第五章作业

16337341 朱志儒

思考题

5.3 Rijndael 允许块的长度为 128、192 或 256 位，而 AES 仅允许长度为 128 位的块。

5.4 状态数组保存处理过程中每个阶段的 128 位块的中间结果。

5.5 S 盒的的构造：

1) 按字节值的升序逐行初始化 S 盒，在行 y 列 x 的字节值是{yx}；
2) 把 S 盒中的每个字节映射为它在有限域 $GF(2^8)$中的逆，{00}被映射为{00}；
3) 把 S 盒中的每个字节的 8 个构成位记为$(b_0, b_1, b_2, b_3, b_4, b_5, b_6. b_7)$。对 S 盒的每个字节的每个位做变换：$b_i' = b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod8} \oplus b_{(i+7)mod8} \oplus c_i$，其中$(c_7, c_6, c_5, c_4, c_3, c_2, c_1, c_0) = (01100011)$。

5.6 字节替代：字节替代是一个简单的查表操作，将状态数组中每个字节映射为一个新的字节。映射方式：把字节的高 4 位作为行值，低 4 位作为列值，以这些行列值作为索引从 S 盒的对应位置取出元素作为输出。

5.7 行移位变换：状态数组的第一行保持不变，把第二行循环左移一个字节，第三行循环左移两个字节，第四行循环左移三个字节。

5.8 行移位变换影响了状态中的 12 字节。

5.9 列混淆：列混淆对每列独立地进行操作，每列中的每个字节被映射为一个新值，此值由该列中的 4 个字节通过函数变化得到。

5.10 轮密钥加变换：128 位的状态位与 128 位的轮密钥 XOR。

5.11 密钥扩展算法：输入值是 4 个字，输出值是一个 44 个字组成的一维线性数组，输入密钥直接复制到扩展密钥数组的前 4 个字，然后每次使用 4 个字填充扩展密钥数组余下部分。

习题

5.1 证明：因为a(x) × b(x) mod $(x^4+1)=1$，所以b(x) $= a^{-1}(x) mod(x^4+1)$ 成立。

5.2 （a）{01}的逆是{01} （b）{01}在 S 盒中的项为{7C}。

5.3
w(0) = {00 00 00 00}; w(1) = {00 00 00 00}; w(2) = {00 00 00 00};
w(3) = {00 00 00 00}; w(4) = {62 63 63 63}; w(5) = {62 63 63 63};
w(6) = {62 63 63 63}; w(7) = {62 63 63 63}

5.4 （a）

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

（b）

01	05	09	0D
00	04	08	0C
03	07	0B	0F
02	06	0A	0E

（c）

7C	6B	01	D7
63	F2	30	FE
7B	C5	2B	76
77	6F	67	AB

（d）

7C	6B	01	D7
F2	30	FE	63
2B	76	7B	C5
AB	77	6F	67

（e）

75	87	0F	A2
55	E6	04	22
3E	2E	B8	8C
10	15	58	0A

5.6（a）轮密钥加（b）列混淆（c）字节替代（d）行位移变换（e）不需要该元素，因为列混淆使列中的每个字节改变了列中其他每个字节，就不需要交换行；行位移变换将字节从一列移动到另一列，就不用交换列。

5.10 扩展密钥数组：W0 = 1010 0111；W1 = 0011 1011；W2 = 0001 1100；W3 = 0010 0111；W4 = 0111 0110；W5 = 0101 0001。

第 0 轮：

轮密钥加：1100 1000 0101 0000

第一轮：

字节替代：1100 0110 0001 1001

行移位：1100 1001 0001 0110

列混淆：1110 1100 1010 0010

轮密钥加：1110 1100 1010 0010

第 2 轮：

字节替代：1111 0000 1000 0101

行位移：0111 0001 0110 1001

轮密钥加：0000 0111 0011 1000

密文：0000 0111 0011 1000