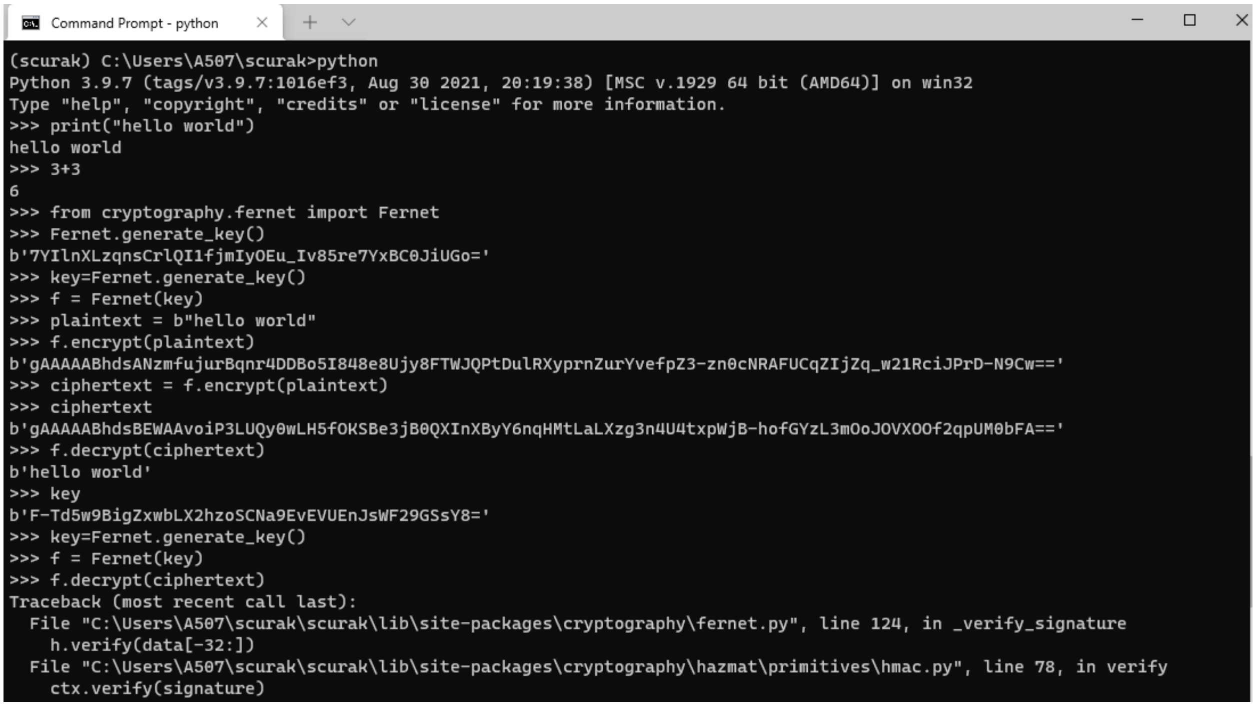
LAB 2

Symmetric key cryptography - a crypto challenge

Zadatak je bio riješiti odgovarajući crypto izazov. Plaintext koji je trebalo otkriti enkriptiran je korištenjem *high-level* sustava za simetričnu enkripciju iz navedene biblioteke Fernet. Bez pristupa enkripcijskom ključu, trebalo je dešifrirati odgovarajući ciphertext.

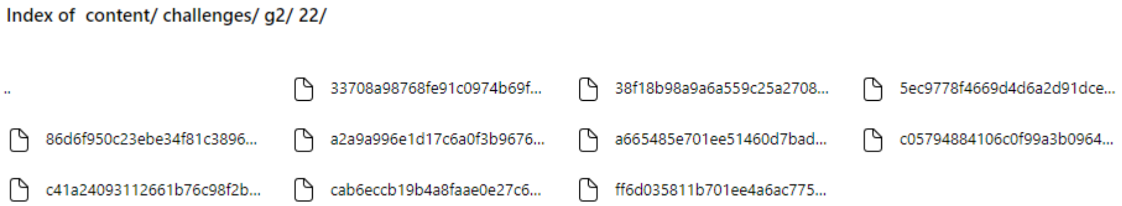
Prvo smo otvorili Python virtualno okruženje. Za enkripciju smo koristili Python biblioteku cryptography.



```
(scurak) C:\Users\A507\scurak>python
Python 3.9.7 (tags/v3.9.7:1016ef3, Aug 30 2021, 20:19:38) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> print("hello world")
hello world
>>> 3+3
6
>>> from cryptography.fernet import Fernet
>>> Fernet.generate_key()
b'7YIlnXLzqnsCrlQI1fjmIyOEu_Iv85re7YxBC0JiUGo='
>>> key=Fernet.generate_key()
>>> f = Fernet(key)
>>> plaintext = b"hello world"
>>> f.encrypt(plaintext)
b'gAAAAABhdsANzmfujurBqnr4DDBo5I848e8Ujy8FTWJQPtDulRXyprnZurYvefpZ3-zn0cNRAFUCqZIjZq_w21RciJPrD-N9Cw=='
>>> ciphertext = f.encrypt(plaintext)
>>> ciphertext
b'gAAAAABhdsBEWAAvoiP3LUQy0wLH5fOKSBe3jB0QXInXByY6nqHMtLaLXzg3n4U4txpWjB-hofGYzL3mOoJOVXOOf2qpUM0bFA=='
>>> f.decrypt(ciphertext)
b'hello world'
>>> key
b'F-Td5w9BigZxwbLX2hzoSCNa9EvEVUEnJsWF29GSsY8='
>>> key=Fernet.generate_key()
>>> f = Fernet(key)
>>> f.decrypt(ciphertext)
Traceback (most recent call last):
  File "C:\Users\A507\scurak\scurak\lib\site-packages\cryptography\fernet.py", line 124, in _verify_signature
    h.verify(data[-32:])
  File "C:\Users\A507\scurak\scurak\lib\site-packages\cryptography\hazmat\primitives\hmac.py", line 78, in verify
    ctx.verify(signature)
```

Kratko upoznavanje s Fernetom.

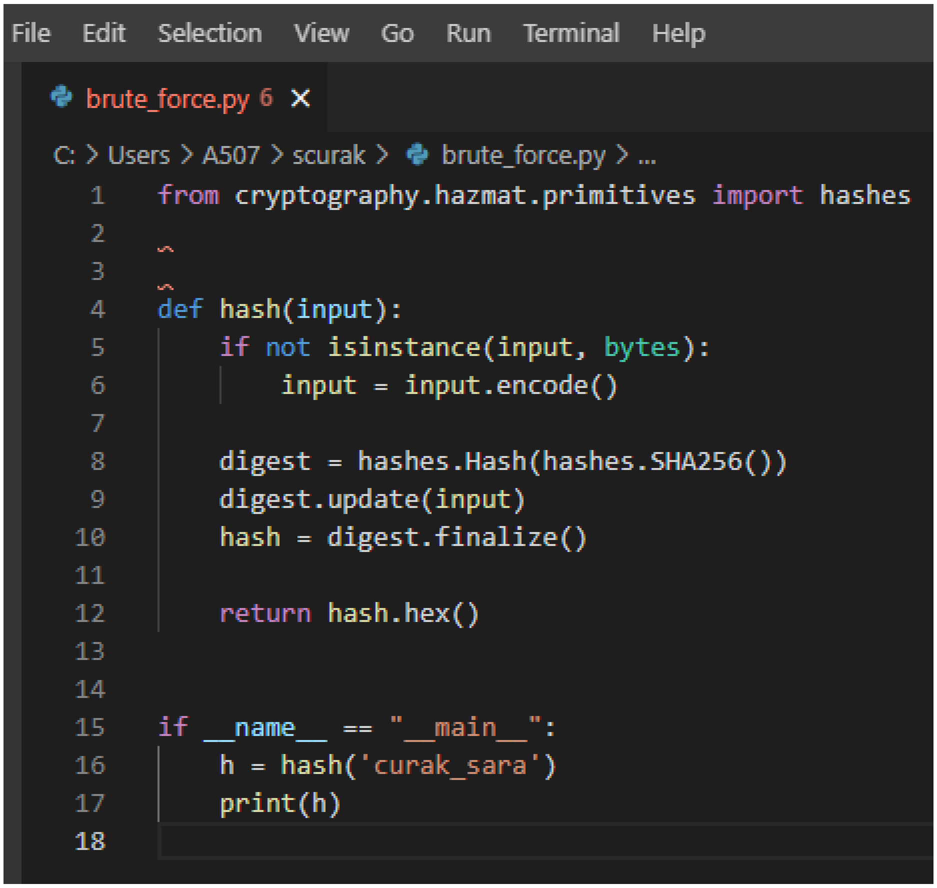
Zatim je uslijedio **Crypto challenge.**



Index of content/ challenges/ g2/ 22/

..
33708a98768fe91c0974b69f...
38f18b98a9a6a559c25a2708...
5ec9778f4669d4d6a2d91dce...
86d6f950c23ebe34f81c3896...
a2a9a996e1d17c6a0f3b9676...
a665485e701ee51460d7bad...
c05794884106c0f99a3b0964...
c41a24093112661b76c98f2b...
cab6eccb19b4a8faae0e27c6...
ff6d035811b701ee4a6ac775...

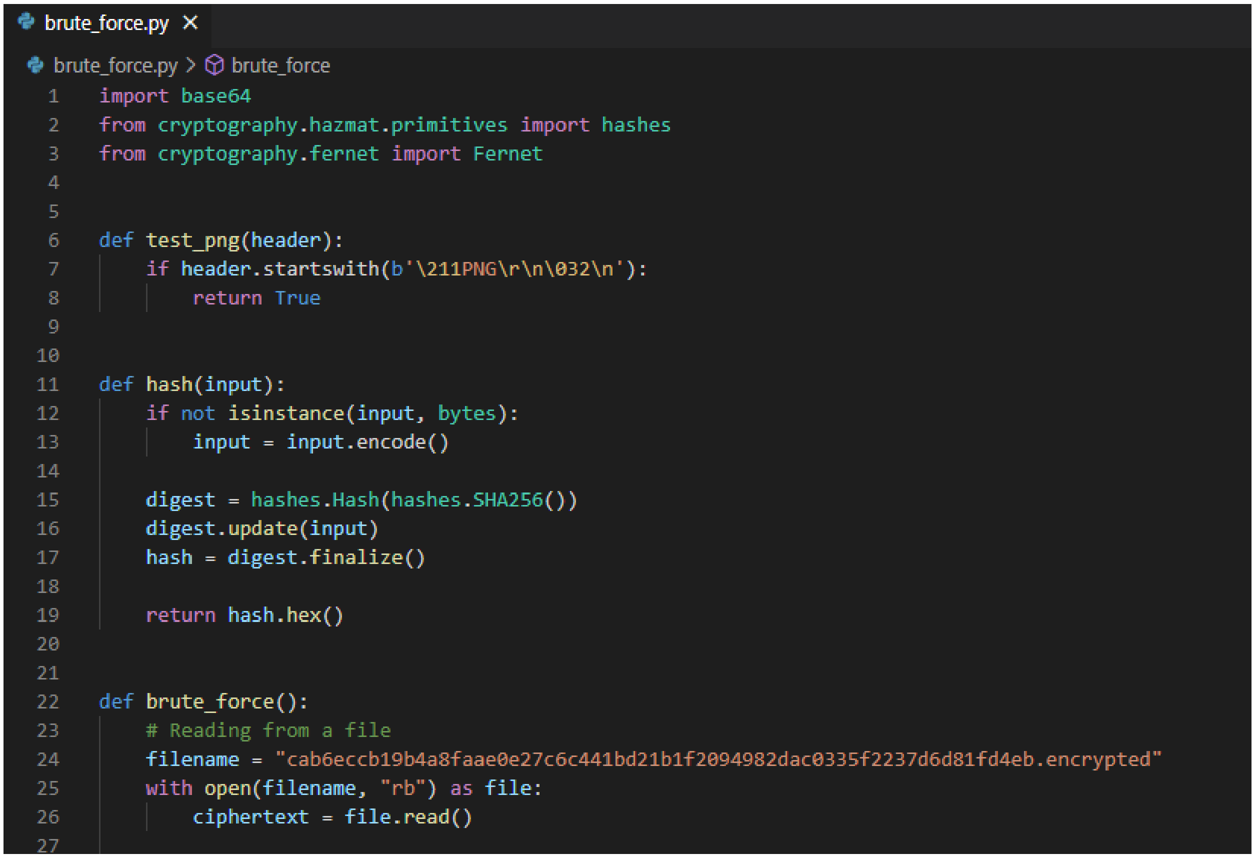
Svaki file je pripadao jednom studentu, prvo je trebalo otkriti koji je vaš file.



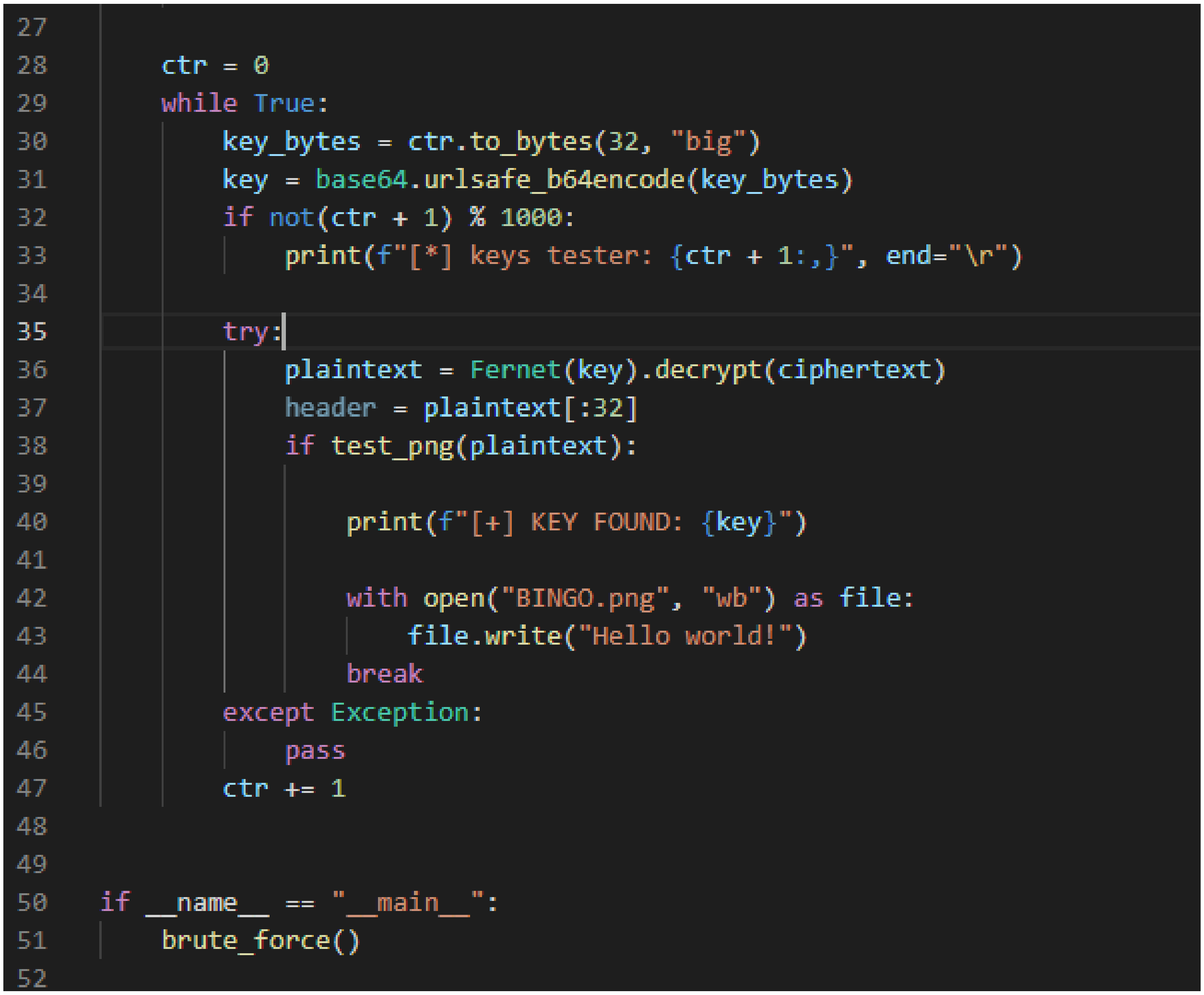
```python
from cryptography.hazmat.primitives import hashes


def hash(input):
    if not isinstance(input, bytes):
        input = input.encode()

    digest = hashes.Hash(hashes.SHA256())
    digest.update(input)
    hash = digest.finalize()

    return hash.hex()


if __name__ == "__main__":
    h = hash('curak_sara')
    print(h)

```

Moj file je bio:
cab6eccb19b4a8faae0e27c6c441bd21b1f2094982dac0335f2237d6d81fd4eb

U dokumentu se nalazio ciphertext kojeg je trebalo dešifrirati.



```python
import base64
from cryptography.hazmat.primitives import hashes
from cryptography.fernet import Fernet


def test_png(header):
    if header.startswith(b'\211PNG\r\n\032\n'):
        return True


def hash(input):
    if not isinstance(input, bytes):
        input = input.encode()

    digest = hashes.Hash(hashes.SHA256())
    digest.update(input)
    hash = digest.finalize()

    return hash.hex()


def brute_force():
    # Reading from a file
    filename = "cab6eccb19b4a8faae0e27c6c441bd21b1f2094982dac0335f2237d6d81fd4eb.encrypted"
    with open(filename, "rb") as file:
        ciphertext = file.read()

```



```
    ctr = 0
    while True:
        key_bytes = ctr.to_bytes(32, "big")
        key = base64.urlsafe_b64encode(key_bytes)
        if not(ctr + 1) % 1000:
            print(f"[*] keys tester: {ctr + 1:,}", end="\r")

        try:
            plaintext = Fernet(key).decrypt(ciphertext)
            header = plaintext[:32]
            if test_png(plaintext):

                print(f"[+] KEY FOUND: {key}")

                with open("BINGO.png", "wb") as file:
                    file.write("Hello world!")
                break
        except Exception:
            pass
        ctr += 1


if __name__ == "__main__":
    brute_force()

```

Nakon pokretanja programa, krenulo je pretraživanje ključeva.

Kjuč je pronađen.

Saznali smo ga je naš plaintekst, zapravo slika.

Zatim smo trebali pronaći gdje se nalazi BINGO.png, gdje se nalazila poruka za svakog studenta.

Sara Ćurak

Računarstvo 120