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 o 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 o 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 o 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





