001110 \oplus 00011011) \otimes 0010) \oplus 10000111$

$= (00010101 \otimes 0010) \oplus 10000111$

$= 00101010 \oplus 10000111 = 10101101$

3.计算0x37在有限域$F_2[x]/m(x)$的逆元

扩展欧几里得除法后得到：

$x^8 + x^4 + x^3 + x + 1 = (x^5 + x^4 + x^2 + x + 1)(x^3 + x^2 + x) + x^4 + 1$

$x^5 + x^4 + x^2 + x + 1 = (x^4 + 1)(x + 1) + x^2$

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

即

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

即逆元是$x^4 + x^3$

4.调研 SM4 算法，其迭代结构属于何类型？并详细描述加解密及密钥编排的步骤。

迭代结构

SM4 使用 Feistel 网络结构

加解密：

输入数据：首先将 128 位（16 字节）的明文分成四个 32 位的数据块 X[0], X[1], X[2], X[3]。

轮函数：进行 32 轮迭代，每一轮都使用一个不同的轮密钥 RK[i]。

轮函数每一轮的操作：将当前状态中的三个连续的数据块（X[i-3], X[i-2], X[i-1]）与当前轮密钥 RK[i] 进行异或操作。

对得到的结果应用非线性变换（通过 S 盒）。

应用线性变换 L（循环移位和异或操作）。

最后将结果与第四个数据块 X[i] 异或，生成新的数据块 X[i+1]。

输出密文：在第 32 轮结束后，最终的四个 32 位数据块（X[35], X[34], X[33], X[32]）组合成 128 位的密文输出。

解密过程与加密过程类似，不同之处在于轮密钥的使用顺序相反（从 RK[31] 到 RK[0]），其他操作保持不变。

密钥编排：

密钥扩展过程用于从初始密钥生成 32 个 32 位的轮密钥 RK[i]：

初始化：将 128 位的主密钥分为四个 32 位的部分 MK[0], MK[1], MK[2], MK[3]。

生成初始密钥：将每个部分与固定的 FK 参数进行异或运算，得到初始的 K[0], K[1], K[2], K[3]。

轮密钥生成：对于每一轮 i，执行以下操作：

将当前的 K[i+1], K[i+2], K[i+3] 与固定的 CK[i] 参数进行异或运算。

对得到的结果应用非线性变换 τ（S 盒）。

应用线性变换 L（特定的循环移位和异或操作）。

最后将结果与 K[i] 异或，生成新的 K[i+4]，即轮密钥 RK[i]。