Lab 4: Message authentication and integrity

1. zadatak

U prvom zadatku smo napisali poruku kojoj želimo osigurati autentičnost.

Problem se sastoji od dva dijela:

1. Kreiranje ili osiguranje poruke
2. Osiguravanje autentičnosti poruke

Prvo treba otvoriti file i pročitati skrivenu poruku.Zatim smo hashirali tu poruku MAC funkcijom i povezali potpis s porukom. Za verifikaciju integriteta poruke smo ponovno pročitali sadržaj skrivene poruke i sadržaj datoteke koja sadrži potpis. Zatim smo potpisali sadržaj i uspoređivali novi potips s originalnim.

2. zadatak

Potrebno je odrediti koje su transakcije dionica autenticne i nakon toga ih posložiti po vremenu.