**密码学第三次作业参考答案**

**1.**【理想分组密码】

对于位分组长度的理想分组密码：

（1）试证明其不同可逆映射个数为个。

（2）根据教材4.1.2节，若允许所有可逆映射，则密钥的长度应为位，但密钥空间要小于，试解释原因。

（3）其密钥空间为，也就是说，可以用位对应到唯一一个可逆映射上，试简要解释这样的对应方法。

（4）【选做】现有映射如下，取，，试分别用位密钥和位密钥表示它。对比结果，你有哪些思考？

|  |  |  |  |
| --- | --- | --- | --- |
| 原像 | 像 | 原像 | 像 |
| 0 | 3 | 5 | 1 |
| 1 | 6 | 6 | 4 |
| 2 | 5 | 7 | 9 |
| 3 | 8 | 8 | 0 |
| 4 | 7 | 9 | 2 |

提示：对于第二种表示方法，不妨给所有可逆映射编号，设0映射到0为第个映射，0映射到1为第个映射，以此类推，求取10进制下的密钥再转换成二进制。

（1）𝑛位分组长度的理想分组密码，其可能的明密文有种，映射是明文对密文的一一对应关系，数量上等于密文的排列数，总共有个。从另一个角度考虑，就像单表代替密码一样，映射最高位时共有种情况，映射次高位时只要不选择之前映射过的即可，因此有种可能，以此类推映射倒数第二位1时共有2个选项，最后映射最低位0时只剩下唯一的结果，将各个值相乘，所得结果为。

（2） 位的表示出的绝大部分映射都不是可逆的，是不能被选择为密钥的。真正的密钥个数只有个。

（3）对所有可逆映射以一定规则从0开始进行编号，由于密钥空间（可逆映射个数）总共为，因此可用位二进制数表示。

（4）第一种表示方法：0011 0110 0101 1000 0111 0001 0100 1001 0000 0010（后面可进行填充）；第二种表示方法：首先按照提示计算该映射的编号，转化为二进制为01 0100 0000 1110 1101 1000。思考：第二种表示方法在通信或存储时占用资源较少。

**2.**【Feistel结构】

（1）证明Fesitel密码的解密算法是加密算法的逆。

（2）考虑分组长度为128位，密钥长度位128位的16轮Fesitel密码，假设对于给定的，始终满足。试对于给定的密文，向加密Oracle（加密预言机，可以简单的理解为输入，返回）做一次询问，解密得到。

（3）假设某Fesitel密码的F盒与密钥无关，对于输入的串R，F盒总是将其映射为：

i. 等长的全1串；

ii. R的按位补。

试回答：上面两种映射方法，分别会对加密造成上面样的影响？对于每种映射方式，我们又应该去如何解密密文？

（1）首先确定IP置换及其逆置换起到了求逆的作用：设加密结果为*c*，根据Fesitel流程图，，进行解密运算时，首先进行IP置换，，可见IP置换及其逆置换实现了解密是加密的逆。接下来分析迭代部分：Feistel结构的轮迭代依托于这样的变换结构：。由于异或具有的重要性质，因此调换输入后有即，上式为反求所得，下式利用了异或的性质。可见对于任一轮迭代，都有。经过16轮迭代后，有，因此DES解密算法是加密算法的逆。

（2）对于Fesitel结构的解密，只需要向加密结构中输入密文，然后倒序的输入16个轮密钥，根据的原理就可以获得明文。由于题设,因此倒序输入密钥与正序输入密钥没有差别，所以只需要令oracle将密文c视为原文进行加密，所得到的密文即为之前的明文。

（3）若替换成等长的全 1 串，那么轮迭代的结果为，即的结果为的按位取反。给定输出如下：

以此类推，可以看出上述加密以四轮为一个循环，每四轮又会回到初始状态。

ii) 若替换成按位补，那么轮迭代的结果为，即。给定输出如下：

以此类推，可以看出上述加密以三轮为一个循环，每三轮又会回到初始状态。

**3.**【扩散与混淆】

（1）扩散与混淆的区别是什么？

（2）古典密码的代替与置换一般为\_\_\_\_运算。而在现代的分组密码设计中，\_\_\_\_多为非线性运算，主要用于实现\_\_\_\_；\_\_\_\_仍为线性运算，主要用于实现\_\_\_\_。

A.线性 B.非线性 C.代替 D.置换 E.扩散 F.混淆

（3）请指出扩散与混淆在DES中的具体体现。

（4）【选做】对于现代的分组密码，它的非线性对安全是至关重要的。假设某分组密码，加密位明文分组为位密文分组，若该加密始终满足线性关系。试通过选择密文攻击，构造个选择密文（即查询解密Oracle 次，获得个明密文对），完成对任何密文的破译。

（1）扩散：使明文与密文间的统计关系变得复杂，减少密文中明文的统计特性。混淆：使密钥与密文间的统计关系复杂，阻止攻击者发现密钥。

（2）ACFDE

（3）扩散：初始置换（IP置换），P置换（P盒），扩展置换（E盒）。混淆：S盒。[此外，Fesitel本身的结构可以看作弱的扩散；密钥白化的过程可以看作混淆（异或本身是线性运算，但被用来处理密钥，且密钥外的另一个输入从第二轮迭代起是非线性运算得到的）]

（4）1.令，易知：，该方法对全0输入的加密是平凡的。2.选择密文攻击[只要选择的128个密文组成的方阵满秩即可]：选择第个密文为，获得128个明密文对满足。需要解密新消息时，只要根据密文中为1的位，寻找到对应的，令它们异或即可得到结果。

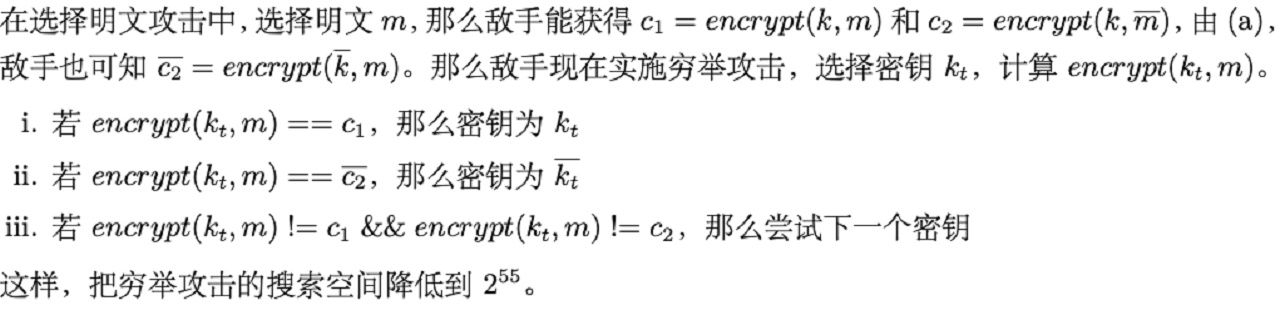
**4.**【DES算法】

（1）DES的密钥输入为\_\_\_\_位，密钥空间为\_\_\_\_，其原因为何？

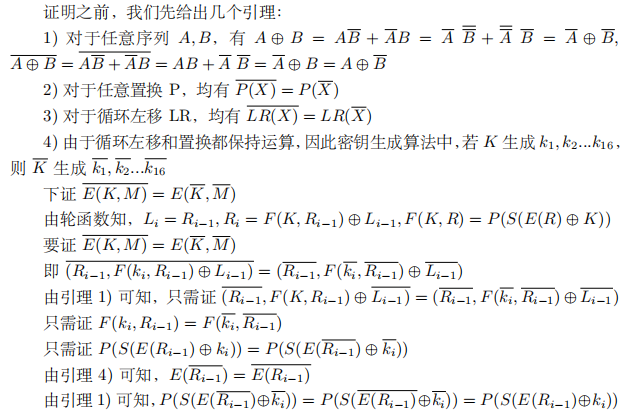
（2）证明：对于DES算法，若明文和密钥都取反，则密文也取反。因此，对DES的穷举攻击实际搜索的密钥个数不是个而是\_\_\_\_个。

（3）证明：DES中每个子密钥的前24位均来自于初始密钥的同一个子集，后24位来自于该子集的补集。两集合均有28位。

（1），原因：有8位是奇偶校验位。

（2）[已知明文攻击（因为每个密钥要计算两次，所以是否降低穷举空间存疑）：已知明密文对，，取反得到，，有。穷举攻击选取，计算和。若，则认为；若。，则认为，即。以此法可以不再测试已穷举密钥取反的情况。选择明文攻击：]

证明示例如下图所示。



（3）初始密钥经过PC-1置换后的前28位和后28位所对应的初始密钥的位数分别构成这两个子集。也就是初始密钥的：[1,2,3,9,10,11,17,18,19,25,26,27,33,34,35,36,41,42,43,44,49,50,51,52,57,58,59,60]位和[4,5,6,7,12,13,14,15,20,21,21,23,28,29,30,31,37,38,39,45,46,47,53,54,55,61,62,63]位。DES的密钥扩展算法是这左右28位分别左移变化的，彼此互不相干；进行PC-2置换生成子密钥时，根据PC-2的对应关系，也是前28位压缩成前24位，后28位压缩成后24位，互不相干。因此原命题得证。

**5.**【DES算法】

本题给出了用一轮DES加密具体数值的例子。假设初始时明文和密钥K相同，其表示如下所示。

用16进制表示为：0 1 2 3 4 5 6 7 8 9 A B C D E F

用2进制表示为：0000 0001 0010 0011 0100 0101 0110 0111

1000 1001 1010 1011 1100 1101 1110 1111

1. 推导第一轮的子秘钥
2. 推导和
3. 扩展得到
4. 计算
5. 把4)中的48位结果分成6位一组的集合，求出对应S盒代替的值
6. 利用5)中得到的结果得到32位结果B
7. 利用置换得到
8. 计算
9. 写出密文

(Tip：建议本题使用程序辅助计算）

1. 首先根据PC-1将64位初始密钥转换为56位，然后将左右28位分别左循环移一位，最后根据PC-2将56位置换选择为48位，即

写成十六进制表达为：0 B 0 2 6 7 9 B 4 9 A 5

写成二进制表达为：0000 1011 0000 0010 0110 0111

1001 1011 0100 1001 1010 0101

1. 和是64位明文经过IP变换后得到的，其结果为
2. 将经过扩展，得到48位结果为

1. 取每6比特的首位和末位构成的二进制数为行号，中间四位构成的二进制数为列号，得到结果如下：
2. 32位结果
3. 对输出的32位结果进行行变换，得到

则此时的密文为

经过16轮加密后，最终密文结果为

**6.**概念题

6.1分组密码主要采用扩散和混淆来抵抗攻击者的统计分析。

6.2 雪崩效应是指当输入发生最微小的改变时，也会导致输出的不可区分性改变

6.3 DES的轮函数F是由三个部分： 扩展置换 、非线性代换 和 线性置换 组成的。

**注意：**

以上作业请使用**pdf**文档格式提交，于**2022年4月3日（星期日）23:59**之前在OJ系统上提交，并将作业命名为“**学号\_姓名\_密码学第三次作业**”。如“20371234\_张三\_密码学第三次作业”。