TEHNIČKA ŠKOLA RUĐERA BOŠKOVIĆA

GETALDIĆEVA ULICA 4, ZAGREB

LEON ŽILIĆ 3.F

RAČUNALNE MREŽE

KRIPTOGRAFIJA U RAČUNALNOJ KOMUNIKACIJI

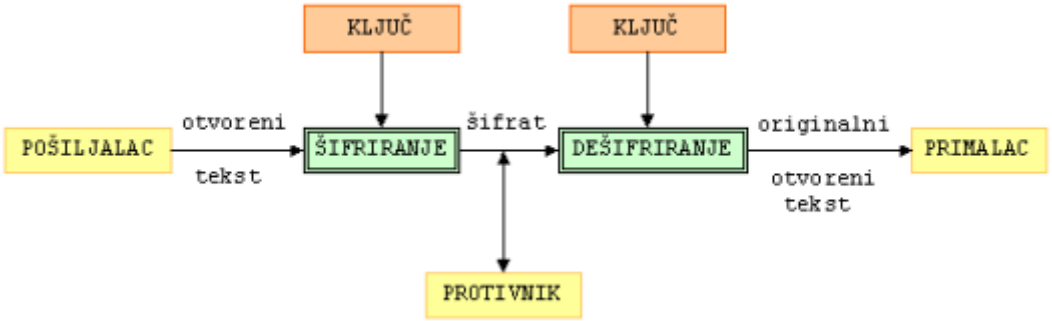
Zagreb, ožujak 2024.

Sadržaj

1. Uvod

Kriptografija je ključni element zaštite podataka u računalnoj komunikaciji. Ovaj seminarski rad istražuje osnove kriptografije i njezinu primjenu u osiguravanju sigurnosti podataka tijekom razmjene putem računalnih mreža.

2. Postupak šifriranja



Slika 1.

Poruka (otvoreni tekst) koju pošiljatelj pošalje primatelju se šifrira preko posebnog ključa koji je već definiran i posjeduju računalo pošiljatelja i primatelja, ali ne i računalo treće osobe(pritivnika). Nakon što se poruka pošalje prvo se šifrira(nastaje šifrat) te se takva šalje u komunikacijski kanal. Protivnik ne vidi originalnu poruku koju je napisao pošiljatelj već šifriranu, a pošto nema ključ ne može saznati što u njoj piše. Nakon što šifrat dođe do računala primatelja, ona se velikom brzinom prevodi nazad u originalnu poruku pomoću ključa. Kada mi otvorimo tu poruku vidjet ćemo je u onom obliku u kojem je poslana.

3. Osnove kriptografije

Kriptografija se temelji na korištenju različitih vrsta kriptografskih algoritama za zaštitu podataka. Postoje simetrični algoritmi koji koriste isti ključ za enkripciju i dekripciju te asimetrični algoritmi koji koriste par ključeva - javni i privatni. Enkripcija podataka uključuje pretvaranje čitljivih podataka u nečitljiv oblik, dok dekripcija podataka vraća podatke u njihov originalni format. Primjeri simetričnih algoritama uključuju AES (Advanced Encryption Standard), dok su RSA i ECC (Elliptic Curve Cryptography) primjeri asimetričnih algoritama.

4. Primjena kriptografije u različitim scenarijima

Kriptografija se ne koristi samo u računalnoj komunikaciji, već je ključna i u različitim područjima kao što su elektroničko bankarstvo, e-trgovina, zdravstvena zaštita i mnogi drugi. Primjerice, u elektroničkom bankarstvu, kriptografija se koristi za osiguravanje sigurnosti financijskih transakcija putem interneta.

5. Analiza prednosti i nedostataka različitih kriptografskih algoritama

Različiti kriptografski algoritmi imaju svoje prednosti i nedostatke. Na primjer, simetrični algoritmi poput AES-a brzi su i efikasni za enkripciju i dekripciju velikih količina podataka, dok asimetrični algoritmi poput RSA-a nude bolju sigurnost, ali su sporiji u obradi.

6. Studija slučaja

Jedan od primjera studije slučaja gdje je kriptografija odigrala ključnu ulogu je Napad na RSA. Ovaj napad je demonstrirao ranjivost RSA algoritma i potrebu za stalnim poboljšanjem kriptografskih tehnika radi očuvanja sigurnosti podataka.

7. Zaključak

Kriptografija je neophodna zaštita u računalnoj komunikaciji i šire. Implementacija odgovarajućih kriptografskih tehnika omogućava pouzdanu zaštitu podataka od neovlaštenog pristupa i manipulacije.

8. Izvori

https://en.wikipedia.org/wiki/History_of_cryptography

https://web.math.pmf.unizg.hr/~duje/kript/kriptografija.html (slika)

https://www.techtarget.com/searchsecurity/definition/cryptography

https://hr.wikipedia.org/wiki/Ra%C4%8Dunalna_sigurnost

https://www.enciklopedija.hr/clanak/kriptografija