Ivan Legac Rudan

Izvještaj s trećih laboratorijskih vježbi

Na trećim laboratorijskim vježbama smo uz pomoć pythona i biblioteke crypthography za Izazov 1 računali mac vrijednost za dani text file i provjeravali integritet tog filea ukoliko je integritet netaknut funkcija bi vraćala vrijednost true u suprotnome false. Naknadnom izmjenom filea smo se uvjerili da je narušen inegritet kada bi funkcija ispisala false.

U drugom izazovu smo uz pomoć funkcije za određivanje integriteta trebali iz deset zadanih poruka i njihovih sig fileova odrediti kojim porukama je narušen integritet a kojima nije. Za to smo morali modificirati prethodno napisan kod za izazov 1.