Laboratorijske vježbe 4

Cilj vježbe je bio primjeniti osnovne kritografske mehanizme za autentikaciju i zaštitu integriteta poruka. Pri tome smo koristili simetrične i asimetrične kriptografske mehanizme:

- ***message authentication code** (**MAC**)* zasnovane na simetričnim ključevima
- ***digitalne potpise*** zasnovane na javnim ključevima.

Na vježbi smo prošli dva zadatka.

Cilj prvog zadatka bila je zaštita integriteta poruka koristeći *HMAC* mehanizam iz Pyhton biblioteka.

Sami smo kreirali neke poruke unutar tekstualne datoteke u lokalnom direktoriju, koje smo zatim učitali u memoriju te generirali MAC vrijednost za danu poruku (funkcija *generate_MAC*). Napravili smo i funkciju za provjeru validnosti MAC-a za poruku (funkcija *verify_MAC*). U slučaju promjene izvorne poruke MAC algoritam uspješno detektira takve promjene.

Cilj drugog zadatka bio je provjeriti autentičnost transakcija dionica i autentične vremenski sortirati.

Sa servera http://challenges.local smo preuzeli personalizirane izazove. Tu su se nalazili nalozi za transakcije i odgovarajući *MAC tagovi.* Za provjeru MAC-a korišten je ključ koji je dobiven od imena studenta. Kroz petlju je izvršena provjera svih transakcija i ako su one autentične dobivena je poruka OK, a ako nije autentična NOK. Na kraju su autentične transakcije vremenski sortirane.