SRP - LAB 4

Message authentication and integrity

cilj vježbe: zaštita integriteta poruke korištenjem simetrične enkripcije (MAC algoritma) i provjera vremenske validnosti poruke

1. **Zaštita integriteta**

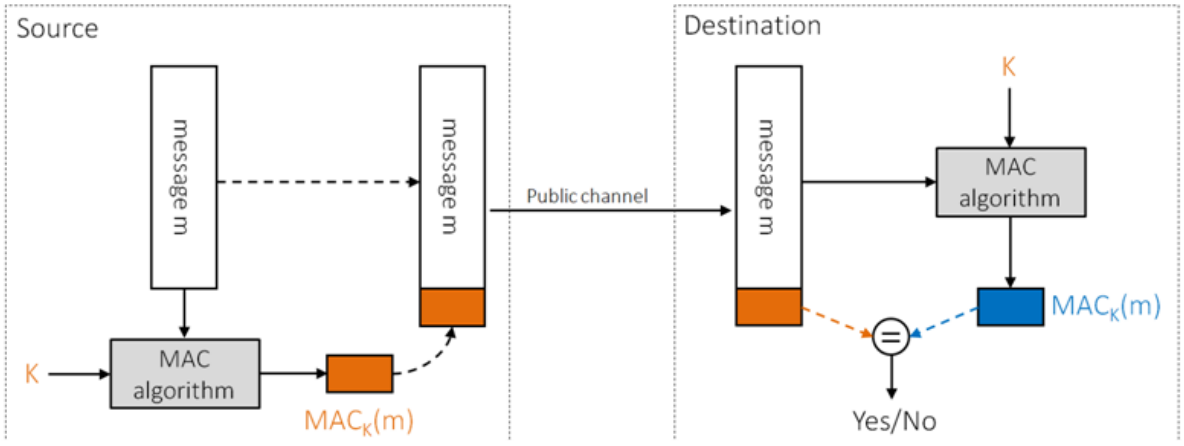
Kreiramo tekstualnu datoteku čiji sadržaj želimo zaštititi.

Korištenjem HMAC mehanizama iz pythonove biblioteke cryptography izračunavamo MAC vrijednost za poruku korištenjem simetričnog ključa. MAC vrijednost spremamo u odvojenu datoteku koju zajedno sa porukom šaljemo primatelju kako bi on mogao validirati integritet poruke.

Primatelj lokalno izračunava MAC vrijednost primljene poruke i uspoređuje s primljenom MAC vrijednosti.

U slučaju da su MAC vrijednosti iste, poruka je validna.

Ako nakon generiranja MAC vrijednosti promjenimo išta ili u poruci ili u samom MAC tagu, primateljeva lokalno generirana MAC vrijednost neće biti ista kao primljena MAC vrijednost i primatelj će znati da je integritet poruke bio narušen.



2. **Utvrđivanje vremenske ispravnu/autentičnosti skevence transakcija (ispravan redosljed transakcija) dionicama**

~ . ~

Provjera timestampa poruke omogućuje nam zaštitu od replay napada.

Ako imamo poruku koja je time sensitive, na primjer nalog za kupnju dionica, želimo se zaštititi od mogućnosti da napadač presretne poruku i primatelju je pošalje tek kasnije kad je cijena dionica porasla. Ako nemamo mehanizam za zaštitu od takve vrste napada, nalog za kupnju bi bio odobren i dionice bi bile kupljene po višoj cijeni.

~ . ~

U zadatku, preuzeli smo datoteku s nalozima za transakciju zajedno s njihovim MAC tagovima. Trebamo provjeriti je li integritet poruke narušen. To radimo izračunavanjem MAC taga svakog naloga i usporedbom s primljenim MAC tagom. Ispravne poruke zadržavamo, a neispravne odbacujemo.