1.: Write a Python function that will take a string and encrypt it using a shift cipher. The function should have the following heading:

def shiftcipher(string, key) where key is a number from 0 to 25. For exampe, if you call it with

shiftcipher('abcde',1) you should get the enciphered string BCDEF. There is a document pythonidioms.pdf on the Canvas page that may be a bit helpful.

The function I write is:

```
def shiftcipher(string, key)
    bstr = bytearray(string,'utf-8')
    for idx, element in enumerate(bstr):
        bstr[idx] = element + key
    return bstr.decode('utf-8')
```

---

2. Exercise 1 in Chapter 2: Ceasar wants to arrange a secret meeting with Marc Antony, either at the Tiber (the river) or at the Coliseum (the arena). He sends the ciphertext EVIRE. However, Antony does not know the key, so he tries all possibilities. Where will he meet Ceasar?

If we use a shift cipher, we can obtain both "river" and "arena" with different keys, therefore there is no way of knowing.

---

3. Exercise 3 in Chapter 2: The ciphertext UCR was encrypted using the affine function $9x + 2 \bmod 26$. Find the plaintext.

To decrypt this message, we first subtract 2 (mod 26), and then multiply by the multiplicative inverse of 9 in the set of all integers mod 26 which is 3. Therefore, the decrypted message is "cat".

---

4. Exercise 5 in Chapter 2 Encrypt howareyou using the affine function $5x + 7 \pmod{26}$. What is the decryption function? Check that it works.

---

by applying the affine transformation given above, the ciphertext is "sbpjqdzbf".

---

5. The following string has been encrypted using a shift cipher. Determine what is the oriinal message: AOLMVBUKHAPVUZA-VULZMVYHIHSHUJLKZBJJLZZHYLOVULZAFJOHYHJALYPUALNYPAFMHPAOSVCLHUKSVFHSAF

---

the decrypted text is: *the foundation stones for a balanced success are honesty character integrity faith love and loyalty.*

---

6. The file hwcipher1 on Canvas page contains encrypted data.

(a) Write a Python program to form counts of each character in this message. For example, you should find that there are 12 instances of the character '5', and 4 instances of the character '3'.

(b) Based on the number of counts and the encrypted text (only! – don't go looking somewhere else for hints), decipher the message.

---

1. Using python's collections library, I computed the counts using Python's "Counts" class which computes the number of time each unique element is used in an array.

2. The decrypted phrase reads: *a good glass in the bishops hostel in the devil's seat forty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the deaths head a beeline from the tree through the shot fifty feet out*

---

7. Exercise 11 in Chapter 2 Suppose you encrypt uwing an affine cipher, then encrypt the encryption using another affine cipher (both are working mod 26). Is there any advantage to doing this, rather than using a single affine cipher? Why or why not?

Consider two affine ciphers $a_1(x) = 5x + 7$ and $a_2(x) = 3x + 2$ both mod 26. If we encrypt data with first a_1 and then a_2, the expression becomes

$$\begin{aligned} a_2(a_1(x)) &= 3(5x + 7) + 2 \\ &= 15x + 21 + 2 \text{ (mod 26)} \\ &= 15x + 23 \text{ (mode 26)} \end{aligned}$$

which is of the form of a single affine cipher. Therefore, an adversary would break the nested cipher with the same effort it would take to break a single cipher and so there is no benefit to using nested affine ciphers.

---

8. Exercise 19 in Chapter 2 Suppose there is a language that only has the letters a and b. The frequency of the letter a is 0.1 and the frequency of b is 0.9. A message is encrypted using a Vegenere cipher (working mod 2 instead of mod 26). The ciphertext is BABABAAABA. The key lengthis 1, 2, or 3.

(a) Show that they key length is probably 2

(b) Using the information on the frequencies of the letters, determine the key and decrypt the message.

---

1. From the book, we know that Vegenere cipher is vulnerable to a two-phased approach. The first finds the length of the key, and the second decrypts the message. In finding the length of the key, we essentially perform convolution on the ciphertext but instead of multiplying the "overlapped" values, we compare them and yield a 1 if they are equal and a zero if they aren't. When performing this "binary convolution" with shifts of 1, 2, and 3, the resulting numbers of matches are 0, 2, and 0 respectively. Because the number of counts for a shift of two are greater than the other two, we would infer that the size of the key is probably two.

2. Now that we have an estimate for the key length, we consider slices of the data that share key values together. The first key value corresponds to a set of values: B B B A B, and the second is A A A A A. From the problem statement, we know that $P_A = 0.1$, and $P_B = 0.9$. Therefore, we infer that the first value of the key shifts the data by zero, and the second shifts the data by one, which yields a decrypted message of B B B B B B A B B B.

---

9. Exercise 27 in Chapter 2 Use the Playfair cipher with the keyword Cryptography to encrypt

Did he play fair at St Andrews golf course.

The encrypted message is: ekioirnoanhfygbzyblfgmznagndodvcmk

---

10. Exercise 28 In Chapter 2 The ciphertext

BP EG FC AI MA MG PO KB HU

was encrypted using the Playfair cipher with keyword *Archimedes*. Find the plaintext.

The decrypted phrase is: Eureka I Have Found It

---

11. Exercise 31. Express your answers in terms of years. Suppose Alice andn Bob are using a cryptosystem with a 128-bit key, so there are 2^{128} possible keys. Eve is trying a burte-force attack on the system.

(a) Suppose it takes 1 day for Eve to try 2^{64} possible keys. At this rate, how long will it take for Eve to try all 2^{128} keys?

(b) Suppose Alice waits 10 years and then buys a acomputer that is 100 times faster than the one she now owns. Will she finish trying 2^{128} keys before or after what she does in part (a)?

---

1. We compute the number of days as $\frac{2^{128}}{2^{64}} = 2^{64}$ days which is 5.0539×10^{16} years.

2. If Eve waits 10 years and then buys a computer that is 100 times faster, we can compute the total time before she will attempt all 2^{128} combinations as

$$\begin{aligned} t_{\text{complete}} &= 10 + \frac{2^{128}}{10 \cdot 2^{64} \cdot 365} \\ &= 5.0539 \times 10^{15} \end{aligned}$$

which is less then the initial time estimate for Eve. Note: if quantum computing takes off, then these numbers are subject to change.