# 密码学第一次作业

计算机学院 2313469 章壹程 25.03.07

##### 1.18

0000->0000

0001->0011->0110->1100->1000->0001

0010->0101->1010->0100->1001->0010

0111->1111->1110->1101->1011->0111

除0000密码流周期为1外其余均为5

##### 1.21(D)

BNVSNSIHQCEELSSKKYERIFJKXUMBGYKAMQLJTYAVFBKVT  
DVBPVVRJYYLAOKYMPQSCGDLFSRLLPROYGESEBUUALRWXM

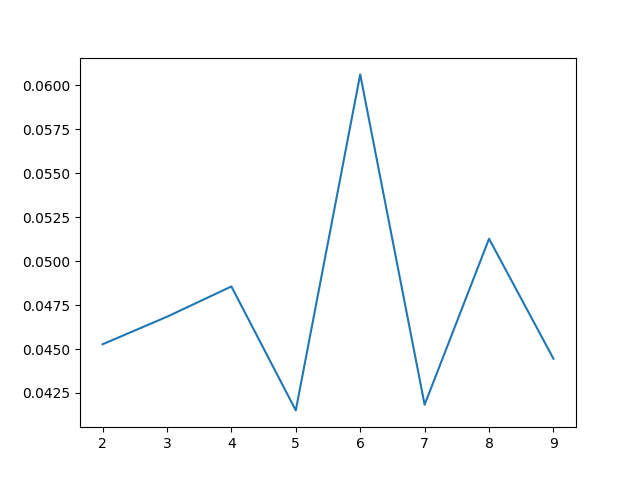
MASAZLGLEDFJBZAVVPXWICGJXASCBYEHOSNMULKCEAHTQ

OKMFLEBKFXLRRFDTZXCIWBJSICBGAWDVYDHAVFJXZIBKC

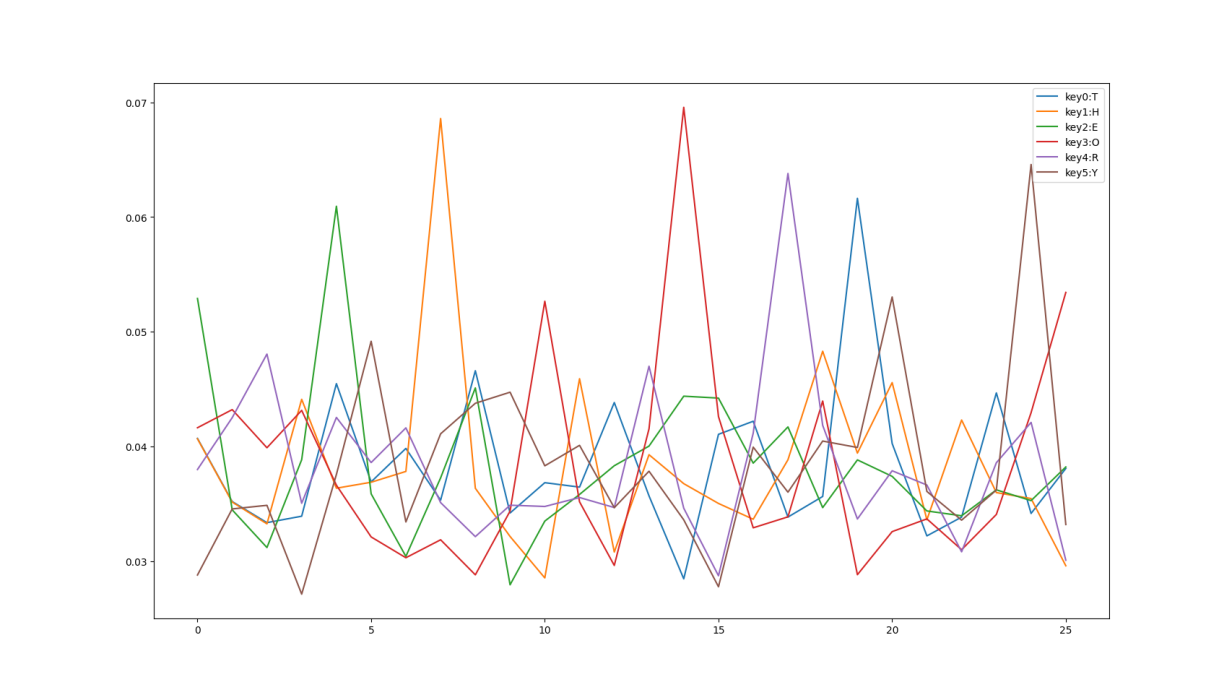
GJIWEAHTTOEWTUHKRQVVRGZBXYIREMMASCSPBNLHJMBLR  
FFJELHWEYLWISTFVVYFJCMHYUYRUFSFMGESIGRLWALSWM  
NUHSIMYYITCCQPZSICEHBCCMZFEGVJYOCDEMMPGHVAAUM  
ELCMOEHVLTIPSUYILVGFLMVWDVYDBTHFRAYISYSGKVSUU  
HYHGGCKTMBLRX

A-Z各种字符均出现且较为均匀，可以排除代换密码、仿射密码等映射方式的密码。

猜测是维吉尼亚密码，编程使用重合指数法进行探查



平均重合指数如图所示，当m=6时平均重合指数很接近英文单词分布，使用拟重合指数法确定位移量。



选取计算出来的重合指数最大的，可解得密钥是THEORY，明文为：

I grew up among slow talkers, men in particular, who dropped words a few at a time like beans in a hill, and when I got to Minneapolis where people took a Lake Wobegon comma to mean the end of a story, I couldn't speak a whole sentence in company and was considered not too bright. So I enrolled in a speech course taught by Orville Sand, the founder of reflexive relaxology, a self-hypnotic technique that enabled a person to speak up to three hundred words per minute.

注：看大写英文实在过于困难，我分了前几个词后就到网上搜了，这一段是摘自[Cryptography Theory and Practice](https://cs.uwaterloo.ca/~dstinson/solns.html) https://cs.uwaterloo.ca/~dstinson/solns.html，粗看是对的