Python Programming and Cryptography

Mckenzie Mack

GenCyber Workshop

Agenda

- Programming Languages
- Programming in Python
- Cryptography
- Encryption: The Caesar Cipher

Learning Objectives

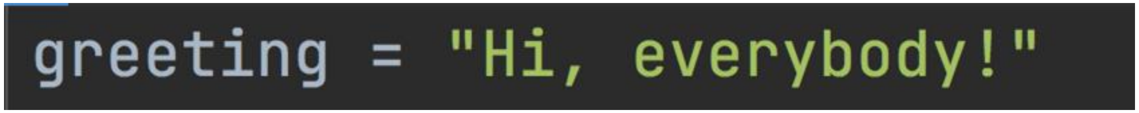
- Demonstrate how to implement simple programming concepts in Python, including variables, if statements, and for loops
- Explore the concept of cryptography and how it relates to application security
- Define encryption and decryption in terms of their relation to cryptography
- Describe how the Caesar cipher algorithm is used for encryption and decryption

Programming Languages

- How does a programmer talk to a computer in a way that they both understand?
  - programmers write in **high-level programming languages**, which allow coders to write instructions in a way that humans can understand
    - the **compiler** translates the high-level language to machine language that the computer understands
  - There are lots of programming languages out there
    - We will be using **Python**, a popular language that's easy to learn

Programming in Python

- To create a variable in Python, use the format **x = y** where **x** is the name of the variable and **y** is its value

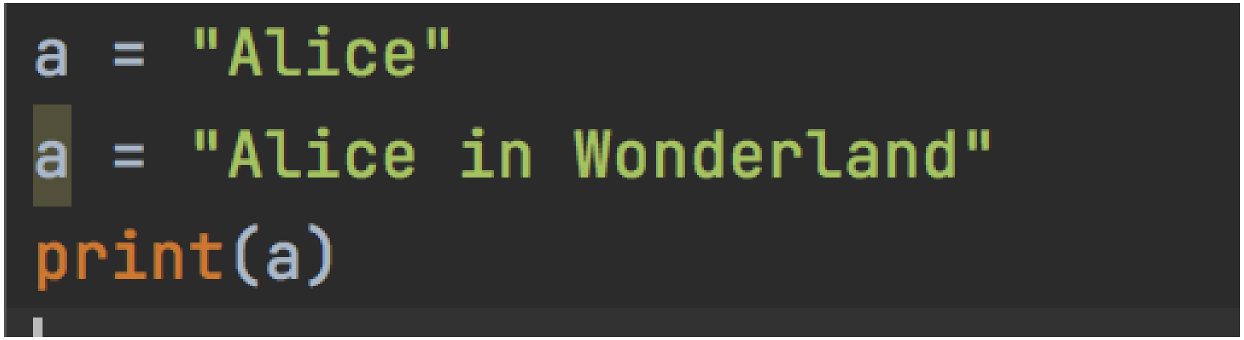


```
greeting = "Hi, everybody!"
```

- The programmer does not have to explicitly state the type of the variable
  - Python sets the data type based on the value of the variable
- Variable names are case-sensitive
  - ex: **name** and **Name** would be two different variables

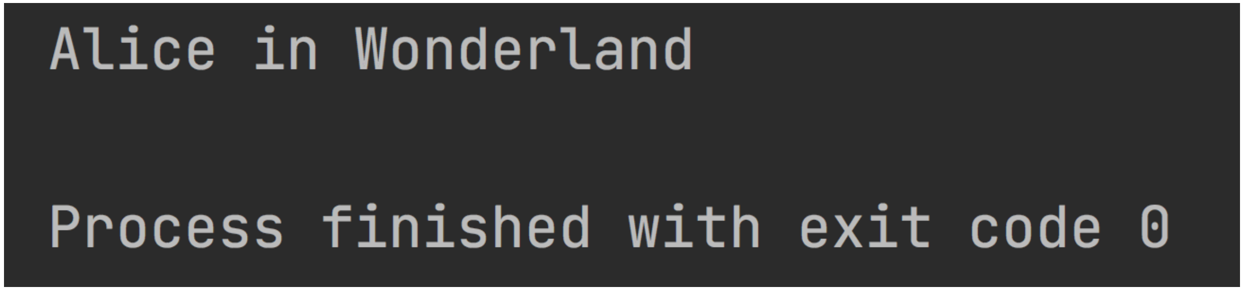
Programming in Python

- The value of the variable can be changed if another assignment statement is used with the same variable name



```
a = "Alice"
a = "Alice in Wonderland"
print(a)
```

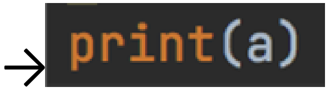
- Output:

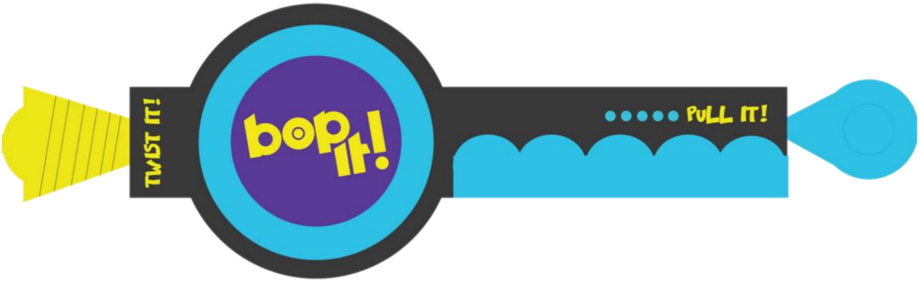


```
Alice in Wonderland

Process finished with exit code 0
```

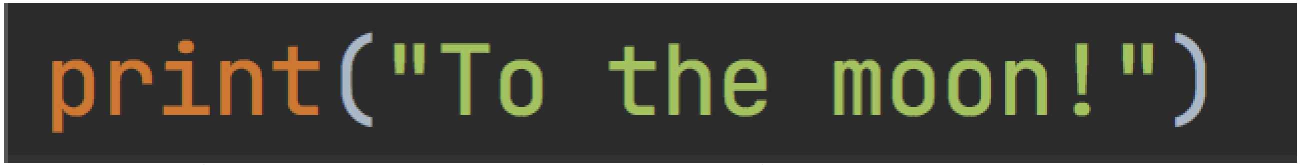
Programming in Python

- You may have noticed this →  `print(a)` on the last slide
- this is an example of a **function**
  - function: section of code that performs a specific task when the function is called
  - think about playing bop it!
    - when the voice calls, “bop it!”, you press the button
    - when the voice calls, “twist it!”, you twist the yellow knob
  - functions work in a similar way



Programming in Python

- to call a function, type the name of the function along with any **arguments** to be passed to the function
  - think of the arguments as input for the function
  - place arguments in parentheses or leave the parentheses empty if none are required



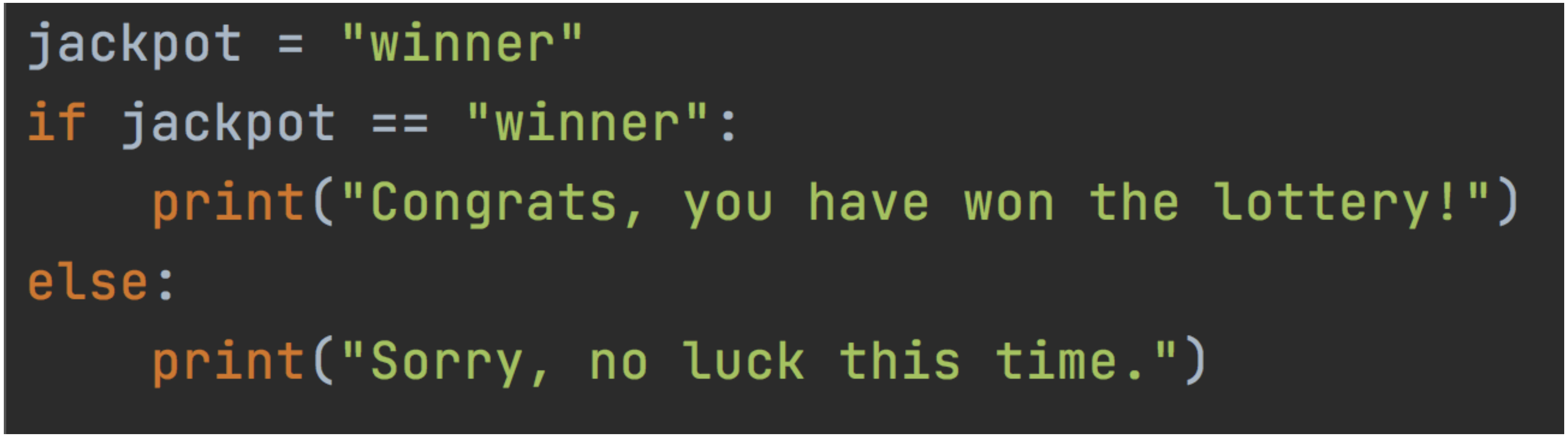
```
print("To the moon!")
```

function

argument

Programming in Python

- to implement the if...else statements that we talked about in the earlier lesson, use the following format:

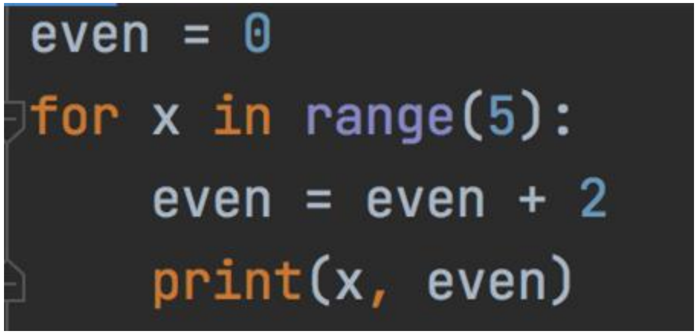


```
jackpot = "winner"
if jackpot == "winner":
    print("Congrats, you have won the lottery!")
else:
    print("Sorry, no luck this time.")
```

- **Note**: always indent the lines that follow the if and else statements

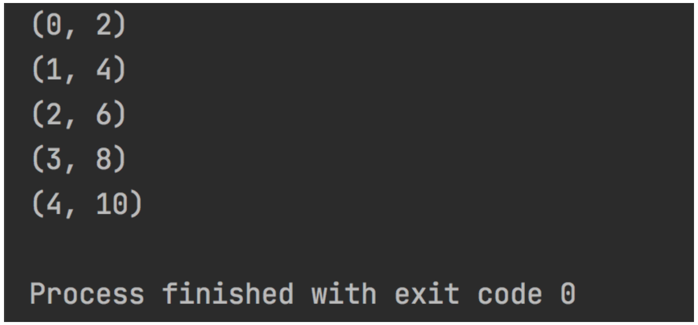
Programming in Python

- to use a for loop:



```python
even = 0
for x in range(5):
    even = even + 2
    print(x, even)
```

- Output ------->



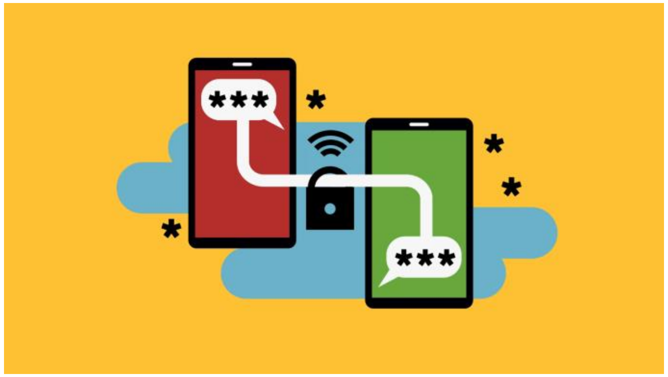
```
(0, 2)
(1, 4)
(2, 6)
(3, 8)
(4, 10)

Process finished with exit code 0
```

- **Note: range(5)** could be replaced by a variable, string, etc.
- a **break statement** can also be added to the indented portion of the for loop to exit the for loop early

Cryptography

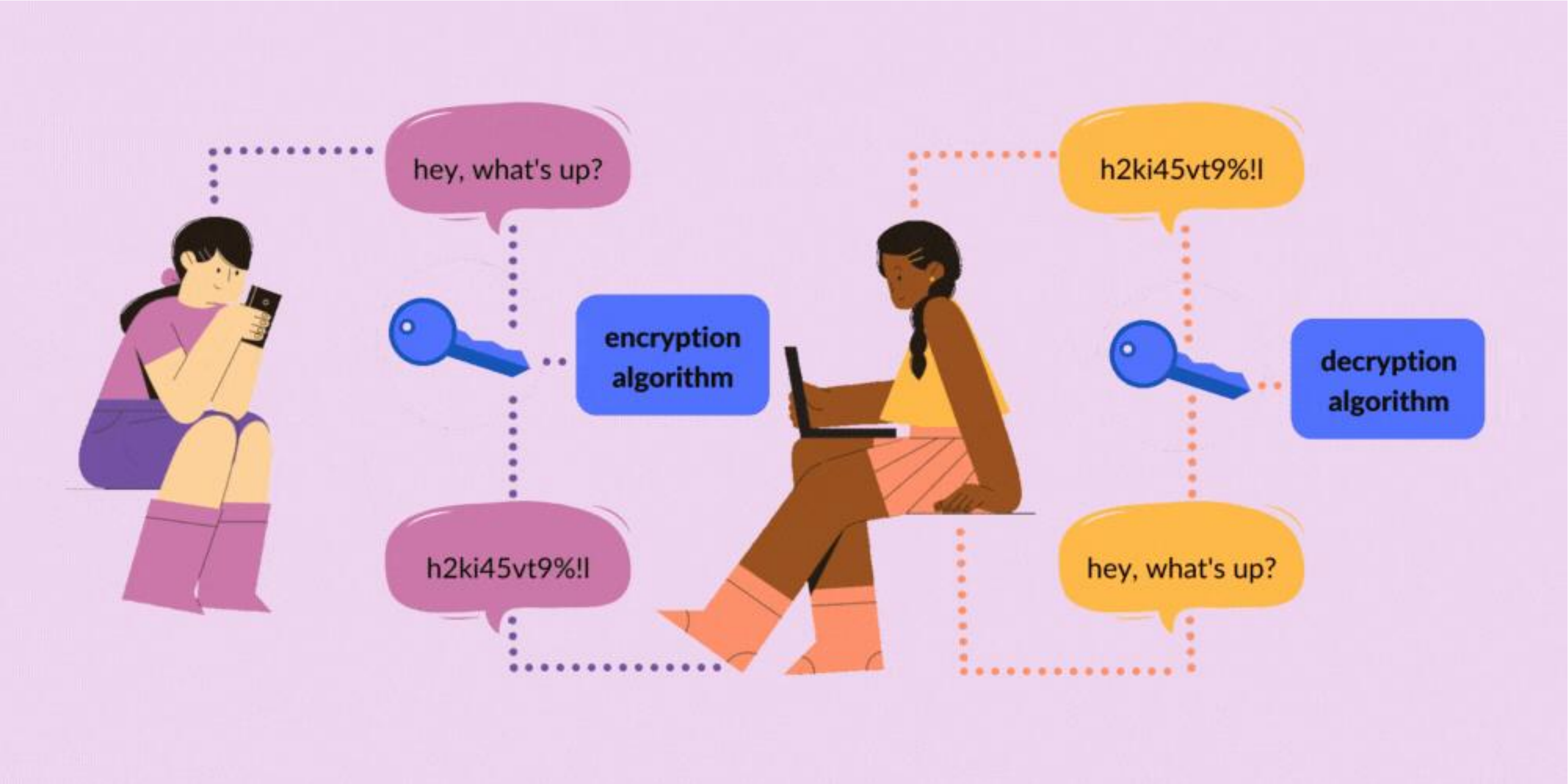
- You probably wouldn’t want everyone seeing the messages that you send on Snapchat
  - How can we using the programming techniques that we have talked about to protect information that we send across applications?
  - Snapchat secures your messages by using **cryptography**
    - cryptography: literally means secret writing
    - art of transforming messages to make them secure
    - you’ve probably used methods of cryptography without even knowing it!



Cryptography

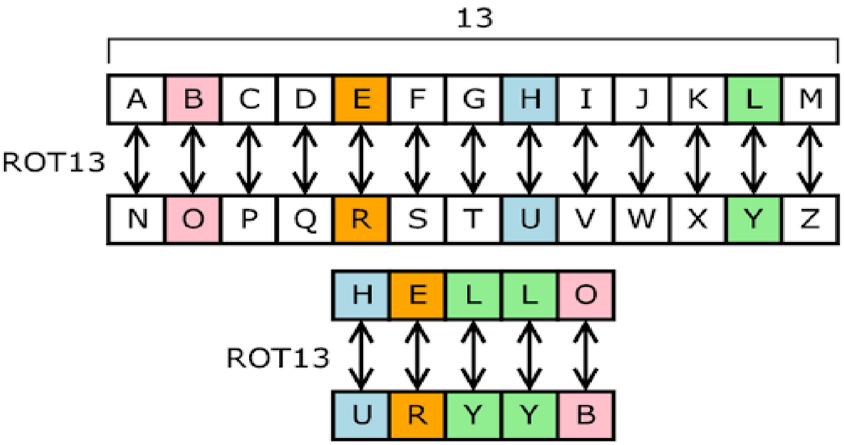
- How cryptography works:
  - two parties have a key that no one else has access to
  - one party uses the key and an algorithm to convert their message (known as **plaintext**) to a secret coded message (known as **ciphertext**)
    - the process of converting plaintext to ciphertext is called **encryption**
  - once the other party gets the message, they use the key and an algorithm to convert the coded message back to the original message so that it can be read
    - this process is known as **decryption**

Cryptography



Encryption: The Caesar Cipher

- One of the earliest encryption algorithms is the **Caesar cipher**
  - invented by Julius Caesar in Ancient Rome
  - to encrypt a message, shift each letter a certain number of times in the alphabet
  - to decrypt the message, shift each letter the same number of times the opposite way
  - in this case, the key is the number of shifts



13

	A	B	C	D	E	F	G	H	I	J	K	L	M
ROT13	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

	H	E	L	L	O
ROT13	↕	↕	↕	↕	↕
	U	R	Y	Y	B

Resources

- https://www.youtube.com/watch?v=Y8Tko2YC5hA
- https://docs.python.org/3/tutorial/controlflow.html
- https://www.youtube.com/watch?v=jhXCTbFnK8o&t=67s

LAB

- complete the questions for the Lab - Write the Caesar Cipher