**密码学第三次作业**

**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。

**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？

**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。

**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。

**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）

**注意：**

以上作业请使用**pdf**文档格式提交，于**2022年3月24日（星期五）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“21371234\_张三\_密码学第三次作业”。