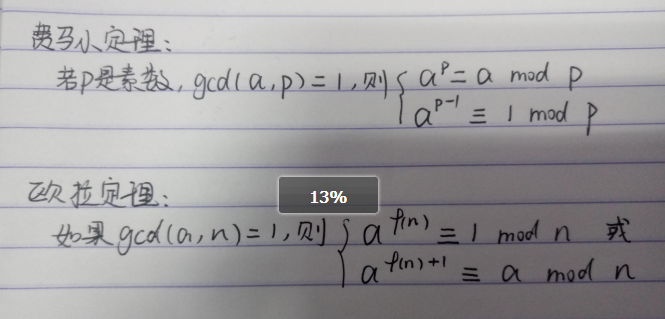
填空题：

1. 被加密的消息称为\_\_\_密文\_\_\_\_\_\_
2. 使消息保密的技术和科学叫做\_\_密码编码学\_\_\_\_
3. 现代密码学中一种重要的假设就是kerckhoffs原则：在评估一个密码系统的安全性时，必须假设敌方知道所用的\_\_算法\_\_\_\_\_\_
4. 对加密信息的攻击主要有5种类型：\_\_唯密文攻击\_\_\_\_\_\_\_\_，已知明文攻击，选择明文攻击，选择密文攻击，选择文本攻击。
5. 基于密钥的算法通常有两类：\_对称算法\_\_\_\_\_\_\_\_和公开密钥算法。
6. 密码学中有两种类型的鉴别\_\_\_实体鉴别\_\_\_\_\_\_\_\_\_和数据源鉴别。
7. \_\_\_数字签名\_\_\_\_\_\_\_\_\_\_可以实现消息的不可否认性。
8. 扩散和\_\_混乱\_\_\_\_\_\_\_\_正是抓住了设计分组密码的本质而成为现代分组密码设计的里程碑。
9. cryptalogy是指对不安全信道上的通信及相关问题的研究，而设计能够进行这种通信的密码系统的过程则称为\_\_\_\_\_\_\_\_\_\_\_\_\_,cryptanalysis所处理的问题是破译这种密码系统。
10. \_\_隐写术\_\_\_\_\_\_\_\_是将秘密消息隐藏在其他消息中。

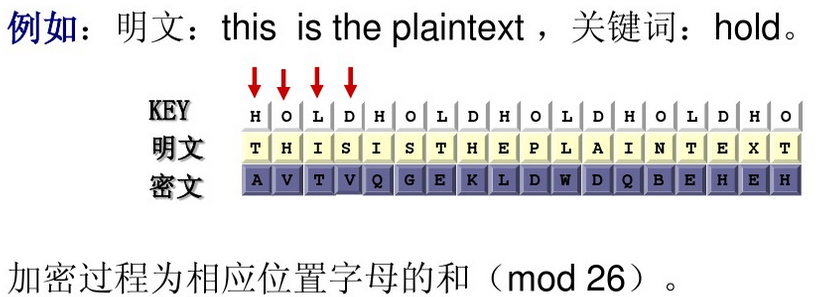
名词解释：

1. 单向散列函数：把可变长度输入转换为固定长度输出且不可逆的一种函数。
2. 查分分析与线性分析的区别：查分密码分析是一项技术，特别是差异模式的选择明文被加密，差异所产生的的密文的模式提供信息，可以用来确定加密密钥。

线性密码分析的基础上寻找线性近似描述块密码进行转换。

1. 写出费马小定理：
2. 欧拉定理 ：
3. 分组密码和流密码的差别是什么：分组密码一次处理一个数据组，而流密码则是以一个元素（一个字母或一个比特）为基本处理单元产生形同长度的输出。

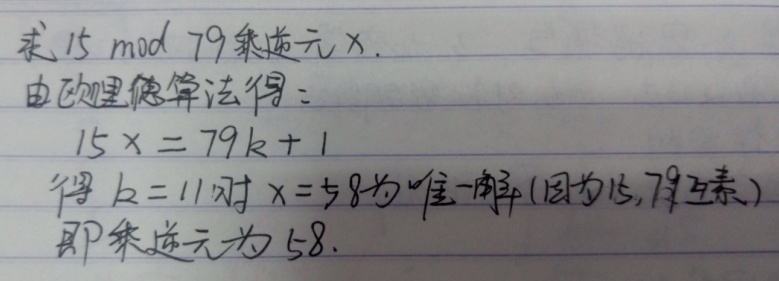
计算题：1、用Vigenere密码加密单词“I love you”，密钥为leg



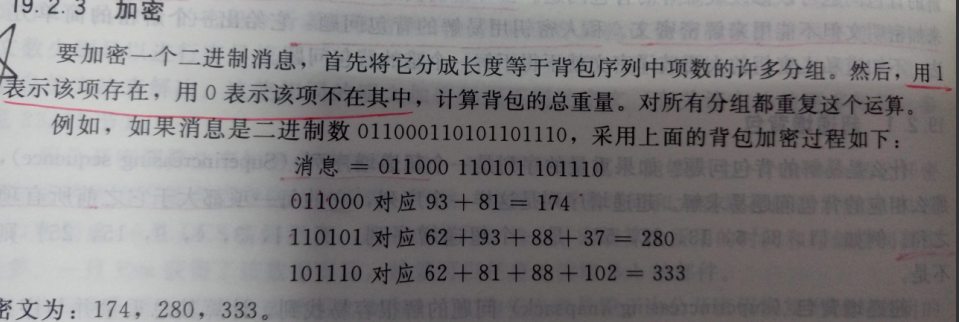


T pugi ezz

1. 用扩展欧几里德算法求15 mod 79乘逆元



3、已知消息是二进制数011000110101101110，背包序列是{ 62，93,81,88,102,37 } ，求用背包加密的密文是什么。



4、用户A和B使用Diffie-Hellman密钥交换技术来交换密钥，设公用素数q=71,本原根a=7

若用户A的私钥XA=5，则A的公钥YA为多少？Ya=7~5 mod 71 =51

若用户B的私钥XB=12，则B的公钥YB为多少？Yb=7~12 mod 71=4

共享的密钥为多少？K=7~(5\*12) mod 71 = 62

5.希尔密码

假设在AES中第0轮的密钥的128位全都是0

求：在第一轮的轮密钥是w(4) w(5) w(6)w(7)

问答题：

1. 协议的特点有哪些:
2. 协议中的每个人都必须了解协议，并且预先知道所要完成的所有步骤。
3. 每个人都必须统一并遵循它。
4. 协议必须是清楚的，每一步必须明确定义，并且不会引起误解。
5. 协议必须是完整的，对每种可能的情况必须规定具体的动作。
6. 公钥密码体制的主要成分是什么：

明文，加密算法，公钥和私钥，密文，解密算法

1. 说说保密选举至少要有什么样的六项要求：
2. 只有授权的投票者才能投票。
3. 每个人投票不得超过一次。
4. 任何人都不能确定别人投谁的票。
5. 没有人能复制其他人的选票。
6. 没有人能修改其他人的选票而不被发现。
7. 每个投票者都可以保证他的选票在最后的表中被计算在内。
8. 安全hash函数需要具体哪些特征：
9. 伪装：插入到网络欺诈来源的信息。
10. 内容修改：更改消息的内容，包括插入，删除，换位和修改。
11. 修改序列：各方之间的消息，包括插入，删除和重新排序的序列的任何修改。
12. 定时修改：延误或重播消息。
13. 写出由Ron Rivest和Adi Shamir 发明的连锁协议的七个工作过程：（1）A将他的公开密钥传送给B；
14. B将他的公开密钥传送给A；
15. A用B的公开密钥加密他的消息，并将加密消息的一半给B；
16. B用A的公开密钥加密他的消息，并将加密消息的一半给A；
17. A将加密消息的另一半给B ；
18. B将A的两半消息合在一起，并用他的私人密钥解密；B将他加密消息的另一半给A；
19. A将B的两半消息合在一起，并用他的私人密钥解密。
20. 写出DES算法的三个步骤；
21. 变换明文
22. 按照规则迭代
23. 用IP~（-1）做逆置换。

证明题：

若p是素数，则证明Φ（pi）=pi-pi-1