

Srp

2.lab vjezba

Za vjezbu smo trebali desifrirati enkriptirani plaintext.

Enkriptiran je korištenjem high level sustava za simetričnu enkripciju iz biblioteke Fernet:

Otkrili smo osobni izazov koji je namijenjen nama pomocu

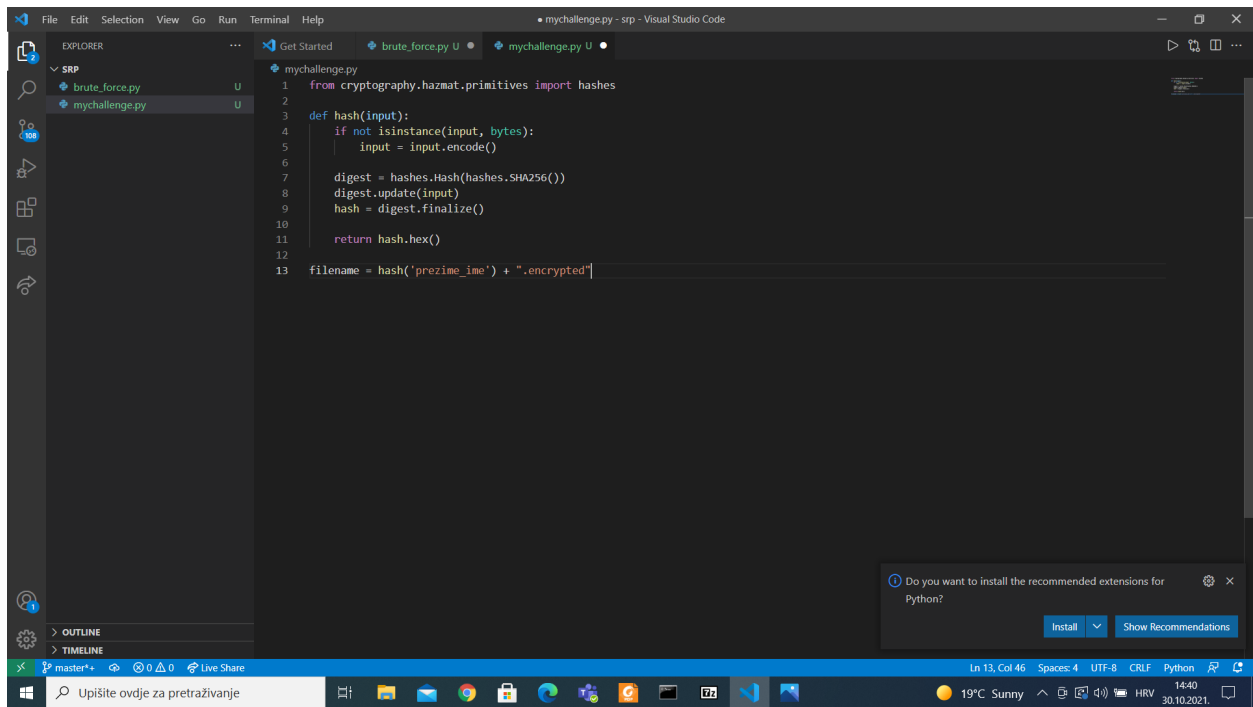
```
from cryptography.hazmat.primitives import hashes

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

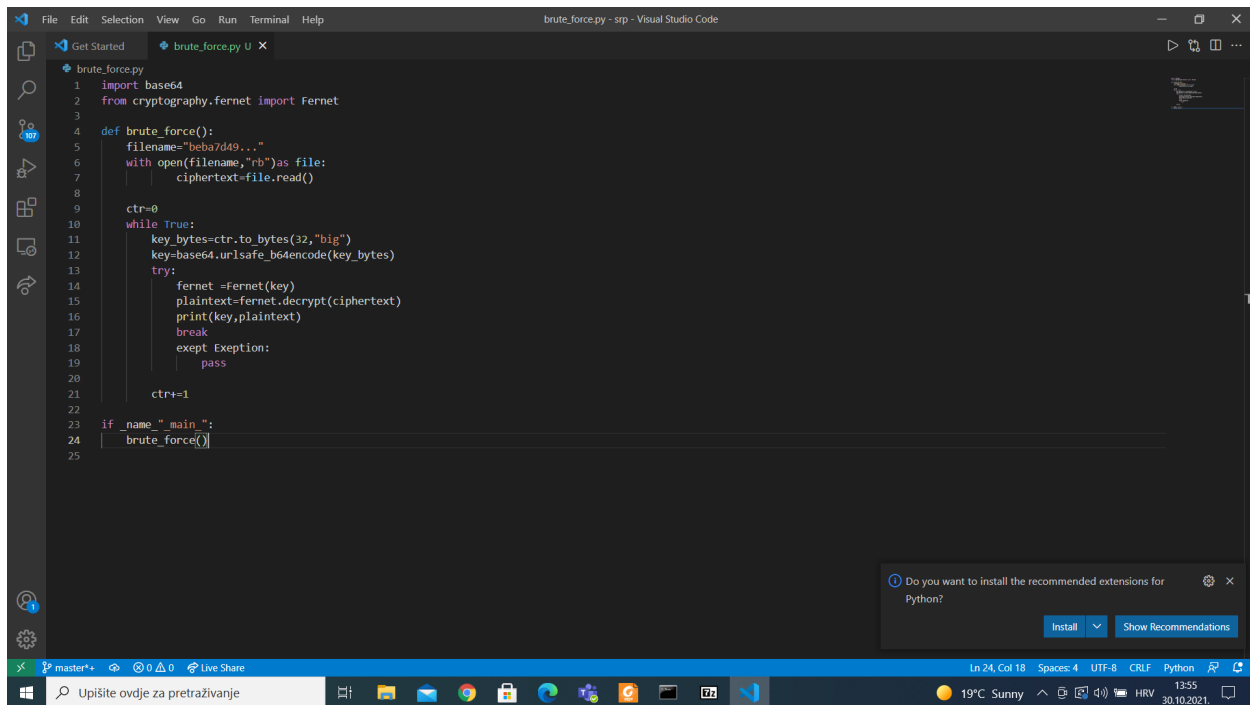
    digest = hashes.Hash(hashes.SHA256())
    digest.update(input)
    hash = digest.finalize()

    return hash.hex()

filename = hash('prezime_ime') + ".encrypted"
```



Nakon toga trebamo brute force algoritmom otkriti ključ za dešifriranje ciphertexta



Problem nam stvara beskonacna petlja i kako izaci iz nje.

Saznali smo da je nas plaintext slika png formata sa određenim headerom te smo stvorili koja testira je li prvi dio plaintexta trazeni format:

```

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

```

Spremimo nas plaintext u file:

```

if test_png(header):
print(f"[+] KEY FOUND: {key}")
# Writing to a file
with open("BINGO.png", "wb") as file:
file.write(plaintext)
break

```

```
1 import base64
2 from cryptography.fernet import Fernet
3
4
5 def test_png(header):
6     if header.startswith(b"\211PNG\r\n\032\n"):
7         return True
8
9 def brute_force():
10     filename="beba7d49..."
11     with open(filename,"rb") as file:
12         ciphertext=file.read()
13
14     ctr=0
15     while True:
16         key_bytes=ctr.to_bytes(32,"big")
17         key=base64.urlsafe_b64encode(key_bytes)
18         if not (ctr+1) % 1000:
19             print(f"[+] Keys tested: {ctr+1:,}", end="\n")
20
21         try:
22             fernet =Fernet(key)
23             plaintext=fernet.decrypt(ciphertext)
24             if test_png(header):
25                 print(f"[+] KEY FOUND: {key}")
26                 # writing to a file
27                 with open("BINGO.png", "wb") as file:
28                     file.write(plaintext)
29                 break
30
31         except Exeption:
32             pass
33
34     ctr+=1
35
36 if __name__ == "__main__":
37     brute_force()
38
```

Program generira ključ te otvorimo BINGO.png u našem direktoriju

Untitled