第三节 作业

1. 尝试推导AES的列混合操作转化为矩阵乘法

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

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

2. 快速计算法，计算0x87乘以0x03模 $m(x)=x^8+x^4+x^3+x+1$的值.

3. 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。

4. （选作）使用 乘法逆元及仿射方法实现AES字节代换操作 的快速运算方法。

第四节 作业

1.调研OFB模式并分析其各自性质。

2.（选做）调研CCM模式，并比较与课堂所讲工作模式异同。