1、证明 AES 的列混合操作等价于矩阵乘法

b(x)=a(x)*c(x) mod x^4+1, c(x)= 03 x^3+01 x^2+01x+02

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

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。

3、计算 0x37 在有限域 $F_2[x]/m(x)$ 的逆元，其中 m(x)= $x^8+x^4+x^3+x+1$。

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。