Homework 2

Suyi Liu

February 16 2017

Extra Credit: I attended the Rubik's Cube Event for at least 45 minutes

1 P1

I tried all possible shifts from 0 to 25 and found the following making most sense:
plaintext: It would be so tempting to just write can you hear me now

2 P2

I tried all possible a_inverse and b(since D(x) = a_inverse(x-b) mod 26) and found the following making most sense: (edited out all but a sample of this output in the diary)
plaintext: I am in there somewhere hiding in that long list of gibberish

3 P3

I found A = C*M_inverse first, and then computed plaintext using A_inverse*C(shown in diary)
plaintext: The tip of the month is to buy low and sell highaaa.

4 P4

I included fuction details in the vigenerek.m file. Implementation details are included in the diary.

5 P5

Yes, the method will still work.
The difference in implementation is that:
consider independent random variables X,Y take values in Z_5, $P(X = i) = P(Y = i) = \mu i$,

Then for x = 0,1,2,3,4:
$P(X + \tau = Y mod 26) = \sum_{i=0}^{4} P(X = i)P(Y = i + \tau mod 26)$
= 0.2500 if $\tau = 0$ (0.05*0.05+0.20*0.20+ 0.25*0.25+ 0.35*0.35+ 0.15*0.15)
= 0.2075 if $\tau = 1$ (0.05*0.20+0.20*0.25+ 0.25*0.35+ 0.35*0.15+ 0.15*0.05)
= 0.1675 if $\tau = 2$ (0.05*0.25+0.20*0.35+ 0.25*0.15+ 0.35*0.05+ 0.15*0.20)
= 0.1675 if $\tau = 3$ (0.05*0.35+0.20*0.15+ 0.25*0.05+ 0.35*0.20+ 0.15*0.25)
= 0.2075 if $\tau = 4$ (0.05*0.15+0.20*0.05+ 0.25*0.20+ 0.35*0.25+ 0.15*0.35)
Generally speaking, $P(X + \tau = Y mod 26) = 0.2500$ if $\tau = 0$, and $P(X + \tau = Y mod 26) \leq 0.2075$ if $\tau \neq 0$
So the two specific numbers that we should change are 0.0066 and 0.0045, and we change them to 0.2500 and 0.2075 respectively.
After this step, when we are using relative frequency of five letters(selected from each group of key blocks) to calculate dot product of the vector v with the 4 shifts of the alphabet frequency vector. In this time, just simply use our new population relative frequencies of those five letters.