Lab 4

U ovim vježbama smo radili s MAC algoritmom s kojim smo kreirali kreirali signature za prvo za proizvoljni .txt file. Na taj tekst u .txt filu smo dodali signature i spremili tu novu datoteku kao .sig file, potom smo generirali novi signature za isti .txt file i provjeravali autentičnost poruke.

Zatim smo preuzeli svoj challenge te smo morali provjeriti autentičnost poruka. Svaki .txt file je sadržavao niz oredera koje smo spremali u matricu čitajući jedan po jedan redak, te potom isto napravili s odgovarajućim .sig fileovima. Potom smo KEY za MAC algoritam dobili uz pomoć funkcije encode nad stringom oblika „ime_prezime“.

Istim postupkom kao i za proizvoljni .txt file provjeravamo autentičnost svake poruke, te one autentične izdvajamo u novu matricu.

Naposljetku smo uz pomoć biblioteke datetime mogli sve autentične poruke poredati po datumu i vremenu kada bi trebale biti izvršene.