**第一章**

1.1，1.4

**第二章**

2.2，2.3，2.5，2.6

**第四章**

4.15，4.19

**DES密码算法**

假设明文和密钥有相同的位模式，即：

用十六进制表示：0 1 2 3 4 5 6 7 8 9 A B C D E F

用二进制表示： 0000 0001 0010 0011 0100 0101 0110 0111

1000 1001 1010 1011 1100 1101 1110 1111

1）推导第一轮的子密钥K1

2）推导L0，R0

3）扩展R0求E[R0]

4）计算A= E[R0]^ K1

5）把上题的48位结果分为6位的集合并求对应S盒代换的值

6）利用上题的结论求32位的结果B

7）应用置换求P(B)

8）计算R1=P(B)^ L0

9）写出密文