**密码学第四次作业**

1.【AES解密结构优化】为了使AES解密算法与加密算法具有相同的结构，常常进行如下处理：

（1）交换逆向行移位和逆向字节代替：。示意图如下：

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | (请填写中间步骤的结果) |  |
|  |  |  |

（2）交换轮密钥加和逆向列混淆：。示意图如下(矩阵简记为)：

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | (请填写中间步骤的结果) |  |
| ③ |  |  |

2.【AES列混淆的推导】验证Rijndael密码（AES的原型，二者的主要区别是明文分组长度是否固定）中的逆向列混淆是列混淆的逆：

（1）最基础的方法是借助矩阵验证，其中， ，通过矩阵乘法验证得到结论。

（2）除矩阵外，还可用多项式的等价方法验证（事实上，矩阵法是从该方法导出的）：

* 在Rijndael密码中，，。两多项式系数的运算定义在域上，所模的不可约多项式为。
* 两多项式在该域中进行加法运算时，就是把对应次数的系数在域上相加。可将其中的元素看成位的串，那么加法就等价于操作。
* 两多项式在该域中进行乘法运算时，除了需要记住系数是域上的乘法，还需要明确结果多项式需要模。这里的多项式乘法本身不是Rijndael域中的运算：列混淆时进行乘法模这个次多项式的仅有理由就是为了使运算输出一个次多项式，即（注意到在这个环中减法与加法等同）。
* 欲证，只需证。首先计算6次多项式，然后计算3次多项式，最后验证。请详细写出计算和的过程。

3. 【AES与DES的比较】填写下表：对于列出的DES中的元素，指出AES与之相对应的元素或解释AES中为什么不需要该元素。

|  |  |  |
| --- | --- | --- |
| DES中的元素 | 实现的效果  （扩散/混淆） | AES中的对应元素  （若不存在则解释原因） |
| 函数的输入与子密钥相异或 |  |  |
| 函数的输出与分组左边的部分相异或 |  |  |
| 函数中的盒 |  |  |
| 置换 |  |  |
| 交换一个分组的两半部分 |  |  |

**注意：**

以上作业请使用**pdf**文档格式提交，于**2022年3月31日（星期五）23:59**之前在OJ系统上提交，并将作业命名为“**学号\_姓名\_密码学第四次作业**”。如“21371234\_张三\_密码学第四次作业”。