FCC Assignment Brainstorming 22/03/2022

Question 02

General view:

(a&b) * Decrypt ciphertext
- (a) → letter analysis attack
- (b) → brute force attack

(c) * Write a report; explaining your implementation step-by-step. substitution table used in letter freq & key found using brute-force attack

(A) Decrypting ciphertext using letter analysis attack.

steps:
- take a filename as an argument when executing .py program.
- read file by character
- count the frequency of characters A-Z (65-90) & a-z (97-122)
- compare these to a substitution ~~table~~ with % frequencies.
- substitute letters.
- write decrypted cipher to ~~plaintext~~ decrypted_(filename).

(B) Decrypting ciphertext using brute-force attack.

key=(a,b)
a=12
b=26

- take a filename as an argument
- read the first 100-300 characters.
- ~~use a decrypt~~
- For loop that changes the shift (shift) (0 → 25) b
- For loop that changes a 12 numbers ← (a) numbers that have a gcd of 1 with 26. a
- create a def decrypt algorithm for affine with both keys ~~passed~~
- add the decrypted text to an opened file brute_decrypted_(filename)

(E) Make a report
- explain what you did in (a) & (b)
- show substitution table used & preferably letter freq of the ciphertext in a graph.
- What the key was.