Name: suchin kumar  
 Roll No. 2110110524

Brute Force Shift Cipher: Using a dictionary to check for possible plaintexts after shifting by each key is a common approach. However, brute force can be inefficient for large keyspaces. It's good to have a dictionary to speed up the process, but keep in mind that exhaustive searching might not be practical for longer texts or larger keys.

A screen shot of a computer

Description automatically generated

1. Breaking Shift Cipher using IOC (Index of Coincidence): Calculating the IOC for each shift and choosing the one closest to the expected IOC of English text (around 0.065) is a smart approach. It's a more efficient method compared to brute force for shift ciphers.A screen shot of a computer

   Description automatically generated
2. Breaking Vigenère Cipher using Kasiski Test:

The Kasiski Test is a well-known method for breaking Vigenère ciphers. It's good that you're considering the distances between repeated sequences to determine the likely key length. Using the GCD of these distances is a standard step in this process. After finding the probable key length, you're trying to find the key by analyzing the IOC of substrings. This approach is reasonable, although it's worth noting that the Vigenère cipher can still be challenging to break, especially for longer keys or shorter ciphertexts.

**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