LAB 2

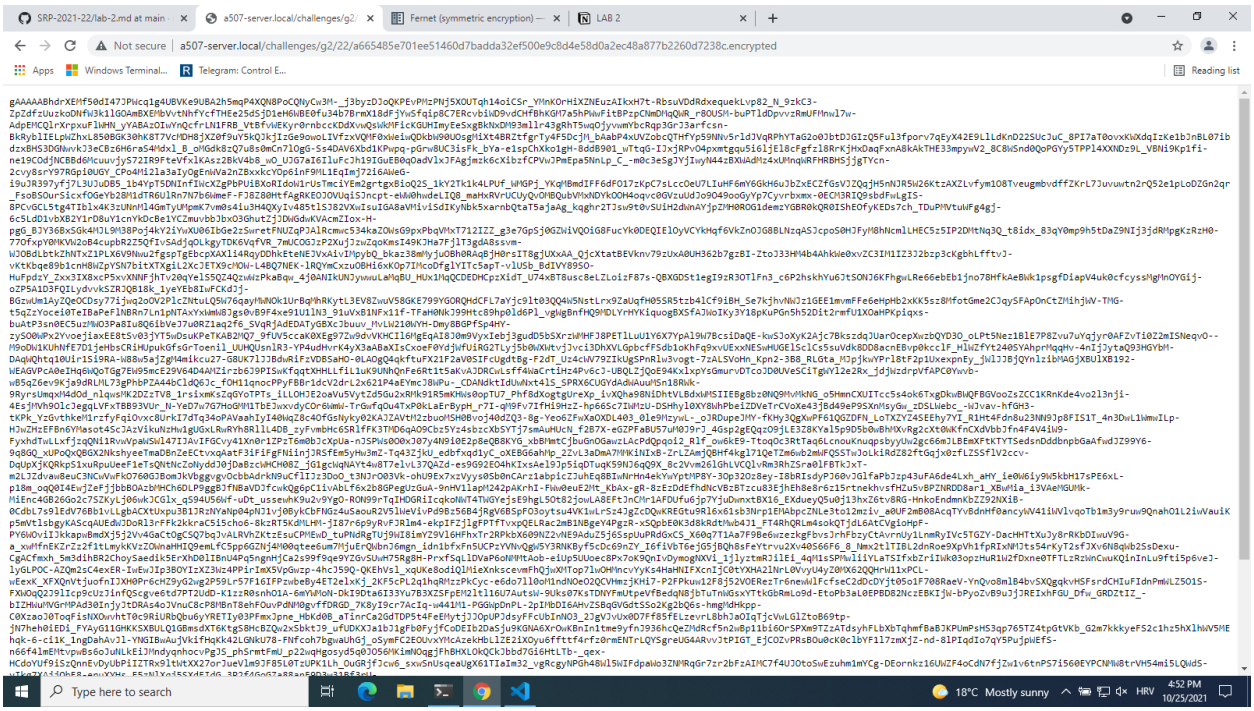
- uz upute profesora smo stvorili virtualno okruženje u Pythonu te instalirali biblioteku potrebnu za realizaciju crypto challenge-a

  ```
  python -m venv name
  pip install cryptography
  ```

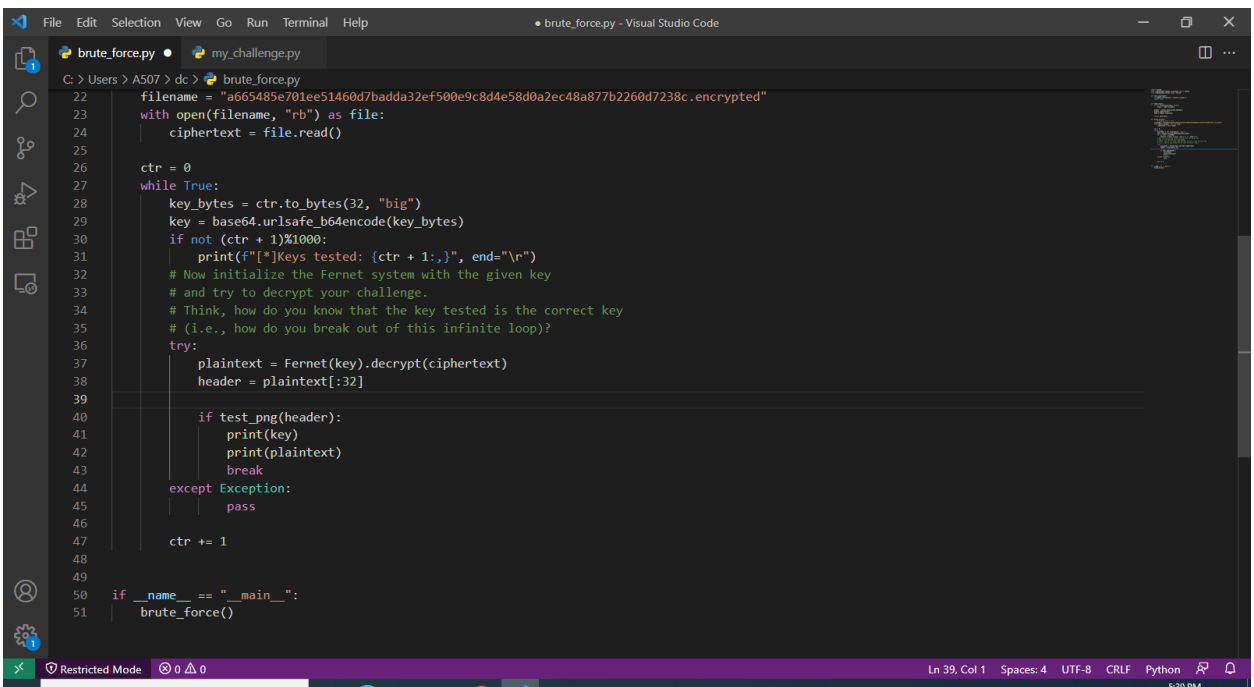
- Plaintext koji smo trebali otkriti enkriptiran je korištenjem high-level sustava za simetričnu enkripciju - Fernet
- Na lokalnom serveru postavljeni su različiti file-ovi i trebali smo dekripcijom otkriti koji je namijenjen nama

```
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('celan_dea')
    print(h)
```

- dekripcijom nam se otkrije ime file-a koji izgleda ovako:



- sada trebamo brute force algoritmom otkriti ključ kojim ćemo od ciphertexta doći do plaintexta te tako riješiti crypto izazov



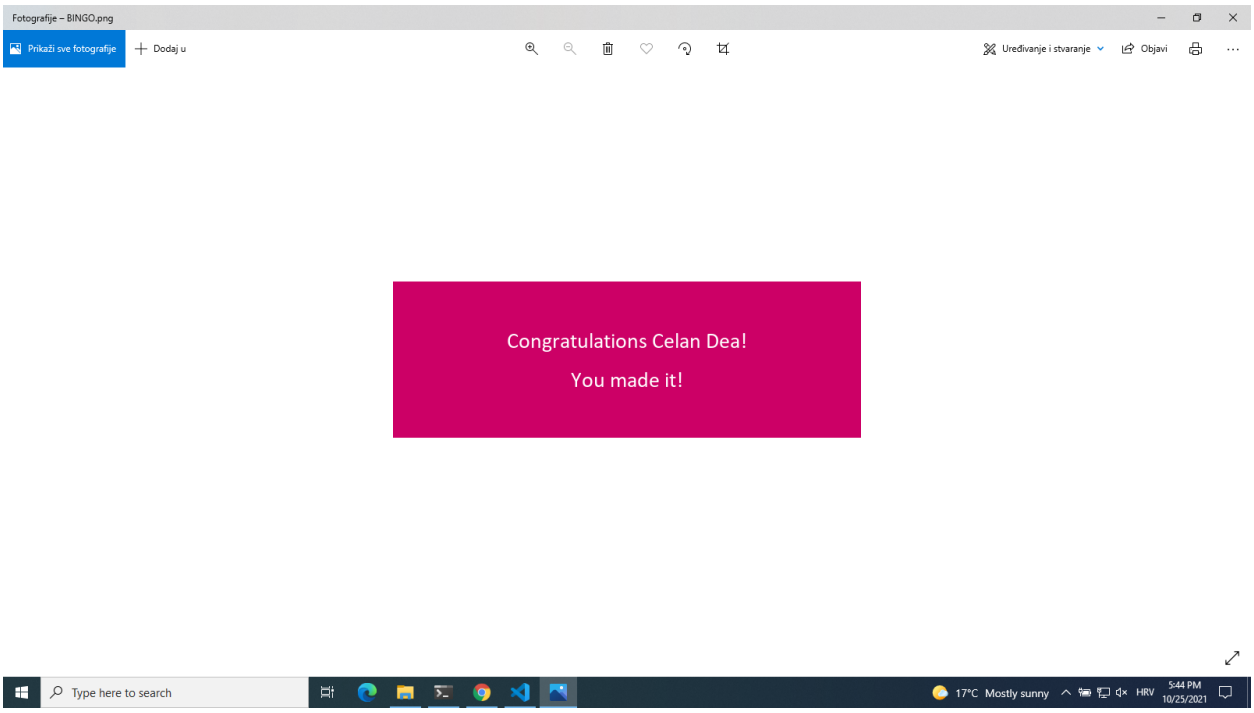
- najveći problem nam je stvorila if petlja i problem kada izaći iz loop-a. To smo riješili saznanjem da je naš plaintext slika .png formata koji ima određeni header te smo stvorili funkciju koja testira je li prvi dio(32b) plaintexta zapravo traženi format:

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

- nadalje, spremimo traženi plaintext u file

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

- program generira ključ te otvorimo BINGO.png u našem direktoriju


Fotografije – BINGO.png
Prikaži sve fotografije
Dodaj u
Uređivanje i stvaranje
Objavi
Congratulations Celan Dea!
You made it!
Type here to search
17°C Mostly sunny
HRV
5:44 PM
10/25/2021