南京信息工程大学 实验（实习）报告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 日期 |  | 得分 |  | 指导教师 |  |
| 班级 |  | 学号 |  | 姓名 |  |

单表密码实现与分析

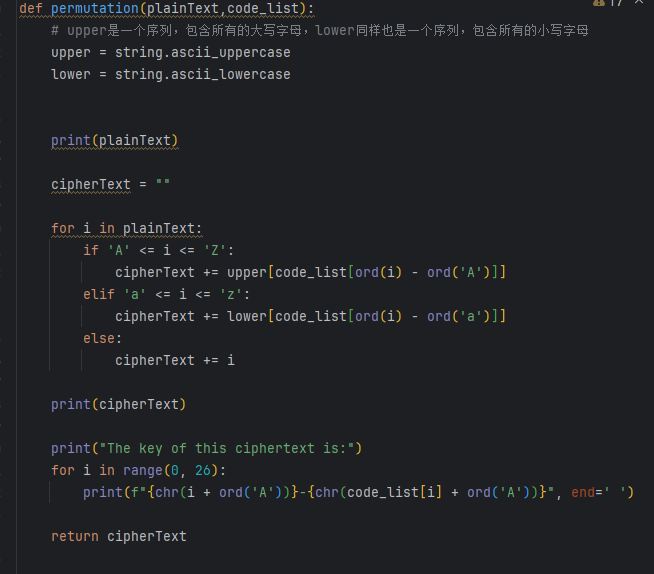
1．实验目的：

1. 掌握单表密码加密算法；
2. 掌握单表密码常见的攻击方法。

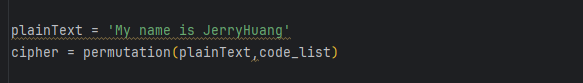
2．实验内容：

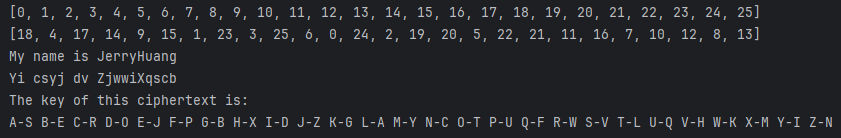
1. 实现单表密码的加解密算法对英文文本进行加密；
2. 统计明文和密文文本字母出现概率，对单表密码进行攻击分析，用实际的数据来说明问题。
3. 实验步骤
4. 单表密码的实现

代码实现：



代码实验部分及输出





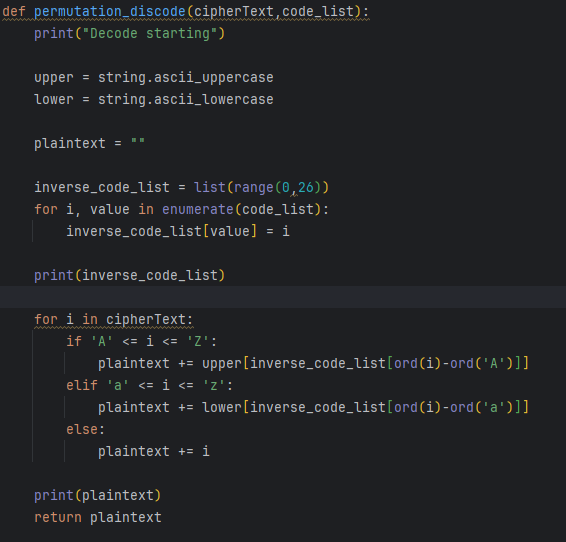
明文为：“My name is JerryHuang”

输出的密文为：“Yi csyj dv ZjwwiXqscb”

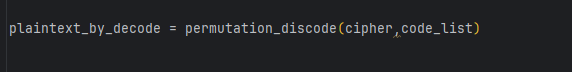
对照关系为：“A-S B-E C-R D-O E-J F-P G-B H-X I-D J-Z K-G L-A M-Y N-C O-T P-U Q-F R-W S-V T-L U-Q V-H W-K X-M Y-I Z-N”

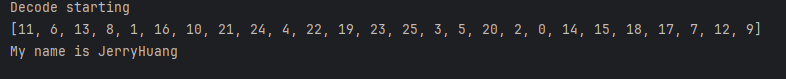
1. 单表密码的解密

代码部分：



代码实验及输出：





这部分代码把上面加密方法返回的密文和相同的密码本作为输入，首先会把密码本和字母的初始位置进行对照，找到密文对用的原文，最后输出原先的明文。

这段代码成功输出一开始的明文：“My name is JerryHuang”。

1. 实验分析和总结
2. 单表密码

单表密码的实现是通过字母的位移和变换来实现的，最简单的凯撒密码就是通过字母的移位来实现，比如把字母向后移动三位，A-D, B-E, C-F....X-A,Y-B, Z-C。但是凯撒密码非常容易被破译，最多只用试26次就可以得到最开始的明文，因此出现了上文所使用的随机单表密码，字母随机排序，并非想最简单的加法单表密码一样进行整体移位，因此大大增加了破译的难度。但是对应密码本需要单独进行生成和传输就像代码中密码本的生成是一个单独的过程，并没有和密文的产生在一起。这样保证了密码生成的依赖性，不会出现无法得到明文的情况。

1. 单表密码的攻击和破解

虽然随机生成的单表密码的保密性要比凯撒密码等加法单表密码的高得多，密钥空间的大小为26！，很难用穷举法暴力破解。但是这个密码也有被破解的可能。

不妨换一下我们要加密的明文，把一句话变为一段话

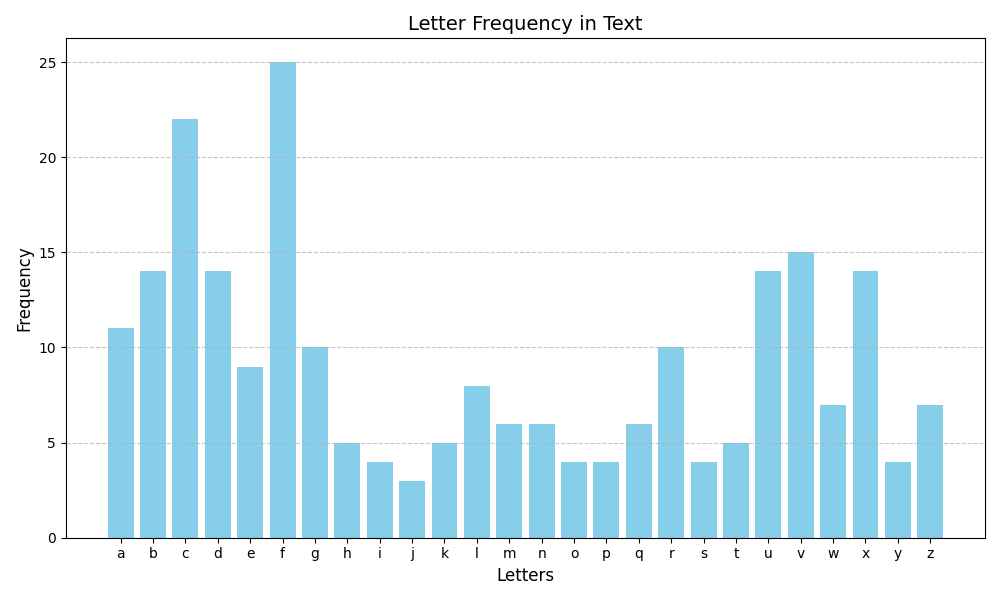
The quick brown fox jumps over a lazy dog while zebras watch quietly from afar. Jack loves quirky vibes and enjoys exploring xylophones in his spare time. Bright sunlight dazzles as he ventures into the lush garden, finding joy in every unique moment. A wizard offered him five juicy kiwis

我们加密后，可以得到这样的密文以及对照表：

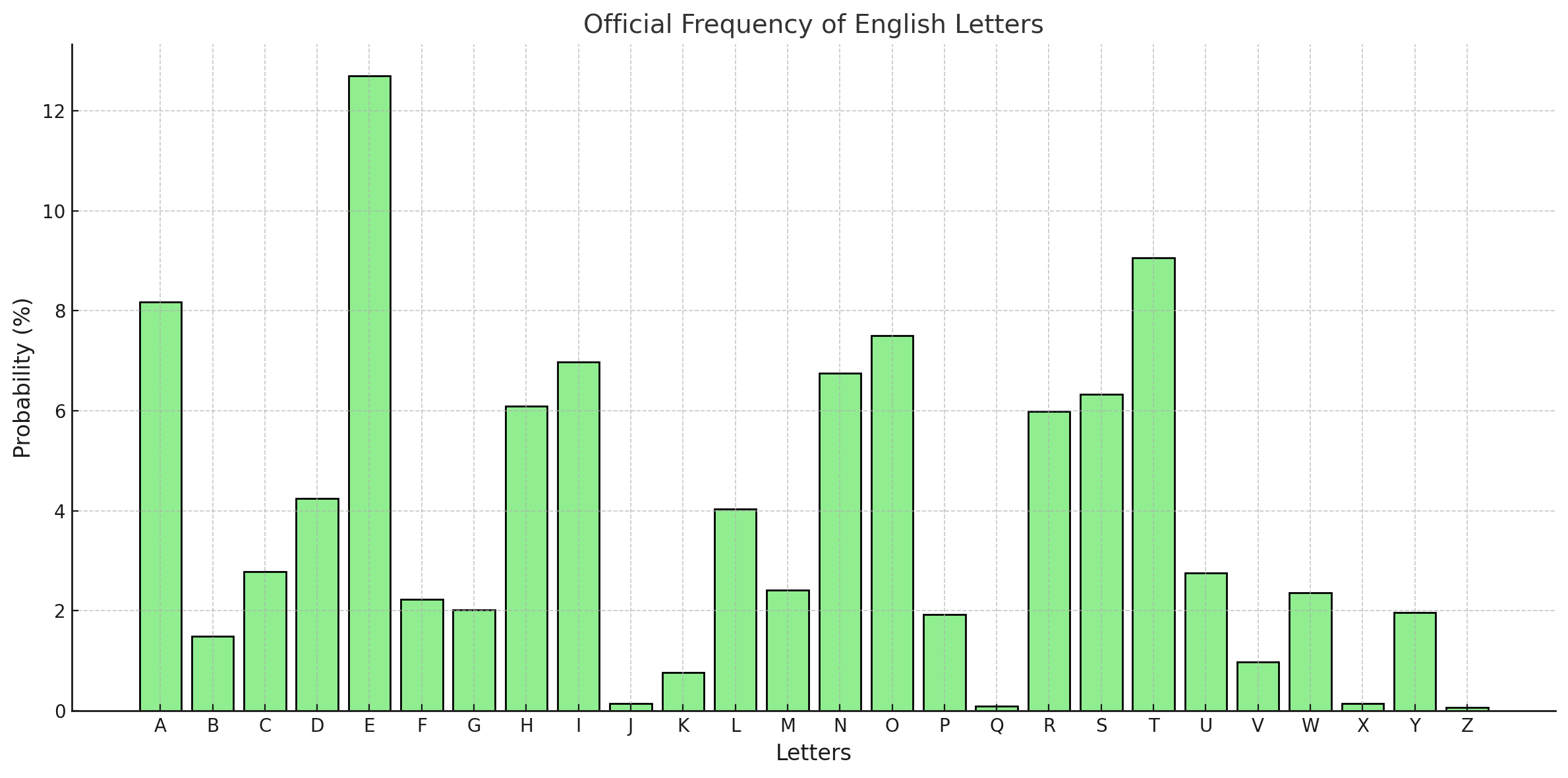
Gaf prcsy oxbkv wbj trmid bnfx u euhl zbq kacef hfoxud kugsa prcfgel wxbm uwux. Tusy ebnfd prcxyl ncofd uvz fvtbld fjiebxcvq jlebiabvfd cv acd diuxf gcmf. Oxcqag drvecqag zuhhefd ud af nfvgrxfd cvgb gaf erda quxzfv, wcvzcvq tbl cv fnfxl rvcprf mbmfvg. U kchuxz bwwfxfz acm wcnf trcsl yckcd.

A-U B-O C-S D-Z E-F F-W G-Q H-A I-C J-T K-Y L-E M-M N-V O-B P-I Q-P R-X S-D T-G U-R V-N W-K X-J Y-L Z-H

通过统计文中每个单词出现的数量，我们可以得到下面这张统计表：



根据官方统计的英文字母出现的概率统计表可知：



从上图可以看出，字母e出现的概率最大，而我们的密文中f字母的出现概率最大，而且根据我们的密码本对照可以发现，字母e对应的正好就是字母f，我们接着看我们密文中出现次数较多的几个字母，它们分别是c、v、x，这几个字母对应的明文字母为，i、n和r，而这几个字母也是出现概率很高的字母。

如果我们要传递的密文的字数继续增加，完全可以通过概率统计的方法把密文破译出来，所以如果我们要传递的密文只是一小段文字，使用这种加密方式完全没问题，但是随着字数的增加，被破译的风险就会增加。