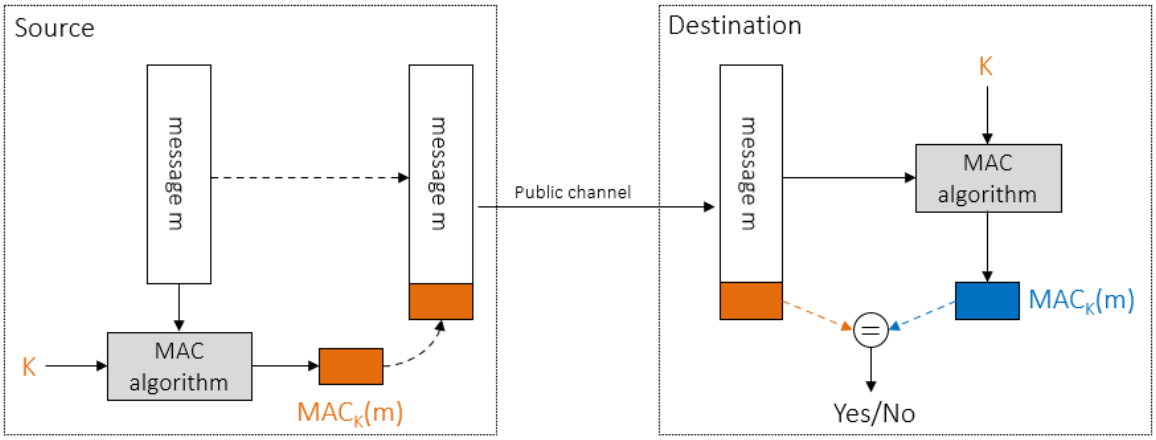
Vježba 4.

Class	SRP
Type	Lecture
Materials	https://github.com/mcagalj/SRP-2022-23

U ovoj vježbi smo pokazali kako se zaštita integriteta poruka i autentifikacija može primijeniti u stvarnom svijetu.

Prvi zadatak je bio zaštita integriteta pomoću *MAC* algoritma:

- otvaramo dokument koji trebamo potpisati
- stvaramo tag/potpis pomoću privatnog ključa
- potpis kao niz bitova ćemo spremiti u odvojeni dokument
- čitamo primljeni dokument i primljeni potpis
- generiramo novi potpis (pomoću privatnog ključa) iz dobivenog dokumenta
- usporedimo primljeni i generiran potpis



Drugi zadatak je bio odrediti ispravnu/autentičnu skevencu transakcija dionicama također pomoću *MAC* algoritma. Postupak je isti kao u prvom zadatku, provjerimo

autentičnost/integritet poruke te sortiramo poruke koje su autentične kako bi dobili sekvencu. Problem još može biti ako poruke ni ne dođu, to možemo riješiti dodavanjem rednih brojeva.