## **第3章 分组密码**

**1．简单画出一般分组密码算法的原理图，并解释其基本工作原理。**

答案：

 分组密码处理的单位是一组明文，即将明文消息编码后的数字序列划分成为位的组，各个长为的分组分别在密钥（密钥长为*t*）的控制下变换成与明文组等长的一组密文输出数字序列。

通常为64或128，解密过程与加密过程相似。

**2．简述分组密码的设计准则。**

答案：分组密码的设计准则主要包括*S*盒带环的设计准则、*P*置换的设计准则、轮迭代函数*F*的设计准则、迭代的轮数以及子密钥的生成方法。遵循明文与密文的扩散和明文与密钥的混淆。

**3．什么是分组密码的操作模式？主要的分组密码操作模式有哪些？其工作原理是什么？各有何特点？**

答案：通常，分组密码算法（如典型的DES）是提供数据安全的一个基本构件，它以固定长度的分组作为基本的处理单位。

分组密码的操作模式就是如何在各种各样的应用中使用这些基本构件。主要有ECB、CBC、OFB、CFB 、CTR等五种分组密码操作模式。

（具体原理及特点参见教材。）

**4．在8位的CFB模式中，若传输中一个密文字符发生了一位错误，这个错误将会造成多大的影响？**

答案：9个明文字符受影响。因为除了与密文字符相对应的一个明文字符受影响外，受影响的该明文字符进入移位寄存器，直到接下来的8个字符处理完毕后才移出。

**5．描述DES的加密思想和*F*函数？**

答案：DES算法的加密过程经过了三个阶段：首先，64位的明文在一个初始置换IP 后，比特重排产生了经过置换的输入，明文组被分成右半部分和左半部分，每部分32位，以和表示。接下来的阶段是由对同一个函数进行16次循环组成的，16轮迭代称为乘积变换或函数，这个函数本身既包含有换位又包含有代替函数，将数据和密钥结合起来，最后1轮的输出由64位组成，其左边和右边两个部分经过交换后就得到预输出。最后阶段，预输出通过一个逆初始置换IP-1算法就生成了64位的密文结果。

*F*函数的变换如下图所示。



**6．为什么要推行使用3DES？**

答案：随着计算机处理能力的提高，只有56位密钥长度的DES算法不再被认为是安全的。因此DES需要替代者，其中一个可替代的方案是使用3DES。3DES的优点：

（1）密钥长度增加到112位或168位，可以有效克服DES面临的穷举搜索攻击；

（2）相对于DES，增强了抗差分分析和线性分析的能力；

（3）具备继续使用现有的DES实现的可能。

**7．AES的主要优点是什么？基本变换有哪些？**

答案：AES的主要优点表现为：汇聚了安全性能、效率、可实现性和灵活性等优点，最大的优点是可以给出算法的最佳差分特征的概率，并分析算法抵抗差分密码分析及线性密码分析的能力。AES对内存的需求非常低，也使它很适合用于受限制的环境中，AES的操作简单，并可抵御强大和实时的攻击。AES的基本变换包括三个代替和一个混淆：

（1）字节代替SubBytes：用一个S盒完成分组中的按字节的代替

（2）行移位ShiftRows：一个简单的置换；

（3）列混淆MixColumns：一个利用在域*GF*（28）上的算术特性的代替；

（4）轮密钥加AddRoundKey：一个利用当前分组和扩展密钥的一部分进行按位异或。

**8．AES的解密算法和AES的逆算法之间有何不同？**

答案：AES的逆算法是相对加密过程中基本变换而言的，即存在InvSubBytes、InvShiftRows、InvMixColumns变换。

AES的解密算法是相对于加密算法而言的，它由InvSubBytes、InvShiftRows、InvMixColumns和AddRoundKey等基本变换构成。

**9．设，设*g*是*S*上的一个置换，若存在一个元素，使得，则称*x*是*g*的一个不动点，计算*S*上具有不动点的置换个数？**

答案：这里用到了一个错排问题：如10本不同的书放在书架上重新摆放，使每本书都不在原来放的位置，有几种摆法？

推广一下得：*n*个有序的元素应有*n*！中不同排列，错排的种数为，错排公式。

根据并集的概率公式得：*S*上具有不动点的置换个数为：

。

**10．证明在DES中，如果，则，其中表示的逐位取反？**

答案：

证明一：（1）因为种子密钥*k*先经过PC-1置换后被按顺序分成左右28bit的*C*0和*D*0，做循环移位后得到*C*1和*D*1，然后经过PC-2置换得到子密钥*ki*，由这个过程得：DES的密钥扩展算法没有任何乘法等扩展运算，仅仅是交换各比特的位置。即。

（2），非线性函数为为第*i*轮子密钥，则有。

（3）加密，也就是每一轮加密结果和正好逐位取反，所以最后密文。

综上所述可以证明结论成立。

证明二：1.若以为主密钥扩展的16个加密子密钥记为，则以为主密钥扩展的16个加密子密钥记为；

2.注意到，不难得出

3.注意到，不难得出

也就是每一轮加密结果和正好逐位取反，所以最后密文。

综上所述可以证明结论成立。

**11．在已知两个明文块以及与之对应的密文的情况下，计算利用中途相遇攻击成功的找到双重的DES的正确密钥的概率？**

答案：设已知DES加密下的两个明文块为及其所对应的密文块为，



我们先分别对明文密文进行解密，然后找的对，设集合且。然后我们利用逐一验证是否等于，，因为成功的密钥只有一对，所以用中途相遇攻击找到DES的正确概率为。

**12．DES中某S盒定义如下，对于输入，做为行号，做为列号查找输出。请求出当输入分别是（101010）、（100010）时的输出？**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S1: | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
|  | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
|  | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
|  | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |
| S2: | 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
|  | 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
|  | 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
|  | 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |
| S3: | 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
|  | 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 13 | 11 | 15 | 1 |
|  | 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
|  | 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |
| S4: | 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
|  | 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
|  | 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
|  | 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |
| S5: | 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
|  | 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
|  | 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
|  | 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |
| S6: | 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
|  | 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
|  | 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
|  | 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |
| S7: | 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
|  | 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
|  | 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
|  | 6 | 11 | 12 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |
| S8: | 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
|  | 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
|  | 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
|  | 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

答案：输入为：101010 输出为6 即0110。

输入为：100010 输出为1 即0001。

**13．DES中某S盒定义如上，请求出当输出是（1010）、（0010）（二进制表示）可能的输入？**

答案：输出是（1010）即10，输入可能为（010010）（010001）（111010）（111001）。

输出是（0010）即2，输入可能为（001000）（001011）（101100）（100111）。

**14．在AES分组密码算法中，字节代替变换SubBytes()将状态中的每个字节按下述方法变换为另一个字节。**

**（1）将每个字节等同于有限域**

****

**中的元素，在这一等同下，将变换为该有限域中的乘 法逆元素，规定00变换为其自身00；**

**（2）对（1）的结果在上做仿射变换：**

**，**

**求字节0x4E=00101110经SubBytes()变换后的值。**

答案：

首先，根据有限域上扩展欧几里得算法求关于0x4E的逆元。将0x4E表示为，

则有，可知其逆为，写作16进制为0xE9。

其次，根据上述代换公式，对0xE9进行变换。



即输出结果为00101111。

**15．在AES中，设为系数在*GF*（28）中的两个多项式，计算？**

答案：

**16．在AES列混合变换MixColumns中，**

=，

已知：=，求（*tij*）4×4 ？

答案：

=

=

**17.在中，对，把其中的任意元素与1字节数据（可用两位十六进制数表示）等同，试给出相应的计算的公式，并计算？**

答案：。



所以。