Lab 5: Notes

1. zadatak:

- unutar mape koju smo stvorili za 5. labove stvaramo txt datoteku s podacima koji nam trebaju (copy pasteamo s https://github.com/mcagalj/SRP-2022-23/blob/main/password-hashing/requirements.txt)
- u terminal upisujemo naredbu `pip install -r requirements.txt`
- provjeravamo vremena izvršavanja različitih algoritama za hashiranje
  - nije pravilo, ali SHA512 uglavnom bude brži od SHA256 (neočkivano)
- ako napadaču treba 1 dan da prođe cijeli dictionary sa SHA256, za Linux_CRYPT_6 bi mu trebalo otprl. 100 dana

2. zadatak:

- registracija korisnika - uvjet je da već ne postoji korisnik s istim korisničkim imenom
- mogu postojati iste lozinke zbog password saltinga —> dva korisnika s dvije iste lozinke imaju različite hash vrijednosti (Hash(password, salt))
- mala dodatna sigurnost je otkrivanje što manje informacija (u ovom slučaju, ako korisničko ime ne postoji pri pokušaju logiranja, sustav javlja da je krivo korisničko ime **ili** lozinka, iako zna da korisnik ne postoji)

```
if user is None:
       print("Invalid username or password.")
       return
```