**单表替换密码及其统计分析实验报告**

作者：王乐天

学号：PB22000230

完成时间2024/6/9

**Github地址https://github.com/wlt314/---**

**摘要**:单表替换密码作为古典密码中十分经典的一种，曾经有着广泛的应用，本文就单表替换密码的原理使用python语言实现了单字母频率统计攻击单表替换密码的源程序，同时添加了双字母频率统计攻击作为修改补充。

**成员及分工**： 成员数目：1

成员姓名：王乐天

成员学号：PB22000230

本次实验由本人独立完成，未以组队的形式合作完成，其中不免有疏漏之处，望见谅。

**实验工具：**pycharm

**加解密功能技术实现**

笔者随意生成了一段英文明文: the quick brown fox jumps over the lazy dog near the bank of the river. as the sun sets, the calm water reflects the vibrant hues of twilight. amidst the rustling leaves, a gentle breeze whispers through the valley, carrying with it the sweet scent of blooming flowers.

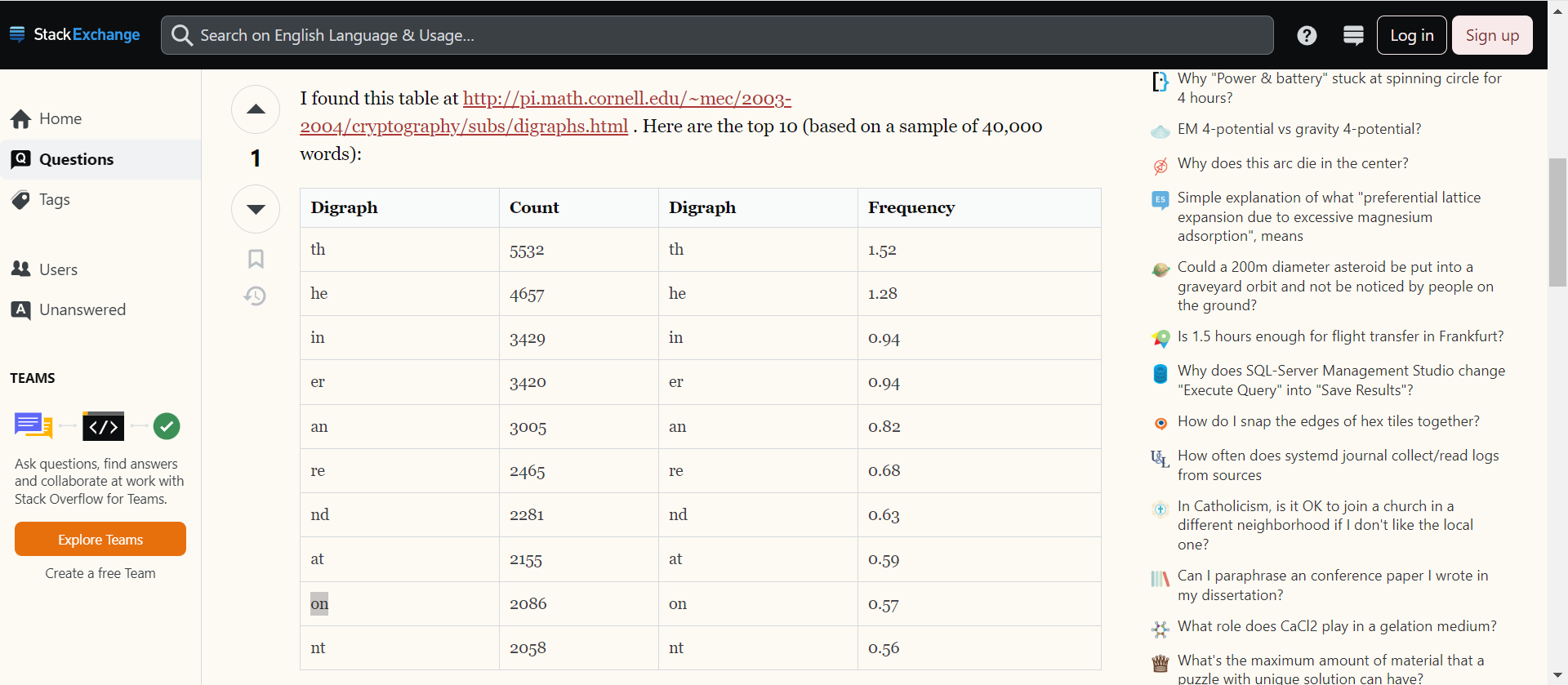
对其使用密钥key = 'zyxwvutsrqponmlkjihgfedcba’进行加密

加密后密文为: gsv jfrxp yildm ulc qfnkh levi gsv ozab wlt mvzi gsv yzmp lu gsv irevi. zh gsv hfm hvgh, gsv xzon dzgvi ivuovxgh gsv eryizmg sfvh lu gdrortsg. znrwhg gsv ifhgormt ovzevh, z tvmgov yivvav dsrhkvih gsilfts gsv ezoovb, xziibrmt drgs rg gsv hdvvg hxvmg lu yollnrmt uoldvih.

直接使用单字母频率统计攻击，结果为: tae qunfk gihld mhx zuyvo hwei tae rsbp jhc desi tae gsdk hm tae inwei. so tae oud oeto, tae fsry lstei iemrefto tae wngisdt aueo hm tlnrncat. synjot tae iuotrndc resweo, s cedtre gieebe lanoveio taihuca tae wsrrep, fsiipndc lnta nt tae oleet ofedt hm grhhyndc mrhleio.

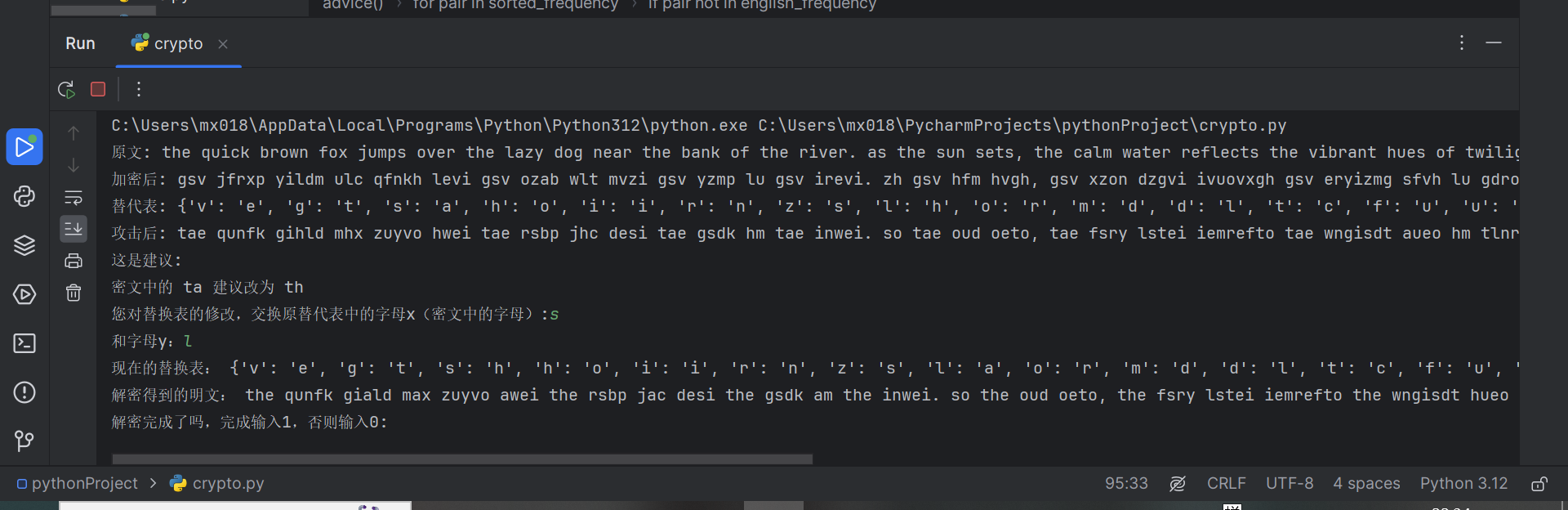
显然由于文本字数太少，仅有e,t等少数几个字母完全符合英文字母频率统计规律，因此笔者采取双字母频率统计来修正，通过统计解密结果的双字母频率，与统计频率比较来修正解密结果

英文双字母统计规律引用的是https://english.stackexchange.com/questions/571896/where-can-i-find-numbers-for-frequencies-of-digraphs的数据



例子中双字母频率最高的为ta，对比统计中的th，建议使用者，修正ta为th，具体操作时，找到替代表中a和h对应的key交换其value值，例子中为s与l（），交换后的解密结果显然更正确了，如此迭代可接近正确明文

修正建议与双字母统计均包含在def advice中



当然如果如此操作仍然不能得到正确明文，可寻求三字母频率统计，由于过于复杂，本文不予考虑。

程序提供了语言指引，当使用者对结果满意时可输入1结束迭代，否则可输入0，继续迭代