**字母频率分析实验报告**

1. 实验步骤：将文本输入，得出结果。
2. 汇总表

|  |  |  |  |
| --- | --- | --- | --- |
| 文本形式 | 文本内容 | 统计图 | 频率最高字母 |
| 有意义短文本 | There will be people willing to help you ward off all the evil in the world | 有意义短文本 | L |
| 有意义长文本 | between 1887 and 1905 there were several attempts,mostly notably by the Dutch physicist Hendrik Lorentz, to explain the result of the Michelson-Morley experiment in terms of objects contracting and clocks slowing down when they moved through the ether.However, in a famous paper in 1905, a hitherto unknown clerk in the Swiss patent office, Albert Einstein, pointed out that the whole idea of an ether was unnecessary, providing one was willing to abandon the idea of absolute time...... | 有意义长文本 | E |
| 随机文本 | sajkduifhyufjkwnhjgcyacuadnjkanhbcuixzhcxjczxkcmjsjnbhiaosqoiwuwysngwrikynbcgsdqpalnfywbcmvyqamygfkkrtn | 随机 | C/N |

1. 结论

有意义长文本得出的频率最高字母为E，符合语言字母统计概率，因此有意义长文本更接近语言字母统计概率。

分析原因：

有意义短文本字母数量过少，无法体现语言字母统计概率；

随机文本是随手打的一串字母，无准确含义，不符合语言字母使用频率；

有意义长文本是我们生活中使用语言的基本模式，因此符合语言字母统计概率。

**古典密码加解密与分析实验报告**

17数媒1班 朱漪雯 201710513023

1. Caesar 密码

1.加密

|  |  |  |  |
| --- | --- | --- | --- |
|  | 加密明文 | 移位值 | 密文 |
| 密码1 | hope and legacy requiem of heaven and earth parisienne walkways | 8 | pwxm ivl tmoikg zmycqmu wn pmidmv ivl mizbp xizqaqmvvm eitseiga |
| 密码2 | maybe if i keep believing my dreams will come to life | 14 | aomps wt w yssd pszwsjwbu am rfsoag kwzz qcas hc zwts |
| 密码3 | cause we are going to shout it loud,even if our words seem meaningless,it is like i am carrying the weight of the world | 20 | wuomy qy uly aicha ni mbion cn fiox,ypyh cz iol qilxm myyg gyuhchafymm,cn cm fcey c ug wullscha nby qycabn iz nby qilfx |

1. 解密

|  |  |  |  |
| --- | --- | --- | --- |
|  | 解密密文 | 移位值 | 明文 |
| 密码1 | pwxm ivl tmoikg zmycqmu wn pmidmv ivl mizbp xizqaqmvvm eitseiga | -8 | hope and legacy requiem of heaven and earth parisienne walkways |
| 密码2 | aomps wt w yssd pszwsjwbu am rfsoag kwzz qcas hc zwts | -14 | maybe if i keep believing my dreams will come to life |
| 密码3 | wuomy qy uly aicha ni mbion cn fiox,ypyh cz iol qilxm myyg gyuhchafymm,cn cm fcey c ug wullscha nby qycabn iz nby qilfx | -20 | cause we are going to shout it loud,even if our words seem meaningless,it is like i am carrying the weight of the world |

3.密文中统计频率最高的三个字母

|  |  |  |
| --- | --- | --- |
|  | 统计图 | 统计频率最高的三个字母 |
| 密码1 | 凯撒密码1 | I/M/V |
| 密码2 | 凯撒2 | S/W/A&Z |
| 密码3 | 凯撒3 | Y/C/I |

4.破译（语言设置为英语）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 密文 | 明文 | 移位值 | 是否破译成功 |
| 密码1 | pwxm ivl tmoikg zmycqmu wn pmidmv ivl mizbp xizqaqmvvm eitseiga | hope and legacy requiem of heaven and earth parisienne walkways | E->M，8 | 是 |
| 密码2 | aomps wt w yssd pszwsjwbu am rfsoag kwzz qcas hc zwts | maybe if i keep believing my dreams will come to life | E->S，14 | 是 |
| 密码3 | wuomy qy uly aicha ni mbion cn fiox,ypyh cz iol qilxm myyg gyuhchafymm,cn cm fcey c ug wullscha nby qycabn iz nby qilfx | cause we are going to shout it loud,even if our words seem meaningless,it is like i am carrying the weight of the world | E->Y，20 | 是 |

1. Vigenere 密码
2. 单词密钥

（1）加密

|  |  |  |  |
| --- | --- | --- | --- |
|  | 加密明文 | 密钥 | 密文 |
| 密码1 | hope and legacy requiem of heaven and earth parisienne walkways | echo | lqws epk ziihqc tleykla sh osexlb epk setav tcywwklbrg dopmdocu |
| 密码2 | maybe if i keep believing my dreams will come to life | nier | zicsr qj z xmig ompzrdmet uc uemedf emcy ksdr bs cvni |
| 密码3 | cause we are going to shout it loud,even if our words seem meaningless,it is like i am carrying the weight of the world | egoist | ggiaw pi gfm yhmtu bg lluib am puil,woit wn gnv cczvl wksu exetwvyeiyg,ql bw rwsw b es qijkcobo lai csqyax ut bzx auftv |

（2）解密

|  |  |  |  |
| --- | --- | --- | --- |
|  | 解密密文 | 密钥 | 明文 |
| 密码1 | lqws epk ziihqc tleykla sh osexlb epk setav tcywwklbrg dopmdocu | echo | hope and legacy requiem of heaven and earth parisienne walkways |
| 密码2 | zicsr qj z xmig ompzrdmet uc uemedf emcy ksdr bs cvni | nier | maybe if i keep believing my dreams will come to life |
| 密码3 | ggiaw pi gfm yhmtu bg lluib am puil,woit wn gnv cczvl wksu exetwvyeiyg,ql bw rwsw b es qijkcobo lai csqyax ut bzx auftv | egoist | cause we are going to shout it loud,even if our words seem meaningless,it is like i am carrying the weight of the world |

（3）密文中统计频率最高的三个字母

|  |  |  |
| --- | --- | --- |
|  | 统计图 | 统计频率最高的三个字母 |
| 密码1 | v1 | E/L/S |
| 密码2 | v2 | M/C/E |
| 密码3 | v3 | W&I/B&G&L&U |

与Caesar密码相比，密文的字母分布更加平均，不太能根据频率确定字母替换规律。

（4）破译

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 密文 | 明文 | 时长 | 密钥长度 | 密钥 | 破译是否成功 |
| 密码1 | lqws epk ziihqc tleykla sh osexlb epk setav | hope and legacy requiem of heaven and earth parisienne walkways | 2s | 4 | echo | 是 |
| 密码2 | zicsr qj z xmig ompzrdmet uc uemedf emcy ksdr bs cvni | maybe if i keep believing my dreams will come to life | 2s | 4 | nier | 是 |
| 密码3 | ggiaw pi gfm yhmtu bg lluib am puil,woit wn gnv cczvl wksu exetwvyeiyg,ql bw rwsw b es qijkcobo lai csqyax ut bzx auftv | cause we are going to shout it loud,even if our words seem meaningless,it is like i am carrying the weight of the world | 2s | 6 | egoist | 是 |

1. 长随机密钥

（1）加密

|  |  |  |  |
| --- | --- | --- | --- |
|  | 加密明文 | 密钥 | 密文 |
| 密码1 | hopeandlegacyrequiemofheavenandearthparisiennewalkways | cascbhasjxjdvuidhsfncjnjudhjnjcxncmjnjbncjncldsfuuhyrs | johgbuddndjftlmtbajzqounuylwnwfbntfqcjsvurrpyhoffedypk |
| 密码2 | maybeifikeepbelievingmydreamswillcometolife | jsakfhfajnjcnvbjsjdihfyeygfbjzxckxvdsivnsdb | vsyljpkitrnrozmrwelvnrwhpkfnbvfnvzjpwbjyaif |
| 密码3 | causewearegoingtoshoutitloudevenifourwordsseemmeaninglessitislikeiamcarryingtheweightoftheworld | asjskhfyqguknbchsaygasuskcnjsbfadhuasjasncjwfqojjjbfsvjksnckncjwhfeuhfwjakmcsjdnvssdcsdmvknvhfj | csdkodjyhkayvoiagsfuulclvqhmwwjnlmiujfojqubajcanjwjsygnckvvsfnrglnegjfnayszilqhjzaykvgifcojjyqm |

（2）解密

|  |  |  |  |
| --- | --- | --- | --- |
|  | 解密密文 | 密钥 | 明文 |
| 密码1 | johgbuddndjftlmtbajzqounuylwnwfbntfqcjsvurrpyhoffedypk | cascbhasjxjdvuidhsfncjnjudhjnjcxncmjnjbncjncldsfuuhyrs | hopeandlegacyrequiemofheavenandearthparisiennewalkways |
| 密码2 | vsyljpkitrnrozmrwelvnrwhpkfnbvfnvzjpwbjyaif | jsakfhfajnjcnvbjsjdihfyeygfbjzxckxvdsivnsdb | maybeifikeepbelievingmydreamswillcometolife |
| 密码3 | csdkodjyhkayvoiagsfuulclvqhmwwjnlmiujfojqubajcanjwjsygnckvvsfnrglnegjfnayszilqhjzaykvgifcojjyqm | asjskhfyqguknbchsaygasuskcnjsbfadhuasjasncjwfqojjjbfsvjksnckncjwhfeuhfwjakmcsjdnvssdcsdmvknvhfj | causewearegoingtoshoutitloudevenifourwordsseemmeaninglessitislikeiamcarryingtheweightoftheworld |

（3）密文中统计频率最高的三个字母

|  |  |  |
| --- | --- | --- |
|  | 统计图 | 统计频率最高的三个字母 |
| 密码1 | v11 | F/D&J&N&U |
| 密码2 | v22 | N&R&V |
| 密码3 | v33 | J/A&N&Y |

（4）破译

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 密文 | 明文 | 时长 | 密钥长度 | 密钥 | 破译是否成功 |
| 密码1 | johgbuddndjftlmtbajzqounuylwnwfbntfqcjsvurrpyhoffedypk | entondvansemputtavilyadfryarusoinsaporeemoretokomectow | 2s | 17 | FBOSORIDALFTERTAB | 否 |
| 密码2 | vsyljpkitrnrozmrwelvnrwhpkfnbvfnvzjpwbjyaif | wandetricraswoemallenexpecarivoniareownfarf | 2s | 11 | ZSLIFWTARAN | 否 |
| 密码3 | csdkodjyhkayvoiagsfuulclvqhmwwjnlmiujfojqubajcanjwjsygnckvvsfnrglnegjfnayszilqhjzaykvgifcojjyqm | nyloombepyghdoviodlcylldbyvsfejatutarjosiajoplinwerdeorctnbattaolamoulveybrotenshalsdrongosbeya | 3s | 17 | PUSWARIUSMUIRSSANSS | 否 |

三．Enigma 密码

（1）加密

|  |  |  |  |
| --- | --- | --- | --- |
|  | 加密明文 | 密钥 | 密文 |
| 密码1 | hope and legacy requiem of heaven and earth parisienne walkways | rotor：I II III  reflector：UKW A | lpgs flf exqree lxlnmfy dq wjcilr nza vwguy ftaxojuyhh rfdroiwx |
| 密码2 | maybe if i keep believing my dreams will come to life | rotor：II I III  reflector：UKW B | ynpfn sq q ejdy qjxuyjrii xb ybqkpg rnvi xgfb yb wscd |
| 密码3 | cause we are going to shout it loud,even if our words seem meaningless,it is like i am carrying the weight of the world | rotor：III II I  reflector：UKW C | bjgfv xu qki aumbs oq xncgh ly mrdk,pxhq rw jmb bpwwv evii jhovnsbbila,rb ga tyor m vy wzktxzau adv bxlsfy kp ius ekncj |

（2）解密

|  |  |  |  |
| --- | --- | --- | --- |
|  | 解密密文 | 密钥 | 明文 |
| 密码1 | lpgs flf exqree lxlnmfy dq wjcilr nza vwguy ftaxojuyhh rfdroiwx | rotor：I II III  reflector：UKW A | hope and legacy requiem of heaven and earth parisienne walkways |
| 密码2 | ynpfn sq q ejdy qjxuyjrii xb ybqkpg rnvi xgfb yb wscd | rotor：II I III  reflector：UKW B | maybe if i keep believing my dreams will come to life |
| 密码3 | bjgfv xu qki aumbs oq xncgh ly mrdk,pxhq rw jmb bpwwv evii jhovnsbbila,rb ga tyor m vy wzktxzau adv bxlsfy kp ius ekncj | rotor：III II I  reflector：UKW C | cause we are going to shout it loud,even if our words seem meaningless,it is like i am carrying the weight of the world |

（3）密文中统计频率最高的三个字母

|  |  |  |
| --- | --- | --- |
|  | 统计图 | 统计频率最高的三个字母 |
| 密码1 | e1 | F&L/R&X |
| 密码2 | e2 | Y/B&Q |
| 密码3 | e3 | B/V/A&I&K&X |

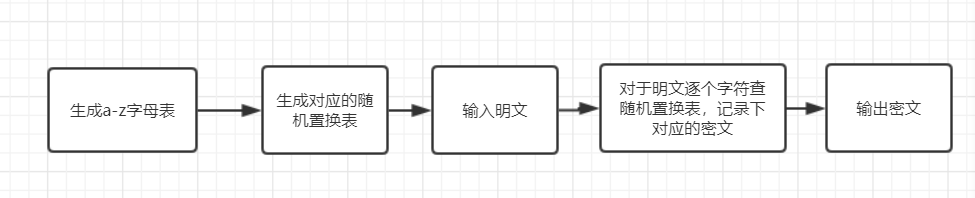
与Caesar密码相比，密文的字母分布更加平均，不太能根据频率确定字母替换规律。

**古典密码编程**

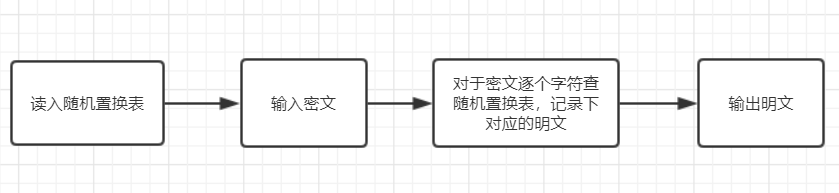
17数媒1班 朱漪雯 201710513023

1. 置换密码
2. 流程图

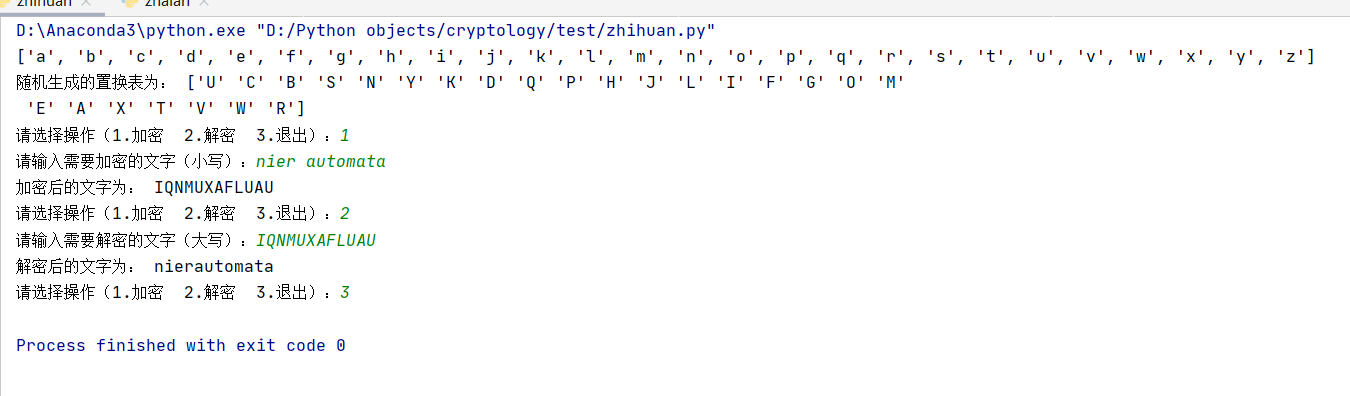
加密：



解密：

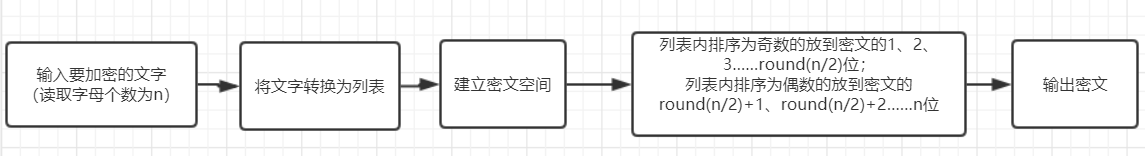


1. 执行结果

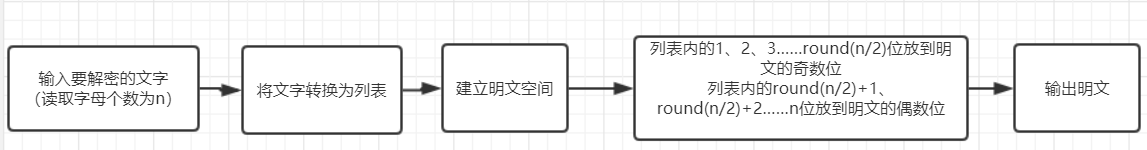


1. 栅栏密码
2. 流程图

加密：



解密：



1. 执行结果

