Name: Naman Sharma  
Roll No. 2110110343

Q1

1. Breaking shift cipher using brute force

I have added a dictionary of around 5,00,000 words which is being used for directly checking for all the possible plaintexts after being shifted by the specific key.



And for those words which aren’t there in the dictionary its directly printing all the possible decryptions.

A screen shot of a computer

Description automatically generated

1. Breaking Shift Cipher using IOC

We are trying to break a paragraph which is being encrypted using shift cipher, we calculate the IOC for each shifts, and which ever IOC is near 0.065, that’s our decrypted text.

I have taken an input in the file input\_for\_shift\_cipher.txt

A screen shot of a computer

Description automatically generated

1. Breaking Vignere Cipher using Kasiski Test.

We break a paragraph which has been encrypted using vignere cipher.  
For this I first count the commonly occurring bigrams, which have appeared at least in the string more than once.

Then I calculate the distances between them, and I take the GCD for all the distances.  
This gives our possible keylength size.  
Then I just for that keylength size I try to find the IOC of the particular string by breaking it into fragments of size of keylength and then forming a string of the zeroth indexes, first indexes till the keylength-1 indexes.

Whichever has IOC closest to 0.065, that becomes my key.

**Assumptions I took:**

I have only been counting bigrams from length 3 to length 8.  
Only taking differences less than 50 between the repeating bigrams index. In class we had only been counting till 20.

I have taken the class example as my input, and it works completely fine for it. A screen shot of a computer

Description automatically generated