Girls' Programming Network

Cryptography

Create a Caesar Cipher encryptor and decryptor!

TUTORS ONLY

This project was created by GPN Australia for GPN sites all around Australia!

This workbook and related materials were created by tutors at:

Sydney, Canberra and Perth

Girls' Programming Network

If you see any of the following tutors don't forget to thank them!!

Writers	**Testers**
Renee Noble	Courtney Ross
Sarah Mac	Maddie Jones
Alex McCulloch	Jess Austin
Jess Austin	Maggie Liuzzi
Bhavna Yadav	
Lyndsey Thomas	

Part 0: Caesar Ciphers

Caesar Ciphers are a shift cipher. This means we are going to encrypt messages by shifting the alphabet along and replacing the letters in our secret message.

This is what the alphabet would look like if we shifted it by 3 letters:

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 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

We don't want some of our letters falling off the end so we wrap them around.

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
↓ ↓
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

Another great way to represent this is in a circle! That does the wrapping for us!

To **encrypt** a message we replace a green letter with the matching purple letter:

GPN → JSQ

To **decrypt** a message we take a purple letter and replace it with the matching green letter:

FRGH → CODE

(reading purple to green is the same as rotating the wheel -3)

Task 0.1: Encrypt and decrypting messages

Using the rotated wheel above can you encrypt and decrypt these messages

Encrypt	Decrypt
SECRET → VHFUHW	FUDFN → CRACK
CIPHER → FLSKHU	FDHVDU → CAESAR

Cipher Wheels

Sometimes we want to use **different keys**. So we want a different amount of rotation. We've given you a **cipher wheel** that lets you do this rotation!

Grab your cipher wheel! You can rotate the inner wheel to try different shifts.
Let's give it a try!

Task 0.2: Encrypt with a key of 10!

Let's try using a different key. **Let's try 10**. Rotation your cipher wheel so the **green A** lines up with the **purple K**. **Encrypt** this message:

MYSTERY → W I C D O B I

Task 0.3: Encrypt with a key of 24!

Let's try a **key of 24**. Rotate your wheel 24 spots and **encrypt** this message. (You can ignore spaces)

GPN IS GREAT → E N L   G Q   E P C Y R

Task 0.4: Decrypt with a key of 7!

Let's try a **key of 7**. Rotate your wheel 7 spots and **decrypt** this message:

JYFWAVNYHWOF → C R Y P T O G R A P H Y

Task 0.5: Decrypt with a key of 11!

Let's try a **key of 11**. Rotate your wheel 11 spots and **decrypt** this message:

DATY ESP HSPPW → T H E E A G L E H A S L A N D E D

☑ CHECKPOINT ☑

If you can tick all of these off you can go to Part 1:

☐ You used your cipher wheel!

☐ You encrypted all the message!

☐ You decrypted all the secret messages!

Part 1: Setting up

Task 1.1: Making a python file

Open the start menu, and type 'IDLE'. Select IDLE Python 3.

1. Go to the file menu and select 'New File'. This opens a new window.
2. Go to the file menu, select 'Save As'
3. Choose Desktop and save the file as 'caesar_cipher.py'

TUTOR TIPS

- Make sure they saved it as .py or they won't get syntax highlighting
- Suggest they save it somewhere they can find easily, e.g. Desktop

Task 1.2: You've got a blank space, so write your name!

At the top of the file use a comment to write your name!
Any line starting with # is a comment.

```
# This is a comment
```

☑ CHECKPOINT ☑

If you can tick all of these off you can go to Part 2:

☐ You should have a file called caesar_cipher.py

☐ Your file has your name at the top in a comment

☐ Run your file with F5 key and it does nothing!!

TUTOR TIPS

The code should look like this (no bonuses):

```
# <the student's name>
```

Part 2: Tell me your secrets

Task 2.1: Welcome message

1. Let's `print` out a message to welcome the user.

```
Welcome, this is the Caesar Cipher
```

Hint

If we wanted to print out "Hello, World!" we'd do it like this:
`print("Hello, World!")`

TUTOR TIPS

You may need to remind them to use the F5 key to run the program

Task 2.2: What is your secret message?

1. Use `input` to ask for a secret message. Store the secret in a variable called `message` so we can use it in our code!

Hint

If you want to ask for somebody's name, you can do it like this:
`name = input("What is your name? ")`

TUTOR TIPS

Some students may try and `print` "What's your name", and use single quotes without escaping the apostrophe. Tell them to use double quotes instead.
Incorrect: `print('What's your name?')`
Correct: `print("What's your name")`

Task 2.3: What is the key to your secret message?

1. Use `input` to ask for the key to your secret message. Store it in a variable called `key` so we can use it in our code!

For example, we can print the below when asking the user to input the key:

```
How many letters to rotate by:
```

Task 2.4: Convert key to integer

1. Use `int()` to convert variable `key` to an integer

Task 2.5: Print your secret message

1. Let's `print` our secret message that we got from the user earlier.

☑ CHECKPOINT ☑

If you can tick all of these off you can go to Part 3:
☐ Print a welcome message
☐ Ask for secret message
☐ Ask for key to the secret message
☐ Convert key to integer format
☐ Print your secret message
☐ Run your code

TUTOR TIPS

The code should look like this (no bonuses):

```python
# <the student's name>
print("Welcome, this is the Caesar cipher")
message = input("What's the secret message? ")
key = input("How many letters to rotate by: ")
key = int(key)

print(message)
```

★ BONUS 2.6: What's the name of your secret language?

Waiting for the next lecture? Try adding this bonus feature!!

Let's come up with the name of our secret language and `print` the language of our secret message.

★ BONUS 2.7: Customize welcome message

Waiting for the next lecture? Try adding this bonus feature!!

Let's customise the welcome message for the user.

For example, if the user typed in Lyndsey, then `print` the welcome message for Lyndsey.

```
Welcome to my amazing cipher, Lyndsey
```

TUTOR TIPS

The code should look like this (with bonuses):

```python
# <the student's name>
name = input("What's your name? ")
print("Welcome to my amazing cipher, " + name)
message = input("What's the secret message? ")
key = input("How many letters to rotate by: ")
key = int(key)

print(message)
```

Part 3: Getting a secret letter

Strings and Ints

Task 3.1: How do we get a secret letter?

Let's try doing this with pen and paper!

1. Get the first letter of the word and write it in the second column below.

2. Count how far through the alphabet that letter is. You may want to use your cipher wheels to count with. Put this in the third column. Remember that computers start counting at 0, so you should count like a computer does!

3. Using **5 as the key**, add 5 to the index of that first letter to get our secret letter index. Put that in the fourth column.

4. Now count through the alphabet to find what letter is at the secret letter index. Write it in the last column. Remember again that computers start counting from 0!

5. In the next steps, we'll write code to do this for us!

Message	First letter	Letter Index	Secret Letter Index	Secret Letter
apple	a	0	5	f
banana	b	1	6	g
carrot	c	2	7	h
grapes	g	6	11	L

Hint

Counting the wheel can take a long time. You can use this table to look up the indexes of the letters:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Task 3.2: Let's store the alphabet!

1. Write a variable that stores the alphabet in a string like this:
    ```
    alphabet = 'abcdefghijklmnopqrstuvwxyz'
    ```

Task 3.3: Get a Letter!

1. Now **store the first letter** of the message in a variable called `current_letter`

2. To test your code print out the `current_letter`. Try these examples, write what is printed for `current_letter`! See if it is the first letter of the word!

Message	current_letter
gpn	g
abracadabra	a
pizza	p
zoink	z

Hint

Remember that you can get the first letter of a string like this:
```
name = "gpn"
first_letter = name[0]
```

Task 3.4: Find that letter!

Next we need to figure out where in the alphabet that letter is!

1. **Make a variable** called `current_index` which will store which position in the `alphabet` the `current_letter` is!

2. **Print** out the `current_index` and **write** what number is printed for each of these examples to make sure it's right! Remember that indexes start at 0.

Message	current_letter	current_index
gpn	g	6
abracadabra	a	0
pizza	p	15
zoink	z	25

You can use this to find the index of a letter in a string

```
word = "gpn"
p_index = word.index("p")
```

Task 3.5: Turn the key!

So we've got the position of the original letter, now we have to use the key to shift it to get a new index (later we'll use this to get the secret letter). To do that we need to work out the index of the secret letter which will be the `current_index` plus the key.

1. Make a variable called `new_index` and set it to be the index of the secret letter.

2. Using 5 as the key, print out the `new_index` and write what number is printed for each of these examples to make sure it's right! Remember that it should be what you wrote down for the last task plus your key!

Message	current_letter	current_index	new_index
gpn	g	6	11
abracadabra	a	0	5
pizza	p	15	20
zoink	z	25	30

For example if we wanted to take the message "cipher" the table would look like this:

Message	current_letter	current_index	new_index
cipher	c	2	?

Since our key is 5 and our current_index is 2, we can work out that new_index should be the current_index plus the key, so it's 5+2 which is 7!

Task 2.5: Secret Letter!

Next let's use the new index to get the secret letter from the alphabet.

1. Make a variable called `new_letter` to store the letter in the alphabet that is at the `new_index` position.

2. Print the new letter!

3. Fill out the table below for each of the examples using 5 as the key.

Message	current_letter	current_index	new_index	new_letter
gpn	g	6	11	L
abracadabra	a	0	5	f
pizza	p	15	20	u
zoink	z	25	30	????

Did it work with zoink? Don't worry, we're going to fix it in the next task!

Hint

Remember that you can get a letter out of a string like this:
```
name = "Alex"
index = 2
letter = name[index]
```

Task 3.7: Zoink!

1. What happens when you put in "zoink" and a key of 5?

You get an error!
This is because when you try to go 5 letters past 'z' in the alphabet, there isn't a letter there! To fix this we need to make the index wrap around back to 0 when it gets to the end of the alphabet. We can use modulo to make our code do this!

2. Make the `new_index` be the `new_index` modulo 26
3. Overwrite `new_index` with the modulo version of itself

Hint

To modulo something by 5 you do this:
```
number = 21
number = number % 5
```

This line of code takes the index and makes it wrap around.
```
new_index = new_index % 26
```

Modulo(%) is the remainder.
For example:
10 % 3 is 1.
10 % 5 is 0

☑ CHECKPOINT ☑

If you can tick all of these off you can go to Part 3:
☐ You have printed and checked the current_index of all the examples
☐ You have printed and checked the new_index of all the examples
☐ You have used your cipher wheel to check the new letter of all of the examples

TUTOR TIPS

The code should look like this (no bonuses):

```python
# <the student's name>
alphabet = 'abcdefghijklmnopqrstuvwxyz'

name = input("What's your name? ")
print("Welcome to my amazing cipher, " + name)
message = input("What's the secret message? ")
key = input("How many letters to rotate by: ")
key = int(key)

current_letter = message[0]
current_index = alphabet.index(current_letter)
new_index = current_index + key
new_index = new_index % 26
new_letter = alphabet[new_index]

print(current_letter)
print(current_index)
print(new_index)
print(new_letter)
```

★ BONUS 2.1: zoink, ZoInK and ZOINK

Waiting for the next lecture? Try adding this bonus feature!!

At the moment our code only works with letters that are lowercase. Try entering an ALL CAPS word as your message and see what happens.

To fix this we need to change the message to be all lowercase. We can use `message = message.lower()` to do that.

Update your code so we're always using the lowercase version of the message!

TUTOR TIPS

The code should look like this (with bonuses):

```python
# <the student's name>
alphabet = 'abcdefghijklmnopqrstuvwxyz'

name = input("What's your name? ")
print("Welcome to my amazing cipher, " + name)
message = input("What's the secret message? ")
message = message.lower()
key = input("How many letters to rotate by: ")
key = int(key)

current_letter = message[0]
current_index = alphabet.index(current_letter)
new_index = current_index + key
new_index = new_index % 26
new_letter = alphabet[new_index]

print(current_letter)
print(current_index)
print(new_index)
print(new_letter)
```

Part 4: What about words?

Task 4.1: Not just one letter

1. On your cipher wheel, try and code 'gpn' with a **key of 4**, what letters do you get?

gpn = _k t r_

2. Now try putting "gpn" with a key of 4 into your program and seeing if they match.

Did it match what you did by hand?

Right now your code only gets the first letter of the message variable. The computer doesn't know that there are more letters in `message`, we need to tell it!

Task 4.2: Not just one letter

1. First we can remove the code that sets the `current_letter` variable to the first letter of your message. You can do this by making the whole line into a comment.

Hint

Remember:
```
# this is a comment
```

Task 4.3: Working letter by letter

Now we want to add a `for` `loop` so that the computer looks at every letter in the message and turns it into a secret letter.

1. Add the `for` `loop` right under the comment you just made.

Hint

Here's an example of a for loop. Don't forget that when you code a for loop you need to use indents.

```
for letter in word:
    print(letter)
```

Task 4.4: Check the whole secret word

1. Use your cipher wheel to encrypt a 3 letter word, like 'gpn', rotated by 6.

$$g \ p \ n \rightarrow m \ v \ t$$

2. Now type that word and key into your encryptor and see if they match.

3. If it's working you can move onto the next step.

Task 4.5: Everybody get in line!

1. Try your program with a long word like 'zooperdooper'.

The secret word is way too
L
O
N
G
!

Let's print it on one line so that it is easy to read.

Hint

Use the `print(variable, end='')` that you learned in lecture slides to print your secret word on one line.

☑ CHECKPOINT ☑

If you can tick all of these off you can go to Part 4:
☐ Used a comment to remove a line of code
☐ Added a for loop
☐ Check your code with a 3 letter word
☐ Print the word on one line

TUTOR TIPS

The code should look like this (no bonuses):

```
# <the student's name>
alphabet = 'abcdefghijklmnopqrstuvwxyz'

name = input("What's your name? ")
```

```
print("Welcome to my amazing cipher, " + name)
message = input("What's the secret message? ")
message = message.lower()
key = input("How many letters to rotate by: ")
key = int(key)

# current_letter = message[0]
for current_letter in message:
    current_index = alphabet.index(current_letter)
    new_index = current_index + key
    new_index = new_index % 26
    new_letter = alphabet[new_index]

    print(new_letter, end='')
```

★ BONUS 4.6: Take your time

Waiting for the next lecture? Try adding this bonus feature!!

Let's make it look like the computer is thinking very carefully about each letter before it encrypts it.

1. Add `import time` to the very top of your code.

2. At the end of your loop type `time.sleep(0.2)`

This will make the computer wait for 0.2 seconds before it gets the next letter.
Run your code and see what happens. Try other numbers like `0.4` or `1`

TUTOR TIPS

The code should look like this (with bonuses):

```
# <the student's name>
import time
alphabet = 'abcdefghijklmnopqrstuvwxyz'

name = input("What's your name? ")
print("Welcome to my amazing cipher, " + name)
message = input("What's the secret message? ")
message = message.lower()
key = input("How many letters to rotate by: ")
key = int(key)

# current_letter = message[0]
for current_letter in message:
    current_index = alphabet.index(current_letter)
    new_index = current_index + key
    new_index = new_index % 26
    new_letter = alphabet[new_index]
```

```
    print(new_letter, end='')
    time.sleep(0.2)
```

Part 5: Dealing With Spaces

Task 5.1: Testing With A Space!

1. Test your code with 2 words now instead of one, what happens?

You should get a ValueError, this is because the program doesn't know what a space is!

Task 5.2: What If?

To fix this issue, we are going to add some `if` statements to check if the character is in the alphabet variable.

1. In your loop add a line to check if the current letter is in the alphabet

2. If the character is in the alphabet, we want to make it secret with our code indent your code into the `if` statement

Task 5.3: Ignore the spaces

1. Create an else statement to handle when characters are not in the alphabet.
2. Inside the else statement, print the character you are on, but don't encrypt it. Make sure they stay on the same line too.

Hint

An `else` always needs to be attached to an `if` statement
```
if raining == True:
  print ( 'oh no!' )
else:
  print ( 'Yay!' )
```

TUTOR TIPS

The code should look like this (no bonuses):

```
# <the student's name>
import time
alphabet = 'abcdefghijklmnopqrstuvwxyz'

name = input("What's your name? ")
print("Welcome to my amazing cipher, " + name)
message = input("What's the secret message? ")
message = message.lower()
```

```python
key = input("How many letters to rotate by: ")
key = int(key)

# current_letter = message[0]
for current_letter in message:
    if current_letter in alphabet:
        current_index = alphabet.index(current_letter)
        new_index = current_index + key
        new_index = new_index % 26
        new_letter = alphabet[new_index]

        print(new_letter, end='')
    else:
        print(current_letter, end='')
        time.sleep(0.2)
```

☑ CHECKPOINT ☑

If you can tick all of these off you can go to Part :

☐ You have an `if` and `else` statement

☐ If your code can make more than one word secret

☐ Print out a secret sentence

TUTOR TIPS

Some students may forget the colon after the else as well.
Make sure they also print in the else, otherwise those characters will be skipped.

Part 6: Let's Get Cracking!

Task 6.1: Make a Secret Code!

Before we can crack some codes, we need a message to decrypt.

Use your program to get a secret message that we can decrypt (write down your key!!)
Fill in the table below so that we can decrypt it later!

Original Message	Key	Encrypted Message
example	10	O h k w z v o
test case	15	l t h i r p h t
Get the kids to do their own test. These are just some examples		

Task 6.2: To encrypt or decrypt?

At the moment your program can make a secret code, but if we gave that code to someone else, they won't be able to read it!

We will need to add a mode where you can turn the secret message back into normal words using the same key that we used to make the secret message.

We can call the modes `'e'` for encrypt and `'d'` for decrypt.

Use an `input`() statement before the `for` loop to ask the user which mode they would like to use.

Task 6.3: Not So Secret Anymore!

If the user chooses mode `'d'` we will need to change the key value to become the opposite of the coding key value

This can be done by multiplying the key with -1 to create the negative number of the key.

Wrap this key change in an if statement if the user chooses mode `'d'` before the start of the for loop.

For example: If the letters in the word were changed by 3 letters to encrypt the secret word, the letters need to be changed back by 3 letters.

Operators in python

*	Multiplication
/	Division
+	Add
-	Minus

☑ CHECKPOINT ☑

- ☐ Encrypts messages
- ☐ Decrypts messages with correct key
- ☐ Prints original message

TUTOR TIPS

The code should look like this (no bonuses):

```python
# <the student's name>
import time
alphabet = 'abcdefghijklmnopqrstuvwxyz'

name = input("What's your name? ")
print("Welcome to my amazing cipher, " + name)
message = input("What's the secret message? ")
message = message.lower()
key = input("How many letters to rotate by: ")
key = int(key)

mode = input("Do you want to encrypt or decrypt? (e or d) ")
if mode == 'd':
    key = key * -1

# current_letter = message[0]
for current_letter in message:
    if current_letter in alphabet:
    current_index = alphabet.index(current_letter)
    new_index = current_index + key
    new_index = new_index % 26
    new_letter = alphabet[new_index]
```

```python
        print(new_letter, end='')
    else:
        print(current_letter, end='')
    time.sleep(0.2)
```