密码学第四次作业

1.AES解密结构的优化

(1)

1.

$$\begin{pmatrix} S^{-1}(A_1) & S^{-1}(A_2) & S^{-1}(A_3) & S^{-1}(A_4) \\ S^{-1}(B_1) & S^{-1}(B_2) & S^{-1}(B_3) & S^{-1}(B_4) \\ S^{-1}(C_1) & S^{-1}(C_1) & S^{-1}(C_3) & S^{-1}(C_4) \\ S^{-1}(D_1) & S^{-1}(D_2) & S^{-1}(D_3) & S^{-1}(D_4) \end{pmatrix}$$

2.

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ B_2 & B_3 & B_4 & B_1 \\ C_3 & C_4 & C_1 & C_2 \\ D_4 & D_1 & D_2 & D_3 \end{pmatrix}$$

(2)

1.

$$\begin{pmatrix} k_0 \\ k_1 \\ k_2 \\ k_3 \end{pmatrix}$$

2.

$$\begin{pmatrix} y_0 \oplus k_0 \\ y_1 \oplus k_1 \\ y_2 \oplus k_2 \\ y_3 \oplus k_3 \end{pmatrix}$$

3.

$$B \begin{pmatrix} k_0 \\ k_1 \\ k_2 \\ k_3 \end{pmatrix}$$

4.

$$\begin{pmatrix} k_0 \\ k_1 \\ k_2 \\ k_3 \end{pmatrix}$$

2.AES列混淆的推导

(1)

$$A = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

$$B = \begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix}$$

通过矩阵乘法验证

$$A \cdot B = B \cdot A = E$$

(2)

$$a(x) = 03x^3 + 01x^2 + 01x + 02$$

$$b(x) = 0Bx^3 + 0Dx^2 + 09x + 0E$$

在$GF(2^8)$域上，不可约多项式为

$$f(x) = 01x^8 + 01x^4 + 01x^3 + 01x + 01$$

(3)

将其元素看成32位的串，加法就等价于异或操作

(4)

需要模不可约多项式$f(x)$
列混淆时进行乘法模这个**4**次多项式的仅有理由就是为了使运算输出一个**3**次多项式,即

$$x^i \bmod (x^4+1) = g(x), (g(x)\text{的最高次小于等于3次})$$

(5)

6次项系数: $03 \cdot 0B = 1D$
5次项系数: $03 \cdot 0D + 0B \cdot 01 = 1C$
4次项系数: $03 \cdot 09 + 01 \cdot 0B + 01 \cdot 0D = 1D$
3次项系数: $03 \cdot 0E + 02 \cdot 0B + 01 \cdot 09 + 01 \cdot 0D = 00$
2次项系数: $01 \cdot 0E + 02 \cdot 0D + 01 \cdot 09 = 1D$
1次项系数: $01 \cdot 0E + 02 \cdot 09 = 1C$
常数项: $02 \cdot 0E = 1C$

$$c(x) = 1Dx^6 + 1Cx^5 + 1Dx^4 + 00x^3 + 1Dx^2 + 1Cx + 1C$$

$$d(x) = c(x) - 1Dx^2 \cdot f(x) - 1C \cdot f(x) - 1Df(x) = 01$$

3.AES与DES的比较

DES中的元素	实现的效果(扩散/混淆)	AES中的对应元素
f函数的输入与子密钥相异或	混淆	轮密钥加
f函数的输出与分组左边的部分相异或	扩散	列混淆
f函数中的S盒	混淆	S盒
P置换	扩散	行移位
交换一个分组的两半部分	扩散	没有（AES不存在将明文分成两半的举动）