report

陈张萌 2017013678

1.21(4)未知密码

得到密钥长度

先计算m=1时重合指数，发现 m=1时重合指数为 [0.041418761021347 37]，很接近0.038，因此不是访射或者代换密码，推测是Virginia密码。 因此采用和(2)一样的方法得到：

确定密钥内容

根据书上的算法，计算M_g，选择距离0.065最近的g即可。得到密钥为CRYPTO。 虽然我们发现误差仍然很大，推测是因为密文长度不够长导致的。

```
key=24    loss=0.00028571428571426416
C
key=9    loss=0.005196428571428574
R
key=2    loss=0.0062678571428571375
Y
key=11    loss=0.0010000000000000148
P
key=7    loss=0.009214285714285717
T
key=12    loss=0.005428571428571435
O
```

得到明文为：

ILEARNEDHOWTOCALCULATETHEAMOUNTOFPAPERNEEDEDFORAROOMWHENIWASAT SCHOOLYOUMULTIPLYTHESQUAREFOOTAGEOFTHEWALLSBYTHECUBICCONTENTSOF THEFLOORANDCEILINGCOMBINEDANDDOUBLEITYOUTHENALLOWHALFTHETOTALFOR OPENINGSSUCHASWINDOWSANDDOORDTHENYOUALLOWTHEOTHERHALFFORMATCH INGTHEPATTERNTHENYOUDOUBLETHEWHOLETHINGAGAINTOGIVEAMARGINOFERRO RANDTHENYOUORDERTHEPAPER