**Izvještaj – laboratorijske vježbe 4**

Na ovim vježbama upoznali smo se sa autentifikacijom i integritetom poruke te kako ih zaštititi koristeći *Message Authentication Code*(MAC). U ovoj vježbi naučiti ćemo kako funkcionira MAC, kako se generira ključ, generirati potpis, timestamp i sl.

1. **Zadatak**

* primjenom MAC algoritma zaštitili smo integritet poruke
* pomoću MAC algoritma generirali smo digitalni potpis kao potvrdu da je poruka poslana od pravog korisnika, da poruka nije mijenjana te da je kašnjenje minimalno
* MAC algoritam pomoću odabranog ključa i poruke generira digitalni potpis
* potpis pošaljemo zajedno sa porukom na javni kanal
* na odredištu primatelj također primjenjuje MAC algoritam sa odgovarajućim ključem da bi usporedio potpis koji je primio sa onim kojeg je generirao
* potpisi se poklapaju – zaštićen integritet poruke
* potpisis se razlikuju – nešto je mijenjano

1. **Zadatak**

* Bavimo se autentičnim vremenskim sekvencama transakcija dionica
* Svak je dobio vlastitu sekvencu za koje smo provjeravali autentičnost transakcije
* Na nesiguran način generirali smo ključ kojim generiramo MAC vrijednost
* Vršili smo usporedbu MAC vrijednosti preuzetih sa lokalnig poslužitelja sa MAC vrijednostima generiranim kroz petlju
* Kod pojave nepravilnosti dolazi do nepravilne MAC vrijednosti – poruka nije autentična
* Sve potuke smo sortirali prema timestamp-u te smo ih pohranili