Vjezbe 4

Na ovim vjezbama smo radili kako funkcionira MAC algoritam za sto smo iz cryptography library-a importali funkciju za generate-anje MAC signature-a, funkciju za provjeru istoga i exception InvalidSignature.

Prvo smo kreirali .txt file u koji smo upisali text po svojoj volji i zatim generirali signature za taj file i spremili ga u obliku istoimenog file-a sa nastavkom .sig. Zatim (toboze nakon slanja poruke) smo procitali sadrzaj oba file-a, generirali novi signature iz istog .txt file-a te ga usporedili sa vec postojecim signature-om koji smo (toboze) primili od sender-a kako bi provjerili autenticnost poruke.

Sada smo skinili sa servera svatko svoj challenge (.txt i pripadajuci .sig file-ovi) za koje smo trebali provjeriti autenticnost. U svakom .txt file-u se nalazi niz order-a koji smo citajuci jedan po jedan red spremili u matricu te isto napravili za odgovarajuce .sig file-ove. I zadnje, KEY za MAC algoritam smo dobili primjenom funkcije encode na string-u oblika “ime_prezime”.

Istim postupkom provjere kao i u prvom dijelu vjezbi smo u for petlji provjerili autenticnost svakke poruke te one autenticne spremili u novu matricu autenticnih poruka.

Na kraju smo jos import-ali datetime library uz pomoc kojeg smo mogli poredati poruke po datumu kada su poslane te ih tako i ispisati po redu po kojem su trebale i biti izvrsene.