U vježbi 4 bavili smo se autentikacijom i integritetom poruka (**Message Authentication and Integrity**).
Cilj vježbe bio je primijeniti autentikaciju i zaštitu integriteta poruka. Koristili smo simetrični kriptografski mehanizam: message authentication code (MAC) zasnovan na simetričnim ključevima.
Zadatak 1:
Cilj prvog zadatka je zaštita integriteta sadržaja poruke primjenom MAC algoritma. Koristili smo HMAC mehanizam iz **Python** biblioteke cryptography . Učitali smo poruku čiji integritet želimo zaštiti. Izračunali smo MAC vrijednost za zadani file koristeći funkciju generate_MAC. Onda smo učitali poruku i potpis . Za učitanu poruku smo izračunali MAC vrijednost. Izračunati MAC smo usporedili s učitanim potpisom pomoću verify_MAC funkcije. Ako su MAC-ovi jednaki integritet je očuvan.
Zadatak 2:
Cilj drugog zadatka bio je utvrditi vremenski autentičnu skevencu transakcija dionica. Preuzeli smo niz transakcija i njihovih autentikacijskih kodova. Znali smo da je tajna korištena kao ključ u MAC algoritmu bila u obliku *"<prezime_ime>".*encode(). Učitavali smo svaku transakciju i njen MAC tag i uspoređivali ih koristeći funkcije generate_MAC i verify_MAC. Na kraju smo pohranili sve autentične poruke u niz messages koji smo onda sortirali po timestampu.