Character Ciphers

1. Using the Caesar Cipher, encrypt the message ATTACK AT DAWN.
   I used the following code with $a = 1$ and $b = 3$ to get "DWWDFN DW GDZQ".

```
alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
def encrypt(message, a, b):
    out = ""
    for letter in message:
        if letter in alphabet:
            out+=alphabet[(a*(alphabet.find(letter))+b)%26]
        else:
            out+=letter
    return out
```

2. Decrypt the ciphertext message LFDPH LVDZL FRQTX HUHG, which has been encrypted using the Caesar Cipher.
   I used the previous `encrypt()` function with $a = 1$ and $b = -3$ to get "ICAME ISAWI CONQU ERED" (or, "I CAME I SAW I CONQUERED").

3. Encrypt the message SURRENDER IMMEDIATELY using the affine transformation $C \equiv 11P+18 \mod 26$.
   `encrypt("SURRENDER IMMEDIATELY", 11, 18)` produces "IEXXKFZKX CUUKZCSTKJW".

4. Decrypt the message YLFQX PCRIT, which has been encrypted using the affine transformation $C \equiv 21P + 5 \mod 26$.

```
alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
def multiplicativeInverse(num):
    for i in range(1, 26):
        if (num*i)%26 == 1:
            return i
def decrypt(message, a, b):
    out = ""
    aInverse = multiplicativeInverse(a)
    for letter in message:
        if letter in alphabet:
            out += alphabet[((alphabet.find(letter) - b) * aInverse)%26]
        else:
            out+=letter
    return out
```

   `decrypt("YLFQX PCRIT", 21, 5)` produces "READM YLIPS" ("READ MY LIPS").

5. If the most common letter in a long ciphertext, encrypted by a shift transformation $C \equiv P + k \mod 26$ is Q, then what is the most likely value of k?
   The most common letter in plain English is E, so it's likely that E (4) was encrypted to Q (16). Therefore, $16 \equiv 4 + k \mod 26$, so algebra tells us $k = 12$.

6. The message IVQLM IQATQ SMIKP QTLVW VMQAJ MBBMZ BPIVG WCZWE VNZWU KPQVM AMNWZ BCVMK WWSQM was encrypted by a shift transformation $C \equiv P+k \mod 26$. Use frequencies of letters to determine the value of k. What is the plaintext message?
   I wrote a script to generate a frequency table:

```
alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
frequencies = {}
for letter in alphabet:
```

```
    frequencies[letter] = 0

message = input("Message: ")
for letter in message:
    if letter in frequencies:
        frequencies[letter]+=1
print(frequencies)
```

I got the following: `'A': 3, 'B': 4, 'C': 2, 'D': 0, 'E': 1, 'F': 0, 'G': 1, 'H': 0, 'I': 4, 'J': 1, 'K': 3, 'L': 2, 'M': 9, 'N': 2, 'O': 0, 'P': 3, 'Q': 7, 'R': 0, 'S': 2, 'T': 2, 'U': 1, 'V': 7, 'W': 7, 'X': 0, 'Y': 0, 'Z': 4`. The most common letter is M (9 occurences), followed by Q, V, and W (all 7 occurences).
Thus, I will try to shift E, the most common letter in plaintext, to M, a shift of $k = 8$. This produces "ANIDE AISLI KEACH ILDNO NEISB ETTER THANY OUROW NFROM CHINE SEFOR TUNEC OOKIE" (AN IDEA IS LIKE A CHILD NONE IS BETTER THAN YOUR OWN FROM CHINESE FORTUNE COOKIE).

7. If the two most common letters in a long ciphertext, encrypted by an affine transformation $C \equiv aP + b \mod 26$, are W and B, respectively, then what are the most likely values for a and b?
The most common letters in English are E and T respectively. Therefore, if we assume E (4) is encrypted as W (22) and T (19) as B (1), we get the following equations: $22 \equiv 4a + b \mod 26$, $1 \equiv 19a + b \mod 26$.
We can rearrange the first equation to get $b \equiv 22 - 4a \mod 26$, then substitute to get $1 \equiv 19a + 22 - 4a \mod 26$. Further algebra produces $-21 \equiv 15a \mod 26$, or $5 \equiv 15a \mod 26$. By testing integers 1 through 26 for a, it becomes apparent that $a = 9$.
Substituting that back, we get $b \equiv 22-4*9 \equiv 22-36 = 12 \mod 26$. This makes the transformation $C \equiv 9P + 12 \mod 26$
Now, to verify, because math is difficult. E is 4, $9 * 4 + 12 = 36 + 12 = 48 \equiv 22 \mod 26$, so E becomes encrypted as W. T is 19, $9 * 19 + 12 = 183 \equiv 1$, so T becomes encrypted as B. Stuff works out!
This verifies the affine transformation as $C \equiv 9P + 12 \mod 26$.

8. The message WEZBF TBBNJ THNBT ADZQE TGTYR BZAJN ANOOZ ATWGN ABOVG FNWZV A was encrypted by an affine transformation $C \equiv aP + b \mod 26$. The most common letters in the plaintext are A, E, N, and S. What is the plaintext message?
In the ciphertext, the most common letters are A (0), B (1), N (13), and T (19). Therefore, A maps to one of A, B, N, or T, meaning b must be 0, 1, 13, or 19.
This gives us a couple of different cases.

   (a) Case: $b = 0$. This means A maps to A, so E (4) must map to B (1), N (13), or T (19). If E maps to B, then $1 \equiv a * 4 \mod 26$. However, this is not possible, because it requires $a * 4$ to be odd. The same logic can be used for E mapping to N or T. Therefore, b cannot be 0.

   (b) Case: $b = 1$. This means A maps to B, so E must map to A (0), N (13), or T (19). If E maps to A, then $0 \equiv a * 4 + 1 \mod 26$. This would again require $a * 4$ to be odd, which is not possible. If E maps to N, then $13 \equiv a * 4 + 1 \mod 26$, so $a = 3$. If E maps to T, then $19 \equiv a * 4 + 1$, so $a = 11$. Thus, we have two cases to test: $a = 3, b = 1$ and $a = 11, b = 1$.

   (c) Case: $b = 13$. This means A maps to N, so E must map to A (0), B (1), or T (19). Again, it's impossible for E to map to A, since that would require $a * 4$ to be odd. If E maps to B, $1 \equiv a * 4 + 13 \mod 26$, so $14 \equiv a * 4 \mod 26$, so $a = 14$. If E maps to T, $13 \equiv a * 4 + 13 \mod 26$, so $0 \equiv a * 4 \mod 26$, so $a = 13$. However, because $\gcd(a, 26)$ must be 1, neither of these values of a work, so b cannot be 13.

   (d) Case: $b = 19$. This means A maps to T, so E must map to A (0) (impossible because it would require $a * 4$ to be odd), B (1), or N (13). If E maps to B, $1 \equiv a * 4 + 19 \mod 26$, so $8 \equiv a * 4$, so $a = 2$ or 15 (by the gcd rule, just 15). If E maps to N, $13 \equiv a * 4 + 19 \mod 26$, so $20 \equiv a * 4$, so $a = 5$. This gives us two more cases to test: $a = 5, b = 19$ and $a = 15, b = 19$.

Now, I take all my cases ($a = 3, b = 1$; $a = 5, b = 19$; $a = 11, b = 1$; $a = 15, b = 19$) and test them. I'm testing the encrypted string, as well as a string of the most common characters in the ciphertext (ABNT), because that should decrypt to some combination of AENS, allowing me to quickly see if the transformation is correct.
None of those worked and I have no idea why < 3.

I decided to brute force the problem just to see what the correct transformation should be. The most common letters in the ciphertext (A, B, N, and T) each appear 6 times, so I tested every possible value of a (odd numbers 1 through 25, excluding 13) and b (numbers 1 through 25). I filtered the decrypted messages by only outputting messages where A, E, N, and S each appeared exactly 6 times (the most common letters in the plaintext must appear the same number of times as the most common letters in the ciphertext).

```
message = "WEZBF TBBNJ THNBT ADZQE TGTYR BZAJN ANOOZ ATWGN ABOVG FNWZV A"
for a in range(1, 26, 2):
    for b in range(0, 26):
        if(a!=13):
            decrypted = decrypt(message, a, b)
            freqs = freqCount(decrypted)
            if(freqs["A"]==6 and freqs["E"]==6 and freqs["N"]==6 and freqs["S"]==6):
                print(a, b, decrypted)
```

This revealed that the transformation I should have found was $a = 21, b = 13$, and that the plaintext was "THISM ESSAG EWASE NCIPH EREDU SINGA NAFFI NETRA NSFOR MATIO N".
I looked back at my case $b = 13$ to try and figure out where I went wrong. It turns out I did and said a lot of very stupid things. Here is a corrected paragraph, with changes marked:
Case: $b = 13$. This means A maps to N, so E must map to A (0), B (1), or T (19). Again, it's impossible for E to map to A, since that would require $a * 4$ to be odd. If E maps to B, $1 \equiv a * 4 + 13 \mod 26$, so $14 \equiv a * 4 \mod 26$, so $a =$ 10 or 23. If E maps to T, $19 \equiv a * 4 + 13 \mod 26$, so $6 \equiv a * 4 \mod 26$, so $a =$ 8 or 21. However, because $\gcd(a, 26)$ must be 1, a cannot be 10 or 8, so we have two test cases: $a = 23, b = 13$ and $a = 21, b = 13$.
The affine transformation used to encode the message was $C \equiv 21P + 13 \mod 26$ and the message is "THIS MESSAGE WAS ENCIPHERED USING AN AFFINE TRANSFORMATION".

9. Given two ciphers, plaintext may be encrypted by first using one cipher, and then using another cipher on the result. This procedure produces a *product cipher*. Find the product cipher obtained by using the transformation $C \equiv 5P + 13 \mod 26$ followed by the transformation $C \equiv 17P + 3 \mod 26$.
This is essentially a composition of functions. $C \equiv 17(5P + 13) + 3 \mod 26$, which I can then simplify: $C \equiv 17 * 5P + 17 * 13 + 3 \equiv 85P + 221 + 3 \equiv 85P + 224 \mod 26$. I can then use mod rules to simplify to $C \equiv 7P + 18$.