Caesar & Vingenère Ciphers

Julia Ziac

Background: Ciphers & Deciphers

”When first learning to program in Python, it can be hard to ***decipher*** what each part of the code means.”

In this lesson, we’ll decipher, or *pick apart, analyze,* and *understand* different chunks of Python code. But we’ll also talk about deciphering – and, more specifically, *ciphering* – codes in a different way, in the context of secret messages.

Background: Nosy Housemate

The year is 2020. You’re stuck at home, working from home, learning from home. You regularly keep in touch with your best friend by sending them detailed emails. HOWEVER, as time has gone on, you notice your nosy housemate keeps reading your private emails!

Irritated, but persistent, you and your best friend decide to explore different ways to *cipher* your emails to make them unreadable to anyone but you two.

Inbox(1)

```
Dbo zpv sfbe uijt?
```

You just received this email from your friend, what do you think it says?

Quiz 1

□ Hi, how are you?

□ Can you read this?

□ How are you doing?

□ What is your name?

Inbox(1)

`Dbo zpv sfbe uijt?`

You just received this email from your friend, what do you think it says?

Quiz 1

- □ Hi, how are you?
- □ Can you read this?
- □ How are you doing?
- □ What is your name?

Explanation

Correct Answer: Can you read this?

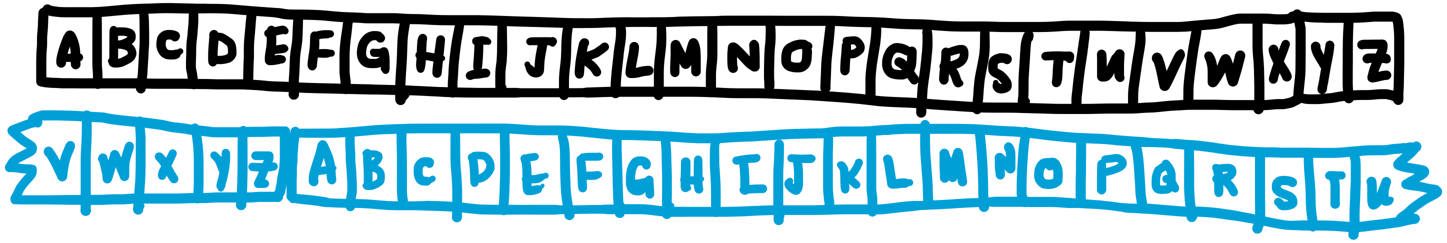
This option matched the word lengths of the original message. Option one also matched the length, but it would have meant the comma changed to an ”o” while the question mark remained. Options three and four both had the correct total number of characters (letters, spaces, and punctuation), but then the word lengths didn’t match.

Furthermore, and most importantly, each letter in the cipher text, `Dbo zpv sfbe uijt?` is one letter further in the alphabet than each letter in the deciphered text. For example, the “C” in “Can” turned into the next letter in the alphabet, “D.”

Caesar Cipher

Your friend used what’s called a “Caesar Cipher,” a famous method of encoding messages by shifting each letter in the alphabet by the same amount.

Your friend shifted each letter just one character further in the alphabet, but Caesar Ciphers can shift by any amount. If the shift takes you past the end of the alphabet, you loop back around to the beginning.



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

If you use a Caesar Cipher which shifts “A” five spaces to “F,” what will “X” become?

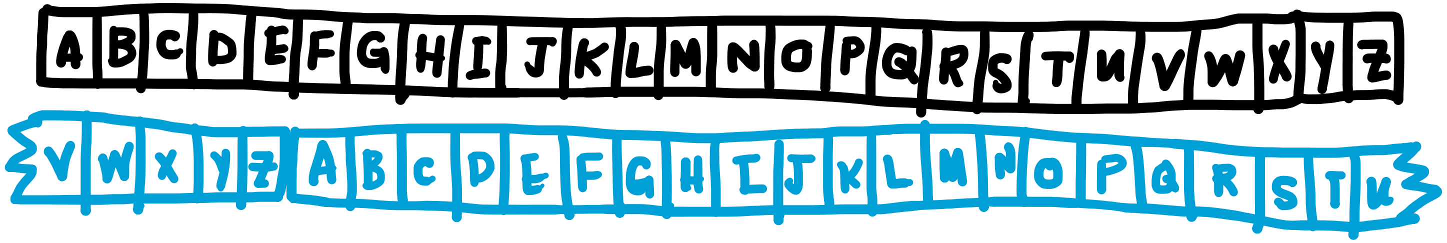
Quiz 1

- □ Y
- □ S
- □ C
- □ B

Caesar Cipher

Your friend used what's called a "Caesar Cipher," a famous method of encoding messages by shifting each letter in the alphabet by the same amount.

Your friend shifted each letter just one character further in the alphabet, but Caesar Ciphers can shift by any amount. If the shift takes you past the end of the alphabet, you loop back around to the beginning.


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U

If you use a Caesar Cipher which shifts "A" five spaces to "F," what will "X" become?

Quiz 1

□ Y

□ S

□ C

□ B

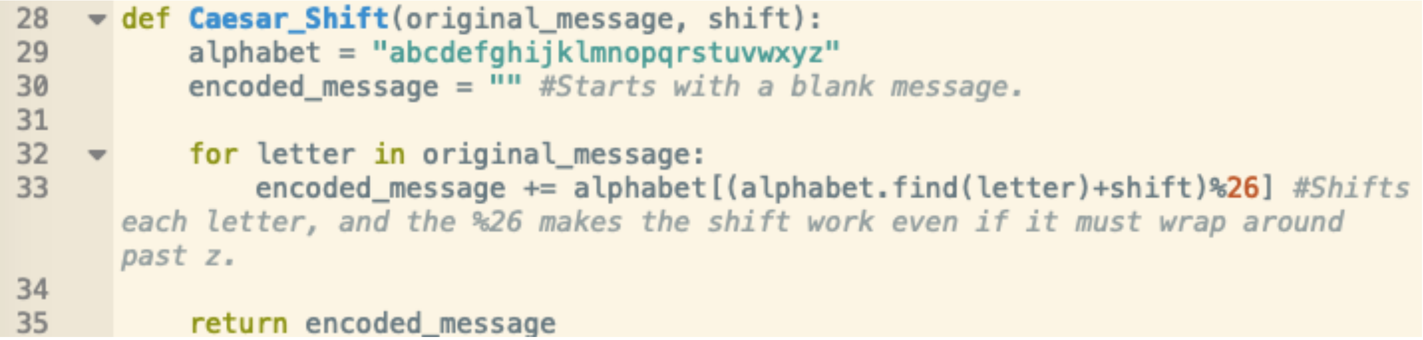
Explanation
Correct Answer: C

Counting five letters starting from A, you get B, C, D, E, **F**. Counting five letters starting from X, you get Y, Z, *wrap around back to* A, B, **C.** In a Caesar Cipher, you count forward in alphabetical order. If you were to count five backwards, you would have gotten S.

Caesar Cipher: Python code

You and your friend are getting pretty tired of counting through letters of the alphabet every time you want to send a message, so you’ve decided to see if the popular programming language Python can help make this process go faster.

Your friend wrote this code:



```python
def Caesar_Shift(original_message, shift):
    alphabet = "abcdefghijklmnopqrstuvwxyz"
    encoded_message = "" #Starts with a blank message.

    for letter in original_message:
        encoded_message += alphabet[(alphabet.find(letter)+shift)%26] #Shifts each letter, and the %26 makes the shift work even if it must wrap around past z.

    return encoded_message
```

Test their code with the original message “howdy” and a shift of 2, by typing in `Caesar_Shift(“howdy”,  2).` **What is the output?**

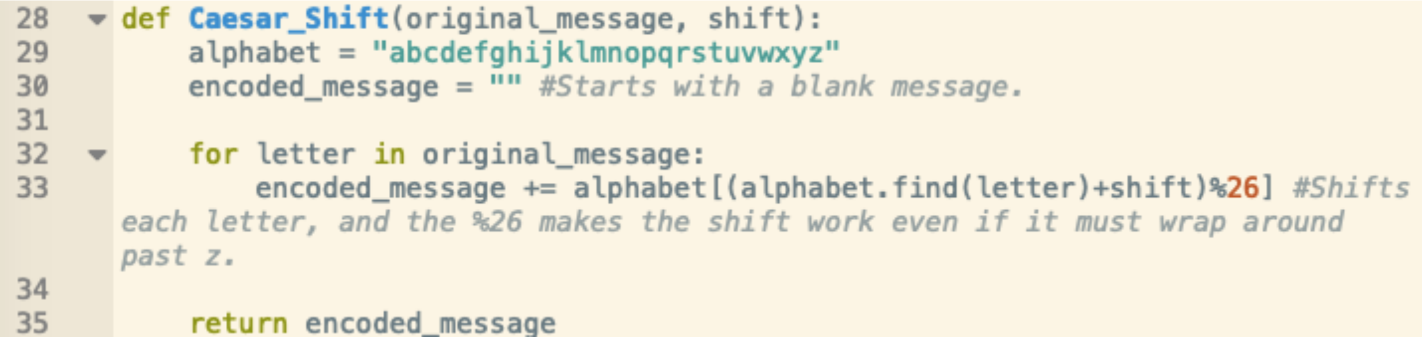
Quiz 1

- □ 'jqyfa’
- □ ‘krzgb’
- □ 'jgnnq’
- □ 'gdkkn'

Caesar Cipher: Python code

You and your friend are getting pretty tired of counting through letters of the alphabet every time you want to send a message, so you’ve decided to see if the very popular programming language, Python, can help make this process go faster.

Your friend wrote this code:



```python
def Caesar_Shift(original_message, shift):
    alphabet = "abcdefghijklmnopqrstuvwxyz"
    encoded_message = "" #Starts with a blank message.

    for letter in original_message:
        encoded_message += alphabet[(alphabet.find(letter)+shift)%26] #Shifts each letter, and the %26 makes the shift work even if it must wrap around past z.

    return encoded_message
```

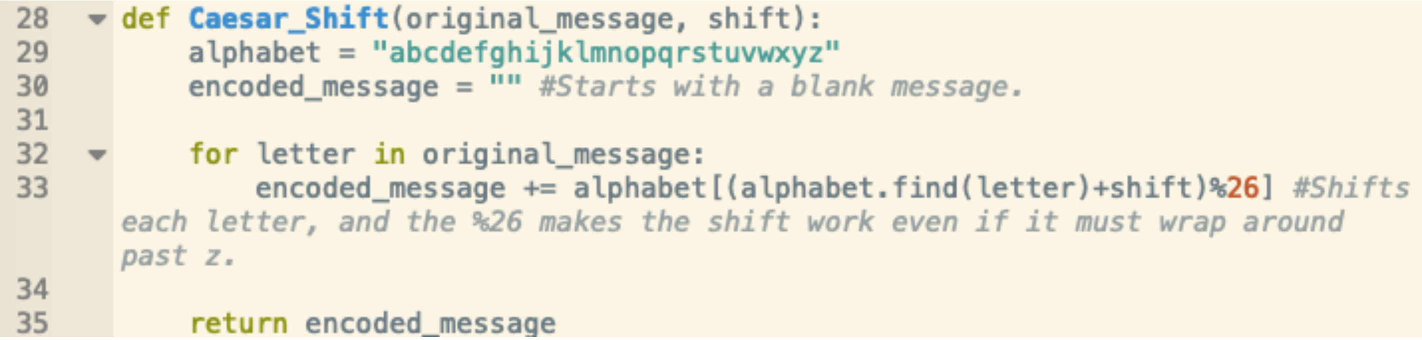
Test their code with the original message “howdy” and a shift of 2, by typing in `Caesar_Shift(“howdy”,  2).` **What is the output?**

Quiz 1

- □ 'jqyfa’
- □ ‘krzgb’
- □ 'jgnnq’
- □ 'gdkkn'

Caesar Cipher: Python code

You start composing a longer email using their code, but you notice something isn't right.



```
def Caesar_Shift(original_message, shift):
    alphabet = "abcdefghijklmnopqrstuvwxyz"
    encoded_message = "" #Starts with a blank message.

    for letter in original_message:
        encoded_message += alphabet[(alphabet.find(letter)+shift)%26] #Shifts each letter, and the %26 makes the shift work even if it must wrap around past z.

    return encoded_message
```

Try typing in a longer message. **What is flawed in their code?**

Quiz 1

□ It doesn't wrap back around to the beginning of the alphabet.

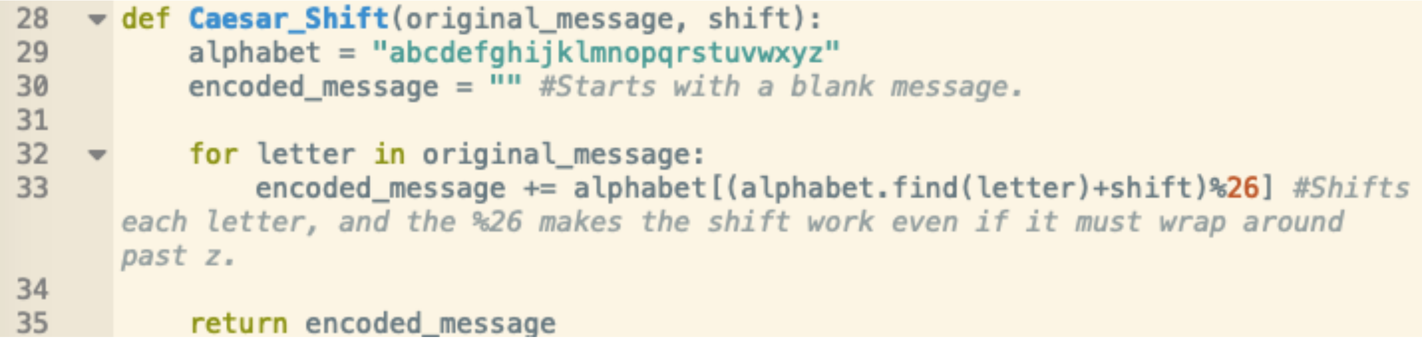
□ It returns the original message.

□ It is completely unrelated to the original message.

□ It makes any punctuation, spaces, or capital letters into the same letter.

Caesar Cipher: Python code

You start composing a longer email using their code, but you notice something isn't right.



```
28  def Caesar_Shift(original_message, shift):
29      alphabet = "abcdefghijklmnopqrstuvwxyz"
30      encoded_message = "" #Starts with a blank message.
31
32      for letter in original_message:
33          encoded_message += alphabet[(alphabet.find(letter)+shift)%26] #Shifts each letter, and the %26 makes the shift work even if it must wrap around past z.
34
35      return encoded_message
```

Try typing in a longer message. **What is flawed in their code?**

Quiz 1

- □ It doesn't wrap back around to the beginning of the alphabet.
- □ It returns the original message.
- □ It is completely unrelated to the original message.
- □ It makes any punctuation, spaces, or capital letters into the same letter.

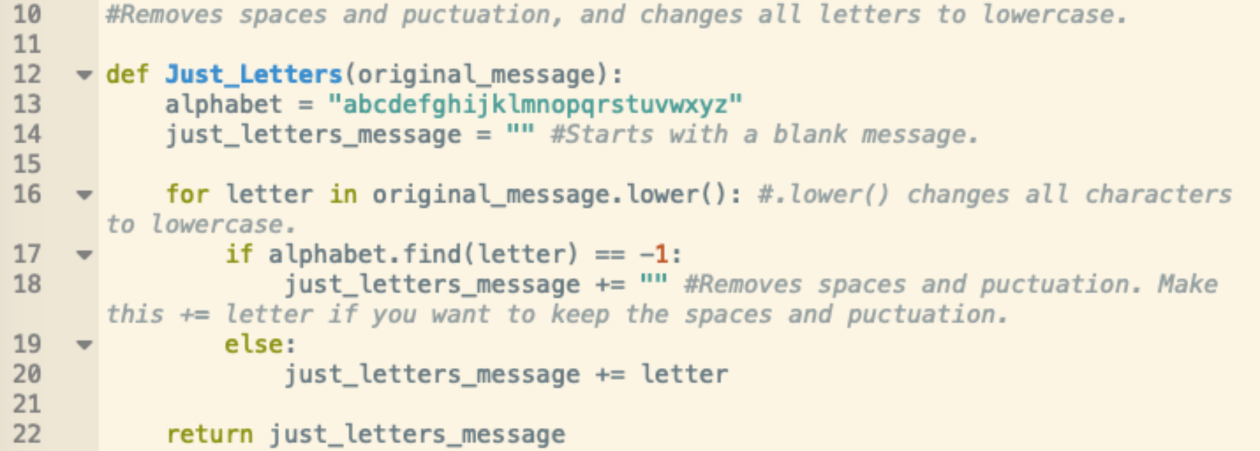
Explanation

Correct Answer: It makes any punctuation, spaces, or capital letters into the same letter.

You'll notice that every punctuation mark, space, or capital letter turns into the same lowercase letter. If you chose a shift of 2, this would always be a b. If you chose a shift of 4, each of these characters would turn into a d. This is because the alphabet in line 29 of their code only contains lowercase letters.

Caesar Cipher: Python code

Your friend creates another function for their code, which removes any punctuation or spaces from the original message and changes any uppercase letters to lowercase.

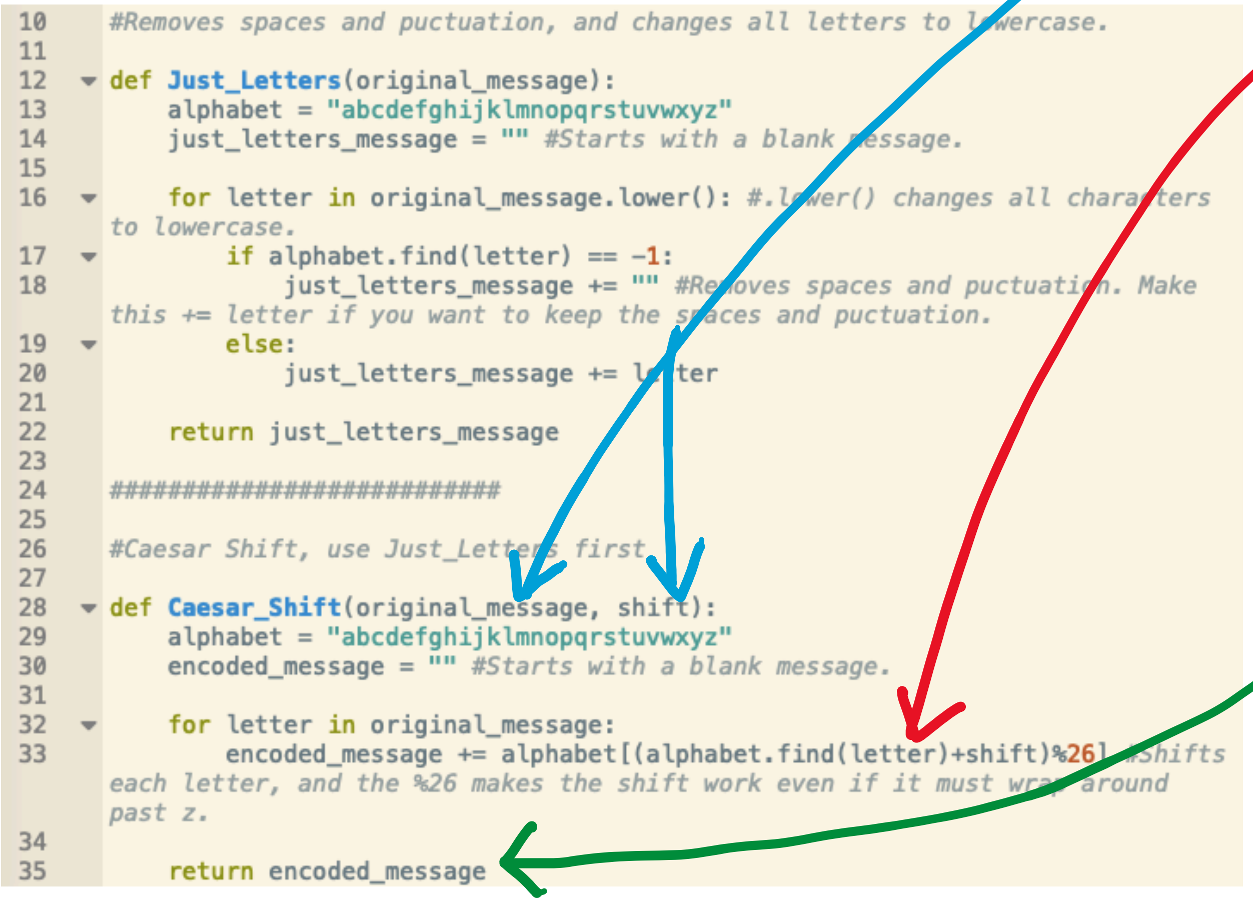


```
#Removes spaces and puctuation, and changes all letters to lowercase.

def Just_Letters(original_message):
    alphabet = "abcdefghijklmnopqrstuvwxyz"
    just_letters_message = "" #Starts with a blank message.

    for letter in original_message.lower(): #.lower() changes all characters to lowercase.
        if alphabet.find(letter) == -1:
            just_letters_message += "" #Removes spaces and puctuation. Make this += letter if you want to keep the spaces and puctuation.
        else:
            just_letters_message += letter

    return just_letters_message
```

Test their improved code with your own message and shift. Your input should look like this: `Caesar_Shift(Just_Letters(“Hi there, Friend!”), 2).`

Caesar Cipher: Python code, a final look

Let’s look at your friend’s code one more time to decipher what Python is doing in the different sections.



```
10  #Removes spaces and puctuation, and changes all letters to lowercase.
11
12  def Just_Letters(original_message):
13      alphabet = "abcdefghijklmnopqrstuvwxyz"
14      just_letters_message = "" #Starts with a blank message.
15
16      for letter in original_message.lower(): #.lower() changes all characters
    to lowercase.
17          if alphabet.find(letter) == -1:
18              just_letters_message += "" #Removes spaces and puctuation. Make
    this += letter if you want to keep the spaces and puctuation.
19          else:
20              just_letters_message += letter
21
22      return just_letters_message
23
24  ###########################
25
26  #Caesar Shift, use Just_Letters first
27
28  def Caesar_Shift(original_message, shift):
29      alphabet = "abcdefghijklmnopqrstuvwxyz"
30      encoded_message = "" #Starts with a blank message.
31
32      for letter in original_message:
33          encoded_message += alphabet[(alphabet.find(letter)+shift)%26] #Shifts
    each letter, and the %26 makes the shift work even if it must wrap around
    past z.
34
35      return encoded_message
```

These are the *inputs* of the Python *function*. Notice that the same words are used in lines 32 and 33 of the code.

Lines 32 and 33 are where the message is being encrypted. Line 32 is telling Python to go through each letter in the message individually. Line 33 then tells Python to see where that letter is originally in the alphabet, then shift it according to the input, then spit out the NEW letter and put that in a *variable* called `encoded_message`. The `%26` is what allows the cipher to wrap around if the shift takes it past z.

Line 35 is the *output* of the Python function. You can even reuse this output as an input to another function, just as we used the output of `Just_Letters` in `Caesar_Shift`, when we typed, `Caesar_Shift(Just_Letters(“Hi there, Friend!”), 2).`

Caesar Cipher: What could make this cipher harder to crack?

While we aren't going to *decipher* secret messages in this lesson, you can see that if your nosy roommate knows what shift was used in your Caesar Cipher, they could crack your secret message pretty easily.

What changes could you make to the Caesar Cipher to make it harder to crack?

Quiz 1

❑ Shift each letter in the original message by a different amount.

❑ Use symbols instead of letters in the ciphered message.

❑ Shift each word by a different amount.

❑ Write the entire message backwards.

Caesar Cipher: What could make this cipher harder to crack?

While we aren’t going to *decipher* secret messages in this lesson, you can see that if your nosy roommate knows what shift was used in your Caesar Cipher, they could crack your secret message pretty easily.

What changes could you make to the Caesar Cipher to make it harder to crack?

Quiz 1

- ❑ Shift each letter in the original message by a different amount.
- ❑ Use symbols instead of letters in the ciphered message.
- ❑ Shift each word by a different amount.
- ❑ Write the entire message backwards.

Explanation
All these options would make the cipher harder to crack! However, we are going to focus on the first one in the next section of this lesson.

Inbox(1)

`wgmosetdkpsas`

Your friend’s nosy housemate is as nosy as yours, so they’re trying ANOTHER cipher and have just sent you this message. **What do you think this message says?**

Quiz 2

- □ Hi there, friend!
- □ Howdy, pal!
- □ How’s it going?
- □ What’s up today?

Inbox(1)

`wgmosetdkpsas`

Your friend's nosy housemate is as nosy as yours, so they're trying ANOTHER cipher and have just sent you this message. **What do you think this message says?**

Quiz 2

- □ Hi there, friend!
- □ Howdy, pal!
- □ How's it going?
- □ What's up today?

Explanation
Correct Answer: Hi there, friend!

This one is MUCH harder to guess. You'll notice the ciphered text has 13 characters and options three and four both have 13 characters without spaces. However, in this cipher method, you ignore ALL spaces and punctuation, so option one is the only option with 13 characters. Now, how did your friend arrive at those characters? Let's find out!

Vigenère Cipher

In this message, your friend used the "Vigenère Cipher." Instead of shifting each letter by the same amount, it uses a *keyword* to shift each letter individually.

Let's see how this keyword shift works by exploring what your friend did to arrive at their encoded message.

Vigenère Cipher: Example

Your friend started with the message, "Hi there, friend!" and the keyword, "Python."

First, they got rid of all the punctuation, spaces, and capitalization in both the original message and the keyword.

hitherefriend

python

Vigenère Cipher: Example

Then, they lengthened the keyword to match the length of the original message by repeating it.

hitherefriend
pythonpythonp

Notice that the repetition of the keyword didn’t end perfectly. That’s ok!

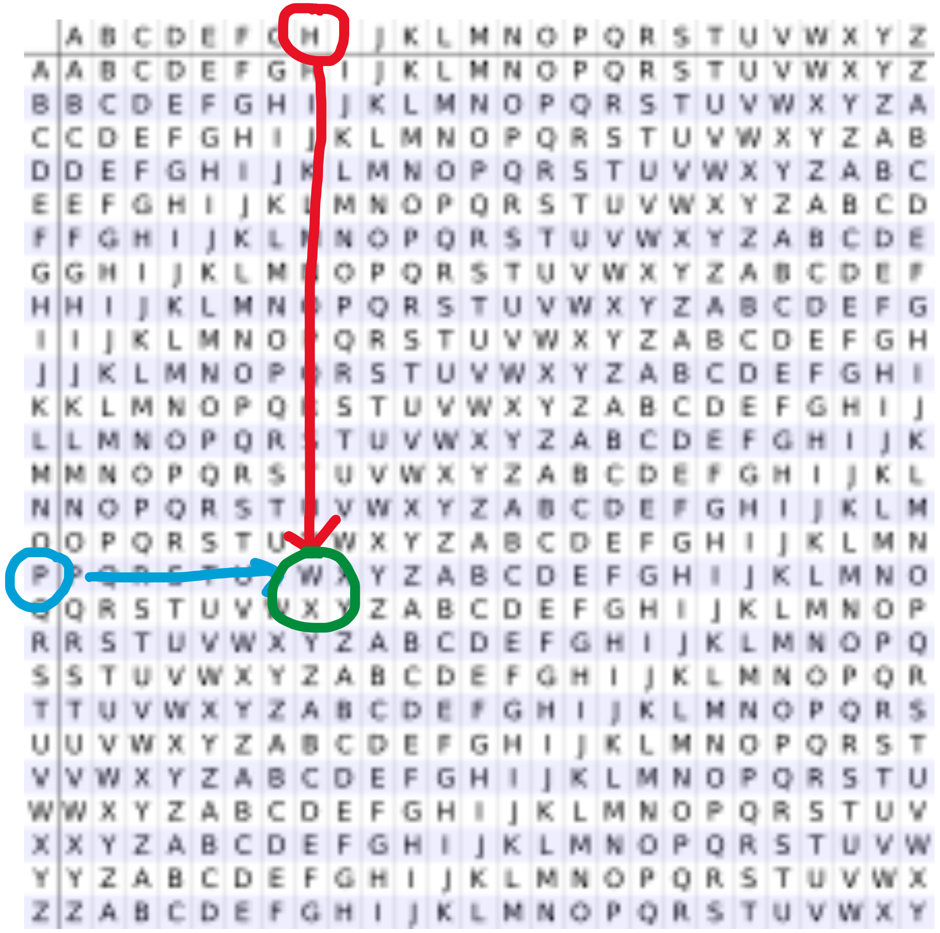
Vigenère Cipher: Example

Next, they used this chart to determine the shift of every letter. For example, the first “h” shifts according to “p” , so it becomes “w”.

h i t h e r e f r i e n d

p y t h o n p y t h o n p

w

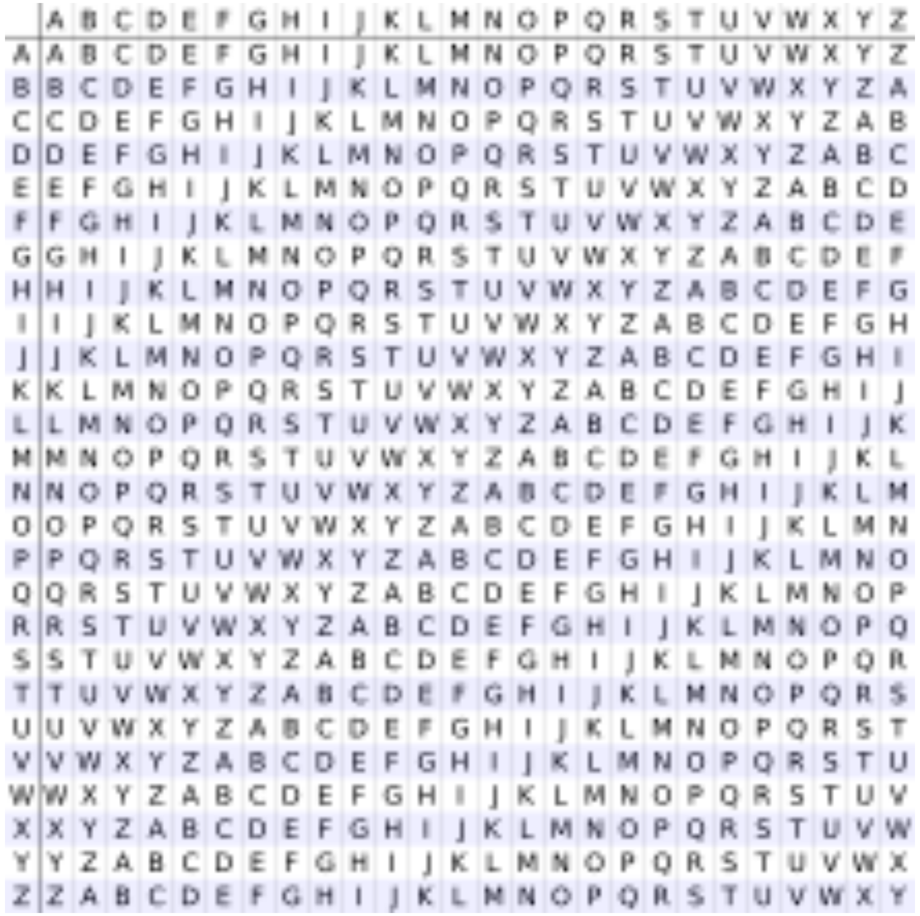


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

The next letter, “i” is shifted by “y”, so it becomes “g”. They continued this method for each letter in the original message to arrive at the encrypted message, “wgmosetdkpsas.”

Vigenère Cipher: Example

Using the Vigenère chart, what would the letter ”g” shifted by “e” become?



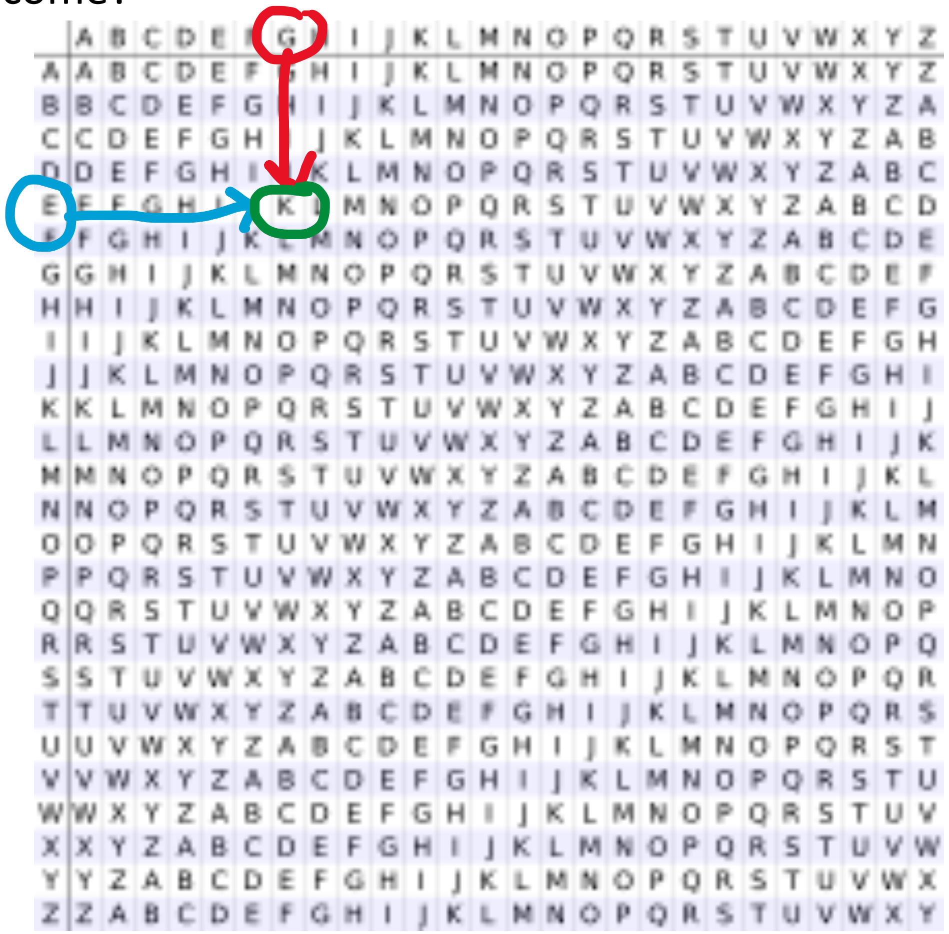
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Quiz 2

- □ k
- □ e
- □ g
- □ a

Vigenère Cipher: Example

Using the Vigenère chart, what would the letter ”g” shifted by “e” become?



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Quiz 2

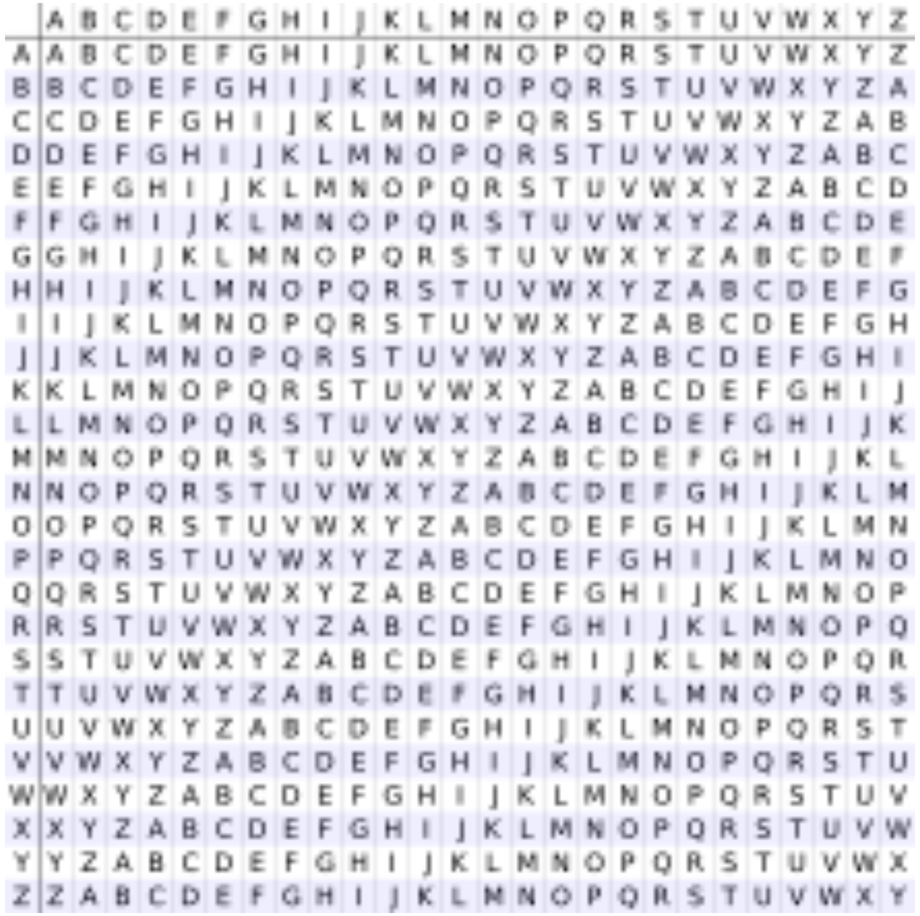
- □ k
- □ e
- □ g
- □ a

Explanation
Correct Answer: k

You’ll notice that if you do the ”opposite” order and shift “e” by “g,” it will also become “k.”

Vigenère Cipher: Example

Using the Vigenère chart, what would the letter ”g” shifted by “a” become?



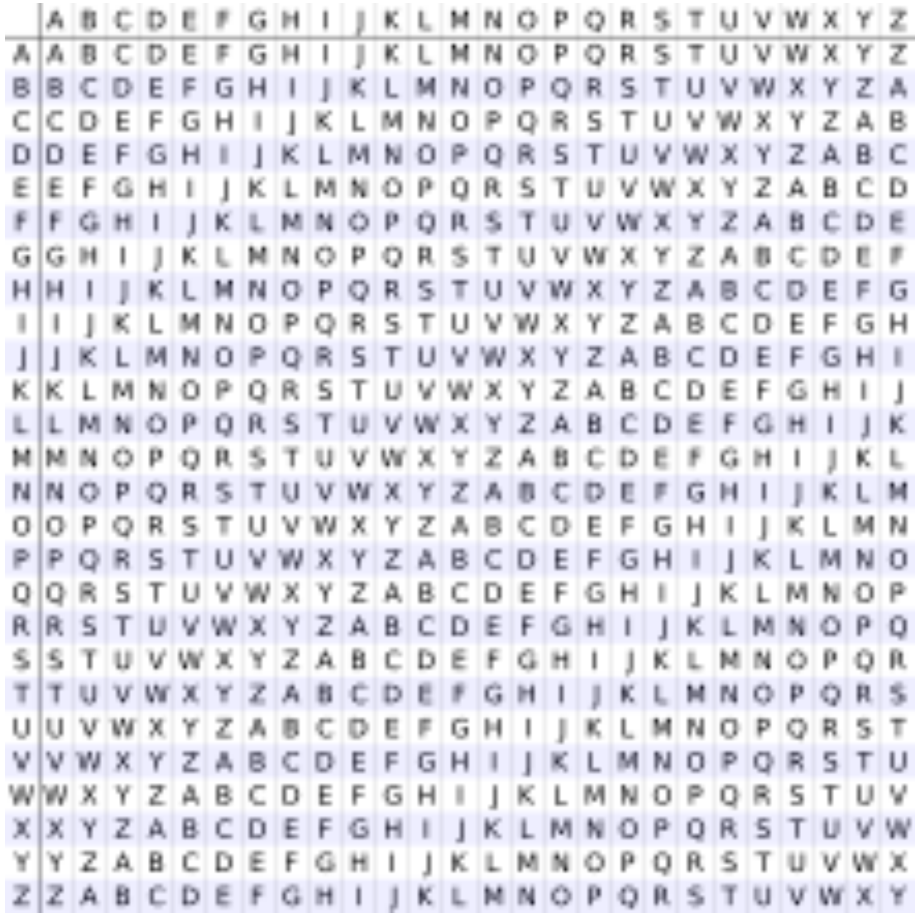
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Quiz 2

- □ k
- □ e
- □ g
- □ a

Vigenère Cipher: Example

Using the Vigenère chart, what would the letter ”g” shifted by “a” become?



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Quiz 2

□ k

□ e

□ g

□ a

Explanation
Correct Answer: g

A shift by “a” is actually no shift at all!

Vigenère Cipher: Example

You just saw that a shift by the keyword letter “a” is actually no shift at all. Looking at the Vigenère table, you’ll notice a shift by ”b” would be a shift of 1. A shift by “c” would be a shift of 2...

This is a pattern which we can use! Each letter in the keyword is almost like doing an individual Caesar Cipher for each letter in the original message.

The keyword letter shows what the Caesar shift should be:

a = 0 shift

b = +1 shift

c = +2 shift ...

What Caesar shift would correspond to the keyword letter “g”?

Quiz 2

- □ 5
- □ 6
- □ 7
- □ -6

Vigenère Cipher: Example

You just saw that a shift by the keyword letter “a” is actually no shift at all. Looking at the Vigenère table, you’ll notice a shift by ”b” would be a shift of 1. A shift by “c” would be a shift of 2...

This is a pattern which we can use! Each letter in the keyword is almost like doing an individual Caesar Cipher for each letter in the original message.

The keyword letter shows what the Caesar shift should be:

a = 0 shift

b = +1 shift

c = +2 shift ...

What Caesar shift would correspond to the keyword letter “g”?

Quiz 2

- □ 5
- □ 6
- □ 7
- □ -6

Explanation
Correct Answer: 6

Even though g is the 7th letter in the alphabet, in order for a to correspond to 0 and b to correspond to 1, g would be 7-1 = 6.

Vigenere Cipher: Python pseudocode

Quiz 2

<drag boxes>

Now that we’ve seen how the Vigenère Cipher relates to the Caesar Cipher, we can use parts of the Python code your friend already wrote to write a new function to create encrypted Vigenère messages.

Looking at this Python *pseudocode* (the ideas behind the code, not the actual syntactically correct code), **drag and drop the boxes into the correct order for creating a Vigenère Cipher program.**

Remove all punctuation and spaces and change all letters to lowercase.

Lengthen keyword to match the length of the original message.

Use Caesar Shift on each letter according to keyword.

Input original message and keyword.

Vigenere Cipher: Python pseudocode

Now that we’ve seen how the Vigenère Cipher relates to the Caesar Cipher, we can use parts of the Python code your friend already wrote to write a new function to create encrypted Vigenère messages.

Looking at this Python *pseudocode* (the ideas behind the code, not the actual syntactically correct code), **drag and drop the boxes into the correct order for creating a Vigenère Cipher program.**

Explanation
Following the steps from your friend’s original Vingenère Cipher and adding our new knowledge about how the keyword shift is just a letter-by-letter Caesar shift, Python must first be given the original message and keyword, then transform it, with the final Caesar shift at the end.

Quiz 2

Input original message and keyword.

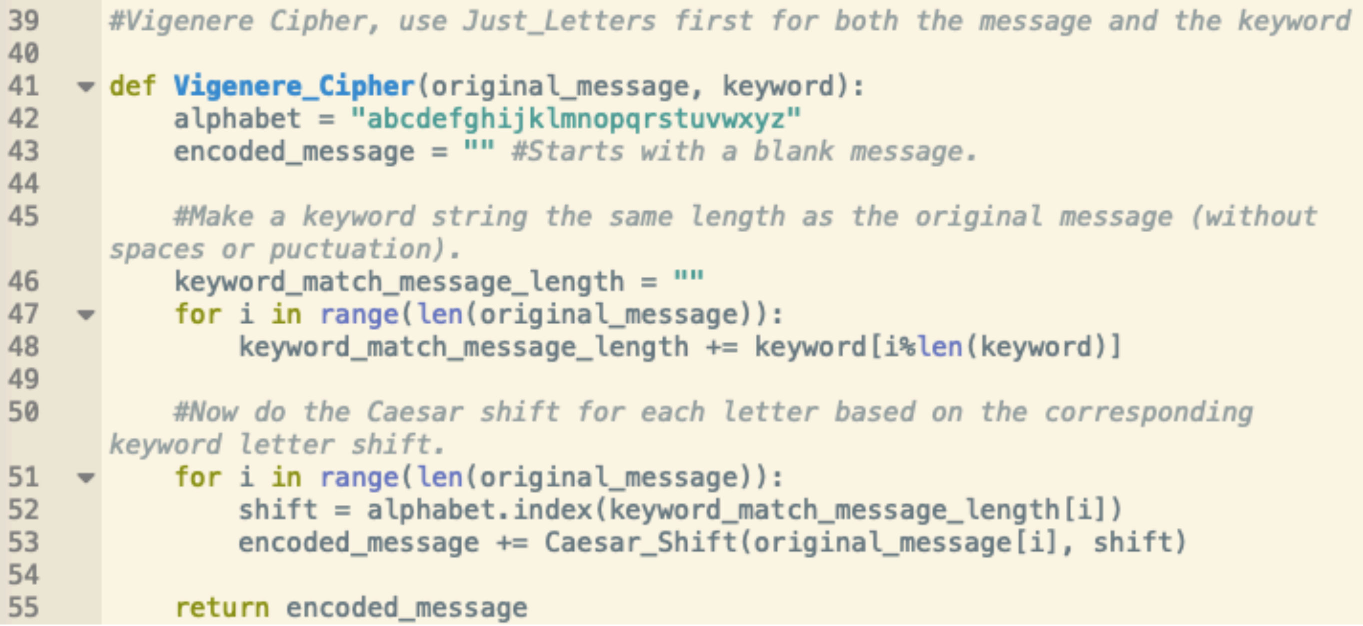
Remove all punctuation and spaces and change all letters to lowercase.

Lengthen keyword to match the length of the original message.

Use Caesar Shift on each letter according to keyword.

Vigenère Cipher: Python code

This is the program your friend wrote to create their Vigenère Ciphers.



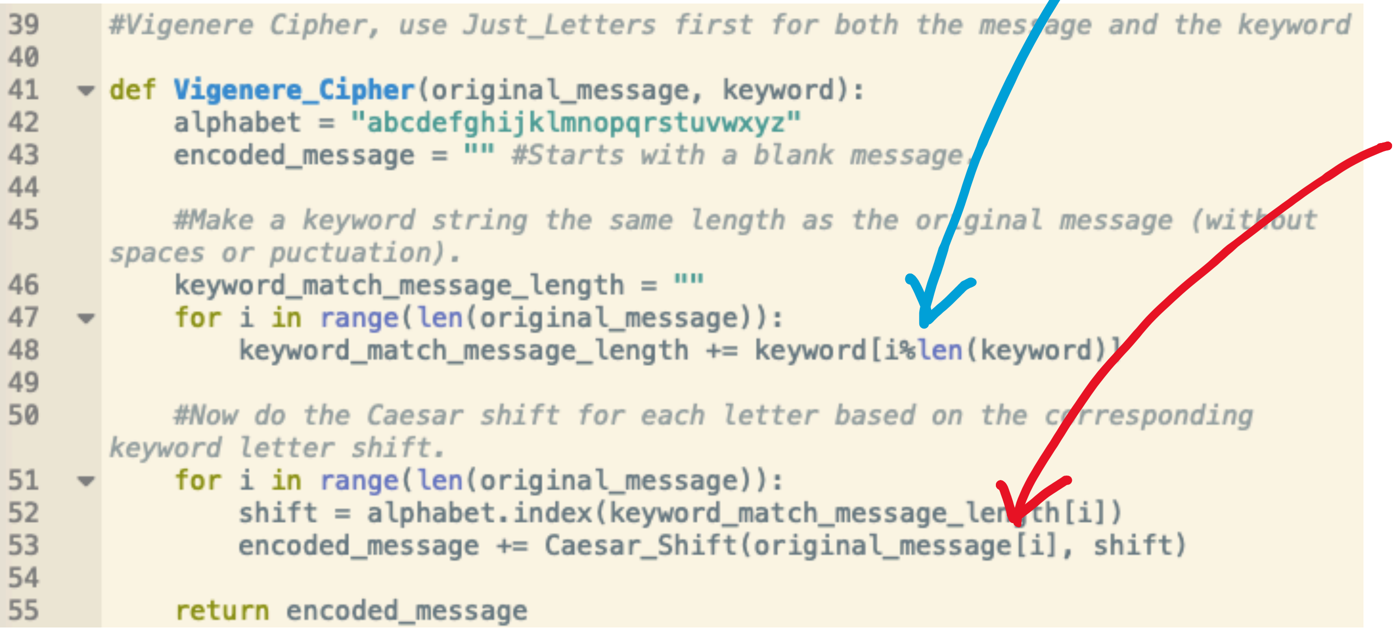
```
#Vigenere Cipher, use Just_Letters first for both the message and the keyword

def Vigenere_Cipher(original_message, keyword):
    alphabet = "abcdefghijklmnopqrstuvwxyz"
    encoded_message = "" #Starts with a blank message.

    #Make a keyword string the same length as the original message (without spaces or puctuation).
    keyword_match_message_length = ""
    for i in range(len(original_message)):
        keyword_match_message_length += keyword[i%len(keyword)]

    #Now do the Caesar shift for each letter based on the corresponding keyword letter shift.
    for i in range(len(original_message)):
        shift = alphabet.index(keyword_match_message_length[i])
        encoded_message += Caesar_Shift(original_message[i], shift)

    return encoded_message
```

It uses the `Just_Letters` code that we used with our Caesar Cipher to get rid of any punctuation, spaces, or capitalization.

Test their code with your own message and keyword. Your input should look like this: `Vigenere_Cipher(Just_Letters(“Hi there, Friend!”), Just_Letters(“Keyword”)).`

Vigenère Cipher: Python code, a final look

Now that you've tested their code, let's see if we can decipher a few final parts of this program.



```
39  #Vigenere Cipher, use Just_Letters first for both the message and the keyword
40
41  def Vigenere_Cipher(original_message, keyword):
42      alphabet = "abcdefghijklmnopqrstuvwxyz"
43      encoded_message = "" #Starts with a blank message
44
45      #Make a keyword string the same length as the orginal message (without
    spaces or puctuation).
46      keyword_match_message_length = ""
47      for i in range(len(original_message)):
48          keyword_match_message_length += keyword[i%len(keyword)]
49
50      #Now do the Caesar shift for each letter based on the corresponding
    keyword letter shift.
51      for i in range(len(original_message)):
52          shift = alphabet.index(keyword_match_message_length[i])
53          encoded_message += Caesar_Shift(original_message[i], shift)
54
55      return encoded_message
```

This % is the same idea as the %26 we saw in the `Caesar_Shift`. This time though, it's wrapping around the *length* or `len` of the keyword.

Line 53 is where `Caesar_Shift` is utilized again. Notice that it has that `[i]` part written next to `original_message`. This is called *indexing* – it's telling Python to use the Caesar Shift on a single letter of the original message at a time.

Vigenere Cipher: What could make THIS cipher harder to crack?

You’ve now learned about two famous methods of ciphering text. The Vigenère is much more complex than the Caesar Cipher, yet you can probably guess that if your nosy housemate knew the keyword they could crack your Vingenère message with some Python code.

As you finish this lesson, let’s brainstorm: **What changes could you make to the Vigenère Cipher to make it harder to crack?**