

Python Basics 2

If Condition

- ال if ومن اسمها شارحه نفسها بمعنى "لو دا اتحقق اعلمي كذا"
- يعني ايه برضو مش فاهم؟ تعالى افهمك

```
#!/usr/bin/python3
x = 10
if x > 5: # لو اتحقق اعلم اللي تحت
    print(f"the number {x} is bigger than 5")
elif x < 5: # لو اللي قبلي متنفذش بص علي ده
    print(f"the number {x} is smaller than 5")
else: # لو مفيش حاجه من فوق متحققش اعلمي ده بقي واخلص
    print(f"the number {x} is crazy")
```

- واحده واحده وتعالى نفهم

الشرح

- اول حاجه انا عملت متغير اسمه x وخزنت فيه رقم 10
- بعد كذا عملت if بقولو يا باشا لو ال x اكبر من 5 اطبعلي الجملة دي
-لو اتحقق الشرط ده تمام وخلاص واقفل البرنامج
-لو متحققش شوف اللي بعدي لو انا عامل else if او else انما لو مش عامل يبقي خلاص
- هنجي نبص هنا هنلاقي اه في else if اللي هيا elif
- بيقولي هنا لو ال x اصغر من ال 5 اطبعلي الجملة دي
-لو اتحقق الشرط تمام وخلاص واقفل
-لو متحققش شوف اللي بعدي ولو مفيش حاجه بعدي خلاص اقفل
- اخر حاجه else يعني لو كل اللي فوق دول متحققش اعلمي ده اطبعلي الجملة يعني

مثال

- تعالى مثلا نفترض اني الرقم هو 5
- اول حاجه هنخش ف اول شرط هل الرقم اكبر من 5 ؟ لا طبعا دا ببساويه
 - ننزل علي اللي بعده هل ال 5 اصغر من ال 5 ؟ اكيد لا دي ببساويه
 - تالت حاجه بيقولي لو كل دول متحققش اعلمي ده

Functions

- الفانكشن معناها اني بعمل block of code بحيث تكون الفانكشن دي بتعملي مهمه معينه
- ممكن بقي اقسام اخلي كل function بتعملي حاجه مختلفه عن التانيه
- عشان اكريت فانكشن بنكتب

```
def <function-name>():  
    function-body  
<function-name>()
```

- خلي بالك لما تعمل الفانكشن وتسيبها كدا انت تمام عادي ومفيش حاجه بس مش هتتنفذ
- لازم اعملها call عشان تتنفذ زي ما وضحت فوق كدا

```
#!/usr/bin/python3  
def firstfun():  
    print("Hi iam here")  
firstfun()
```



Comments

- عشان تعمل كومننت لأي حاجه حط قبلها #



Open System Files and Execute Commands

- عشان افتح ملف معين بالبايثون لازم احدد انا هعمل ايه فيه هل انا عاوز اقرأه بس؟ طب هعدل عليه؟ طب هنفذه او هخليه يشتغل يعني؟

```
#!/usr/bin/python3  
file = open("/home/kali/file.txt", "r")  
print(file.read())
```

- واحدده واحده اول حاجه فانكشن open دي بتخليني أأكسس علي اي فايل جوا النظام
- open("/home/kali/file.txt", "r")
- اول حاجه بكتب مساره عشان اقله انا عاوز انه يملف
- ثاني حاجه بحدد المود هل انا عاوز اقرأ الملف بس او اعدل عليه ولا اعمل ايه
- -read() print(var-name.read()) => r => اقرأه بس
- -write("text") var-name.write("text") => w => اعدل عليه بس هيمسح اللي كان موجوده وهيحط مكانه
- -write("text") var-name.write("text") => a => اعدل عليه بس بضيف علي اللي موجود
- -execute() var-name.execute() => x => اشغله

س

```
#!/usr/bin/python3
import os
os.system("ls")
```

- الكود دا بينفذلي اوامر من خلال ملف بايثون
- اولاً لازم استدعي مكتبة os عشان دي المسؤوله عن عمل اوامر اللينكس
- بعد كذا بكتب os.system("command")
- اول لما تشغل ملف البايثون الامر هيتنفذ علاطول

```
#!/usr/bin/python3
import os
target=input("please enter domain to scan: ")
os.system(f"nmap {target}")
```

- ركز ف الكود ده وافهمه كويس اعتقد انه مش محتاج شرح

س

Encryption and Decryption with Python

- طبعا عارفين نظام التشفير بيكون عبارته عن مفتاحين مفتاح بيستخدم لعمل التشفير (Public Key) ومفتاح ثاني بنفك بيه التشفير (Private Key)

- احنا بقي هنتعلم نعمل المفتاحين دول ونشفر رساله بسيطه كدا

تعالى نعمل اول حاجه المفتاحين كدا

```
#!/usr/bin/python3
import rsa
publickey, privatekey = rsa.newkeys(512)
print(publickey)
print(privatekey)
```

- احنا هنا عملنا استدعاء للمكتبة بتاعت ال rsa ودي لازم استدعيها عشان دي المسؤوله عن عمل مفاتيح التشفير
- بعد كدا لازم نعمل (publickey, privatekey = rsa.newkeys(512) دي بالشكل دا لازم متغيرين هنا عشان هما مرتبطين ببعض مش شرط يكون اسمهم كدا بس حط حاجه معبره يعني عشان متلغبطش بعدين بس اهم حاجه اني لازم احط الاتنين كدا وال 512 دي بحددلو حجم المفتاح بالبت
- وبعد كدا بقولو اطبعهملي عادي
- طب انت كدا عملت المفتاح هنشفر ايه يعني ولا هنعمل ايه.....تعالى اقولك

تشفير رساله بسيطه وفك تشفيرها

```
#!/usr/bin/python3
import rsa
message = b"this is a encrypted message!"
public, private = rsa.newkeys(512)
cipher = rsa.encrypt(message, public)
print(cipher)
```

- بص يا باشا انا لو هشفر رساله لازم احط قبلها b عشان التشفير مبينفعش مع ال string فا احنا بنحولول bytes
- بعد كدا بعمل المفتاحين عادي جدا
- هنا (rsa.encrypt(message, public) بقولو يا باشا شفرلي المتغير اللي اسمه message وشفرهولي بالpublic (زي ماقولنا فوق اني ال public key هو اللي بيشفّر وال private هو اللي بيفك) وبعد كدا خزنهولي في متغير اسمه cipher ممكن انت تسميه اي اسم
- اخر حاجه بقولو اطبعلي بقي التشفير دا تعالي كدا اوريك شكله عامل ازاي

```
(kali@kali)-[~/Downloads]
$ python3 file.py
b'\x15b\x1a\x84*\x86J\xe3\x0c\xaf\x88\x96\xd9\xdf!\x15\xbf\xc6\x05T{\xc5x=,\x1e\xc4\xd6\xa7\xa0\xd6%\x04\x1btU\x88q\x8f\xd2~\xdf\xe3~x\xcd\x9b\x89pjDM\xf6$\x86\xa2\xb7\x96ml\xb3\xd7\x17'
```

- بص شكله عامل ازاي عشان مشفر طبعا تعالي بقي نفك التشفير

```
#!/usr/bin/python3
import rsa
message = b"this is a encrypted message!"
public, private = rsa.newkeys(512)
```

```

cipher = rsa.encrypt(message, public)
print(cipher)
plain = rsa.decrypt(cipher, private)
print(plain)

```

- بص يامعلم هنا نفس الامر برضو اختلف حاجات بسيطه بس
- امر فك التشفير `rsa.decrypt(cipher, private)` ويقولو خزنهولي ف متغير اسمه `plain` وخلي بالك اني هنا بديلو الماسدج المتشفره اصلا اللي هيا `cipher` مش `message` لو اديتلو `message` هيقولك انت عبيط؟ انت عاوز افك تشفير رساله هيا متشفره اصلا!!!.....او مال ايه المتشفر ماهو المتشفر حاليا هو ال `cipher` يارب تكون النقطه دي وضحت
- تعالي بقي اوريك النتيجة بعد ما فكينا التشفير

```

(kali@kali)~[~/Downloads]
$ python3 file.py
b'a!2\x14\xcd\xbe0\xa4B#\xb1\xec\x84\x187)\x19\xb3\xdc%1\xf5\xffv\x14.\x0b\xed\x0bh\xfb?{\r\xb3\xa2\xe6\x89S\xb
bT\xf5\xf0\r\t\x9d\xd16\xcb\xfe\xc8\xc9\x0eU\xd9W\x1b\x04\x9e\x94\xf4l\xe3\x91'
b'this is a encrypted message!'

```