3. laboratorijska vježba: Message authentication and integrity

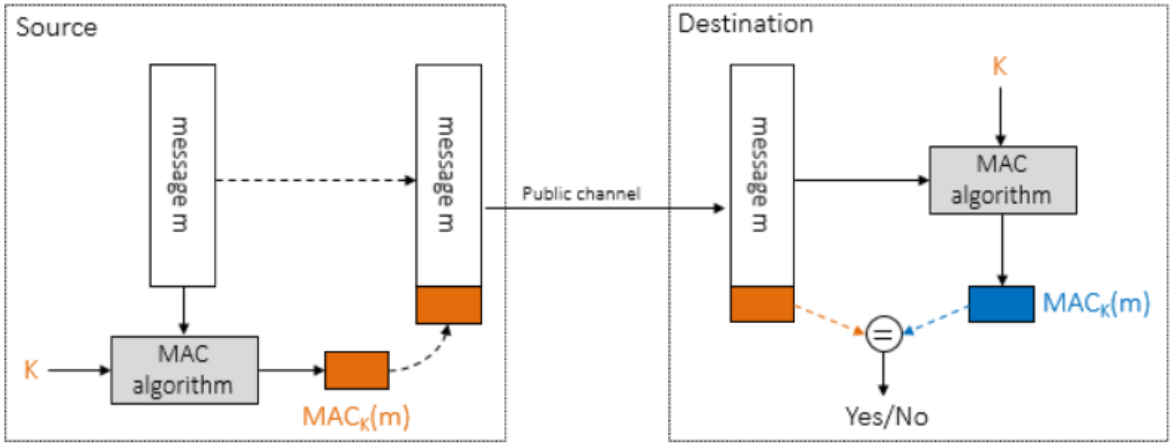
Studentica: Emilija Sarić

Smjer:112

Predmet: Sigurnost računala i podataka

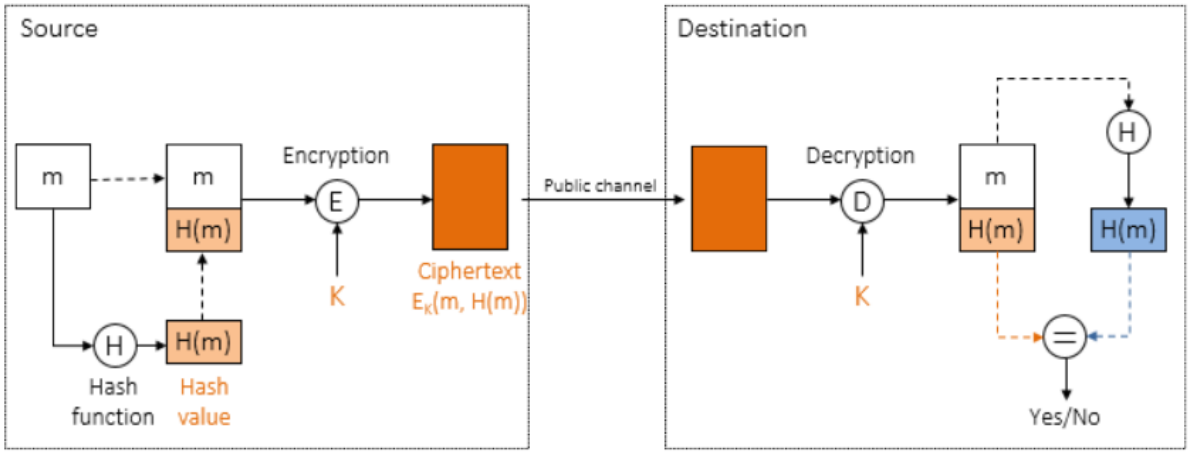
→ Autentikacija poruka (message authentication) štiti od aktivnih napada kao što su primjerice krivotvorenje podataka i transakcija te omogućava dostavu podataka po vremenu i sekvenci i "svježinu" poruke.

→ Kod autentikacije poruka generira se autentikacijska oznaka (authentication tag) i dodijeljuje svakoj poruci kako bi se zaštitila. Autentikacijska oznaka može se generirati na dva načina: message authentication (MAC) algoritmom i pomoću digitalnog potpisa.



Slika 1: Shema MAC algoritma u zaštiti integriteta poruke

→ Kod MAC algoritma možemo koristiti i kriptografsku hash funkciju koja prihvaća unos poruke m i kao izlaz daje "hash value" određene veličine.



Slika 2: Autentikacija poruka s hash funkcijom (osigurani integritet i povjerljivost)

→Za autentikaciju poruka možemo koristiti i public-key kriptografiju koja za enkripciju i dekripciju koristi različite ključeve pa tako imamo javni i privatni ključ.

U ovoj laboratorijskoj vježbi koristili su se simetrični i asimetrični kripto mehanizmi: message authentication code (MAC) i digitalni potpisi zasnovani na javnim ključevima.

IZAZOV 1

U ovom se izazovu provodi zaštita integriteta sadržaja dane poruke primjenom odgovarajućeg MAC algoritma.

IZVOĐENJE VJEŽBE:

1. Kreiranje tekstualne datoteke s odgovarajućim sadržajem čiji se integritet želi zaštiti.

2.Generiranje autentikacijske oznake za danu poruku pomoću odgovarajuće hash funkcije.

3."Potpisivanje" navedene datoteke.

4.Provjera ispravnosti MAC vrijednosti datoteke.

5.Modificiranje sadržaja datoteke ili potpisa.

IZAZOV 2

U ovom se izazovu ispituje ispravnost digitalnog potpisa pomoću public-key kriptografije.

IZVOĐENJE VJEŽBE:

1.Preuzimanje javnog ključa.

2.Preuzimanje slika i odgovarajućih potpisa.

3.Učitavanje javnog ključa iz datoteke (serijalizacija).

4.Provjera ispravnosti digitalnog potpisa (generiranje hash vrijednosti slike i uspoređivanje sa hash vrijednosti odgovarajućeg potpisa dekriptiranog odgovarajućim javnim ključem).

ZAKLJUČAK:

U prvom izazovu zaštićen je integritet datoteke pomoću MAC algoritma što se i potvrđuje modificiranjem sadržaja datoteke pri čemu MAC algoritam detektira navedene promjene.

U drugom je izazovu zaštićen ntegritet slika jer slike imaju odgovarajući digitalni potpis, bez obzira je li on odgovara ili ne. Povjerljivost nije zaštićena, zbog toga što bilo tko tko ima javni ključ može pristupiti tim datotekama.