**密码学实验一实验报告**

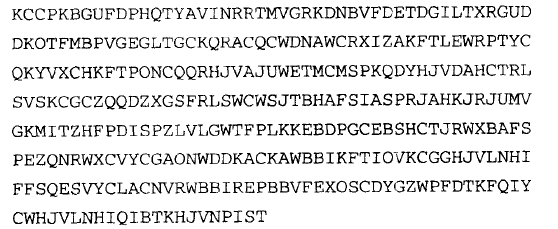
姓名：孟衍璋 学号：16337183

1. **实验目的**

通过实验掌握维吉尼亚密码、希尔密码算法及其分析，加深对其理解。

1. **实验内容**
2. **题目一：**

已知一段密文是由维吉尼亚密码加密而成，需要从密文确定明文。并给出详细的分析过程。



1. **题目二：**

仿射希尔密码是由希尔密码按照以下方式修改得到的：设m是正整数，定义P = C = (Z26)m，密钥由（L，b）组成，L是定义在Z26上的可逆矩阵，b∈（Z26）m。对任意的x = (x1,x2,…,xm)属于P和K = (L,b)∈k，定义y = eK(x) = (y1,y2,…,ym)是y = xL+b。

假设敌手Oscar知道明文：adisplayedequation

被加密成以下密文：DSRMSIOPLXLJBZULLM

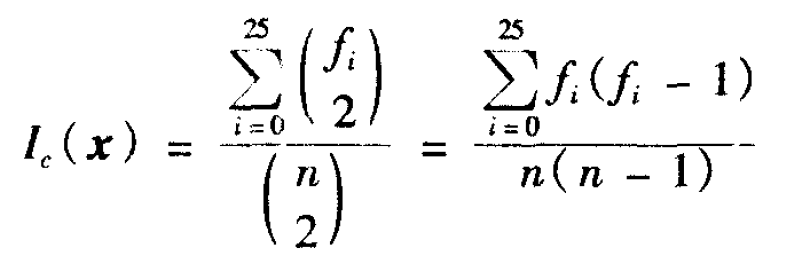
并且Oscar知道m = 3。试求出密钥，要求给出详细过程。

1. **实验及算法原理**
2. **题目一：维吉尼亚密码分析**

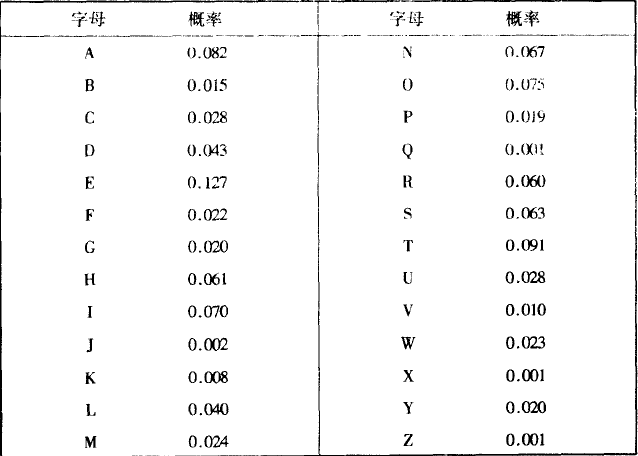
首先，想要分析维吉尼亚密码，需要得到密钥的长度m。有两种方法可以分析确定密钥的长度：Kasiski测试法和重合指数法。我们这里使用重合指数法计算密钥的长度。

我们需要知道重合指数的定义：设x = x1x2…xn是一条n个字母的串，x的重合指数记为Ic(x)，是x中两个随机元素相同的概率。

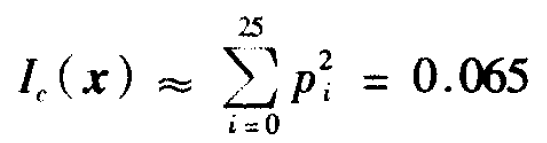
计算字符串x的重合指数，需要知道各个字母在其中出现的频数fi（0≤i≤25）。重合指数计算公式如下：



在人类的自然语言中，用英文字母组成单词进而组成文章时，英文字母并非等概率出现，而且英文字母之间有一定的依赖关系。对英文书中各个字母出现的概率进行统计，可以得到以下的概率分布表：



因此，一篇英文文章，按照上表给出的概率，其中各个字母出现的概率为pi（0≤i≤25），计算重合指数得到：

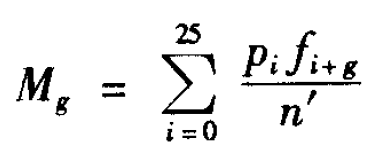


即使对此篇英文文章用移位密码进行加密，此时各个概率将会置换，但是计算出的重合指数不会改变，应该大约为0.065。

现在我们回到分析用维吉尼亚密码加密的密文的问题上，用维吉尼亚密码加密实际上就是用了m个移位密码加密。每隔m位取一个字符，得到的子串就是明文使用移位密码加密的结果。所以如果计算这些子串的重合指数，应该与上述自然语言中的重合指数大致相同，大约为0.065。

所以便可以开始计算，从m = 1开始叠加，计算各个子串的重合指数，当发现计算出的值与0.065相差无几，便可以得到密钥的长度m。

现在终于计算出了密钥的长度，就要进一步分析得到密钥。思路是把原密文分成上述的m个子串，各自分析。假设在子串yi（0≤i≤25）中，各个字母出现的频数为fi（0≤i≤25），令g为使用移位密码的法则时移动的位数，计算：



其中pi为自然语言中各个字母出现的概率。

如果g的值是正确的，那么Mg的值应该大约等于0.065。

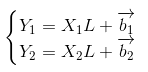
计算出每个子串对应的g的值，便可以确定每个子串使用移位密码法则时移动的位数，进而就能确定密钥的值。

1. **题目二：仿射希尔密码分析**

仿射希尔密码相比于希尔密码而言，增加了向量b的偏移量，即对应于如下的计算公式：



题目信息告诉我们m = 3，因此将明文段与密文段分别分成两个3×3的矩阵，得到如下关系式：



将两式相减，得到：



再计算：

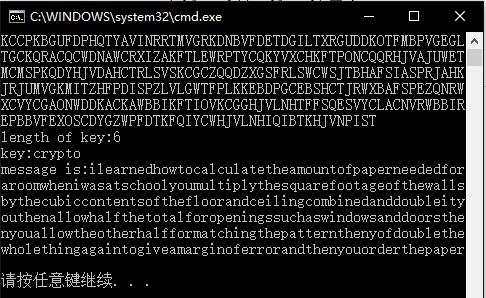


就可以得到密钥L，再将L代入之前的式子计算出。

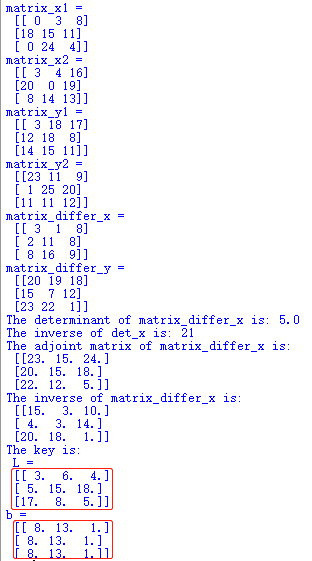
1. **程序清单**



1. **运行截图**
2. **题目一**



1. **题目二**



1. **结果分析**
2. **题目一**

在维吉尼亚密码分析的代码文件中，有三个主要的函数：Keylenth()、Key()、decode()。分别用来计算密钥长度、计算密钥、用密钥恢复明文。

在Keylenth()函数中，先计算每个子串的重合指数，再求出这些值的平均值，如果求得的平均值大于或者等于0.06，就认为其是符合标准的。在本题中，计算出密钥长度为6。

在Key()函数中，将密文段分为6个子串，分别带入不同的g值，验证上述提到的Mg的值，如果其值大于0.055，便认为找到了正确的偏移量。最后将这些偏移量整合起来，对应到字母空间，得到密钥。

剩下的decode()函数，便是根据维吉尼亚密码的加密规则，逆推回去得到对应的明文。

根据得到的结果，用计算出的密钥解密，可以得到有意义的文本。可以证明之前的密钥计算正确。

1. **题目二**

仿射希尔密码分析的文件选择用python书写。先是将对应的明文段与密文段存储进字符串中，再化为对应的数字存储进list中。再按照9个数字一组，构造4个3×3的矩阵，这其中用到了numpy的reshape方法。之后将对应的矩阵做差，由于我们的运算都要在Z26上进行，所以定义了Mod26()函数将矩阵中的每一个数都做模26的运算处理。

之后按照书上的方法计算矩阵的逆，先算出矩阵的行列式（模26条件下），再算出其模26的逆。再定义findAdjointMatrix()函数计算矩阵的伴随矩阵。之后根据求出矩阵的逆。

计算出了矩阵的逆之后，再用一个矩阵乘法的操作便可以得到密钥L。再将L代回原式便能得到密钥b。

1. **总结**

刚开始拿到这个实验，对于分析维吉尼亚密码思路并不是很清晰，于是首先将书上关于维吉尼亚密码分析的内容看了几遍，再结合网上搜索得到的信息，理解了用重合指数法分析出密钥的过程。对于仿射希尔密码的题目，通读了几次之后，在草稿纸上写下了的式子，思路便很明确了，重点就是要实现在模26的条件下求逆的过程，我采用了书上的方法，先计算出了行列式的逆，再算出伴随矩阵，相乘得到矩阵的逆。

想要完成这次实验，首先要理解维吉尼亚密码与希尔密码的加密机制。其次要懂得如何用重合指数法分析出用维吉尼亚密码加密而成的密文的密钥的长度，再进一步得到密钥。而仿射希尔密码的题目，则需要对矩阵的运算比较熟悉。

在刚开始做仿射希尔密码的分析的时候，本来是用的C++语言，但由于有些繁琐，且忘了考虑是在模26的情形下。于是决定改用python语言，在编写的过程中，搜索了numpy中关于矩阵的函数的用法，摸索着完成了分析仿射希尔密码的代码。

这次实验加深了我对维吉尼亚密码和希尔密码的理解，并明白了分析它们的方法。也对古典密码的体系有了更全面的认识。在编写仿射希尔密码分析的代码的时候，也增加了对python语言的熟悉度。总之收获颇丰。