SRP lab 4

U četvrtoj laboratorijskoj vježbi smo koristili osnovne kriptografske mehanizme da bi zaštitili integritet tekstualne poruke i verificirali njenu autentičnost.

U prvom zadatku smo zaštitili integritet poruke primjenom odgovarajućeg MAC algoritma koristeći HMAC mehanizam. Prvo smo učitali file i zatim generirali tajnu/ključ za potpis i potom zapravo “potpisali” poruku. Nakon provjere validnosti MAC-a spremili smo potpis tj. MAC u odvojeni file i potom smo mogli vidjeti da izmjenu originalne poruke MAC algoritam uistinu uspješno detektira kao i bilo kakvu promjenu potpisa.

U drugom zadatku smo preuzeli autenticirane naloge transkacija te smo trebali provjeriti imamo li vremenski ispravan redoslijed transakcija. Za tajnu vrijednost koju smo koristili kao ključ u MAC algoritmu koristili smo naše ime i prezime što nije pretjerano sigurno. Tajna vrijednost odnosno ključ nam je bio potreban da bi provjerili MAC. Da ne radimo manualnu provjeru svih transakcija koristili smo petlju te automatski izvlačili time-stamp i sortirali po vremenu. Iz dobivenih rezultata možemo zaključiti da je prema vremenskoj razlici između primljenih poruka vrlo vjerojatno da nismo primili sve poruke, odnosno da je netko izvršio napad te sam pregledao poruke i koristio informacije iz njih.