Logic

Substitution

- Find the length of the most frequent character in the ciphertext.
- The plaintext distribution shows that the most common letter was ‘e’. Subtract the value of ‘e’ (4) from the most frequent letter to get the displacement value for each letter.
- Loop over ciphertext ○ Subtract the displacement value from each letter to obtain the actual letter (add 26 in case it becomes negative).
- Return the string

Vigenère

Find Length

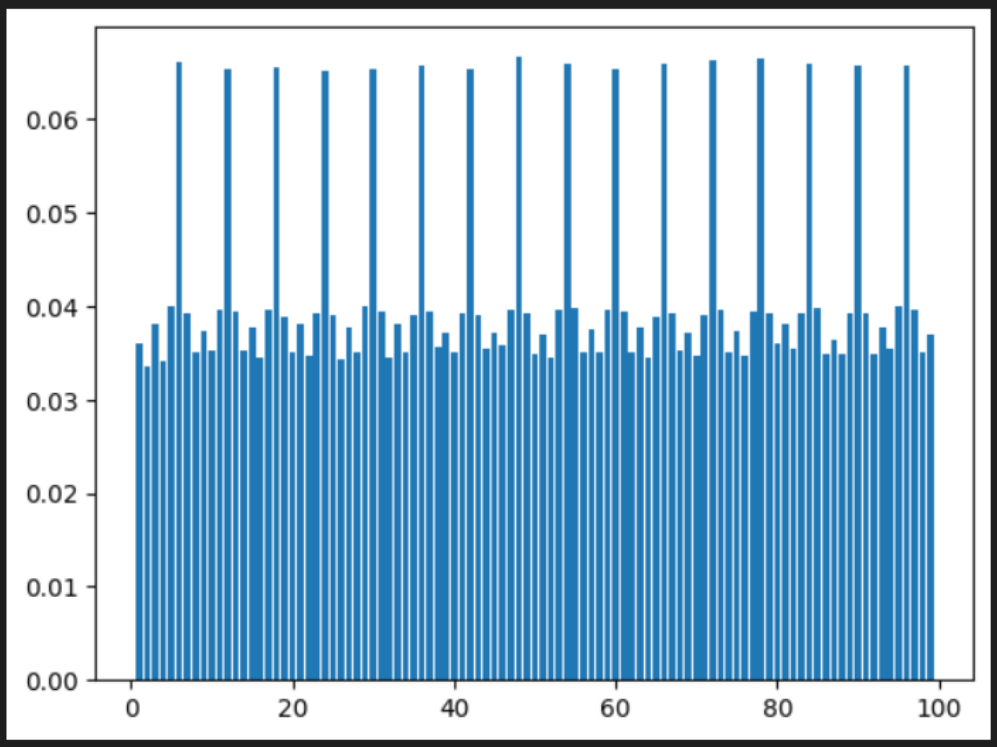
- Loop k = 2 – 100 ○ For each k find the collision proportion using the function rotate_compare() and observe the value
    - The value spikes at certain intervals (This point of the spike is the key length since every nth letter in a key of length ‘n’ is encrypted using the same letter)

Decrypt with length

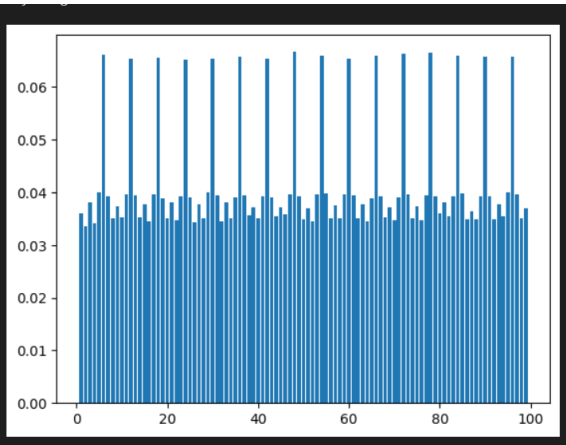
- Given the ciphertext and key length ‘k’ we know that every element after length ‘k’ in the ciphertext is encrypted using the same letter.
- Hence, this can be considered as a substitution cipher and can be solved using the same logic as above for substitution cipher (Assuming that the subtexts follow the same frequency distribution)
- Loop i = 1-k ○ For each i, extract the sub cipher
    - Decrypt the sub cipher using substitution cryptanalysis
- Re-join all the sub ciphers to get the plaintext

Output

```
Lowercase:
contentschaptermrsherlockholmeschapterthecurseofthebaskervilleschaptertheproblemchaptersirhenrybaskervillechapterthreebrokenthreadschapterbaskervilleha
Distribution: ['z', 'j', 'q', 'x', 'k', 'v', 'b', 'p', 'g', 'f', 'y', 'c', 'w', 'm', 'u', 'l', 'd', 'r', 's', 'n', 'h', 'i', 'o', 'a', 't', 'e']
Substitution Encrypted:
ugflwflkuzshlwjejkzwjdguczgdewkuzshlwjlzwumjkwgxlzwtskcwjnaddwkuzshlwjlzwhjgtdweuzshlwjkajzwfjqtskcwjnaddwuzshlwjlzjwwtjgcwflzjwsvkuzshlwjtskcwjnaddwzs
Substitution Decrypted:
contentschaptermrsherlockholmeschapterthecurseofthebaskervilleschaptertheproblemchaptersirhenrybaskervillechapterthreebrokenthreadschapterbaskervilleha
Decrypted No Key:
contentschaptermrsherlockholmeschapterthecurseofthebaskervilleschaptertheproblemchaptersirhenrybaskervillechapterthreebrokenthreadschapterbaskervilleha
Vigenere Encrypted:
tiflmnkmuzipkyjezsyyjdwcbbgduejwzsxtvllzmcllkwwfkbwtisbyjnqlcykupagnwjbhvjjgjlvguzipkyjkqryyfjgbrmcwzvzfdwkhrjlwztylwwjrfewfbhiysvacyuhlmrsukcmrmcddmhr
Vigenere Decrypted:
contentschaptermrsherlockholmeschapterthecurseofthebaskervilleschaptertheproblemchaptersirhenrybaskervillechapterthreebrokenthreadschapterbaskervilleha
Collision Proportion for 1 rotation: 0.03608603724485647
Vigenere Cryptanalyze With Length:
contentschaptermrsherlockholmeschapterthecurseofthebaskervilleschaptertheproblemchaptersirhenrybaskervillechapterthreebrokenthreadschapterbaskervilleha
```




```
Key Length: 6
```




```
Vigenere Decrypted No Key:
contentschaptermrsherlockholmeschapterthecurseofthebaskervilleschaptertheproblemchaptersirhenrybaskervillechapterthreebrokenthreadschapterbaskervilleha
```