Izvještaj druge laboratorijske vježbe

Symmetric key cryptography - a crypto challenge

> U sklopu vježbe student će riješiti odgovarajući *crypto* izazov, odnosno dešifrirati odgovarajući *ciphertext* u kontekstu simetrične kriptografije. Izazov počiva na činjenici da student nema pristup enkripcijskom ključu.

▼ Za pripremu *crypto* izazova, odnosno enkripciju korištena je Python biblioteka `cryptography`. *Plaintext* koji student treba otkriti enkriptiran je korištenjem *high-level* sustava za simetričnu enkripciju iz navedene biblioteke - Fernet.

▼ Fernet koristi sljedeće *low-level* kriptografske mehanizm

- AES šifru sa 128 bitnim ključem
- CBC enkripcijski način rada
- HMAC sa 256 bitnim ključem za zaštitu integriteta poruka

- Timestamp za osiguravanje svježine (*freshness*) poruka

1. **Instaliranje kriptografskog modula i pokretanje Pythona**

```
$ pip install cryptography python
```

2. **Preuzimanje izazova sa servera na osobno računalo**

```
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('barbara_bilic') + ".encrypted"
```

3. **Kod**

```
import base64
from cryptography.fernet import Fernet

def brute_force():



filename="f841381b7bbfb25b32902ab17dec3b1fa616559a7c49b18815e11b25eb83c9.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)

        try:
            fernet = Fernet(key)
```

```
            plaintext=fernet.decrypt(ciphertext)
            print(key, plaintext)
            break

        except Exception:
            pass

        ctr += 1


if __name__ == "__main__":
    brute_force()
```

- za dekriptiranje enkriptirane poruke koristili smo brute force napad
- za enkripciju poruke koristili smo ključeve ograničene entroprije - 22 bita
- u terminalu pokrenemo brute_force() napad i čekamo dok se petlja ne izvrši
- kada se petlja zaustavi to znači da smo uspiješno dekriptirali naš izazov ,a to možemo i provjeriti tako da pronađemo datoteku, u ovom slučaju sliku, na lokalnom računalu