Izvještaj iz 4. laboratorijskih vježbi / SRP /

U 4. laboratorijskim vježbama, demonstrirali smo upotrebu MAC funkcija kojom osiguravamo integritet poruke i autentikaciju korisnika.

U prvom zadatku smo dizajnirali funkciju koja za argumente uzima ključ, koji je zapravo dijeljena tajna između pošiljatelja i primatelja, i poruku kojoj želimo zaštiti integritet.

Način na koji se osigurava integritet i povjerljivost poruke je sljedeći:

- generira se hash vrijednost poruke koja se želi poslati
- ta hash vrijednost (signature/potpis) se konkatanira na poruku
- cijela poruka se enkriptira koristeći ključ (zajedničku tajnu) i šalje na kanal

Verifikacija integriteta poruke se povjerava na način:

- Dekriptira se pristigla poruka koristeći ključ (zajedničku tajnu)
- Hashira se poruka i usporedi sa potpisom
- Ako je sve u redu, poruka je autentična, ako ne, poruka se odbacuje

U drugom zadatku smo trebali provjeriti autentičnost zahtjeva za kupovinu/prodaju dionica. Koristeći for-petlju učitali bi sve datoteke, provjerili autentičnost i odbacili one koje nisu ispravne.