Sigurnost računala i podataka (Lab 2)

Symmetric key cryptography - a crypto challenge

U ovoj vježbi smo trebali riješiti odgovarajući *crypto izazov* tj. dešifrirati odgovarajući *ciphertext* u kontekstu simetrične kriptografije.

Kratko smo se upoznali s Pythonom i načinom na koji funkcjonira preko virtualnog okruženja jer smo za enkripciju koristili Python biblioteku *cryptography* i s Fernet sustavom kojim je enkriptiran *plaintext.*

Nakon toga dobili smo zadatak riješiti izazov tako da smo prvo otisli na jedan server gdje su se nalazili file-ovi i trebali smo pronaći svoj u kojem se nalazio *ciphertext* kojeg smo trebali dešifrirati i pohraniti u datoteku. Kod smo pisali u VS pokretanjem preko virtualnog okruženja.

Pokrenuli smo program koji je pretraživao ključeve sve dok nije našao odgovarajući i tako smo saznali svoj *plaintext*.