

Univerzitet u Zenici

Politehnički fakultet

2022/23

*Računarske mreže*

Kriptografija

Student:

Omar Selimović

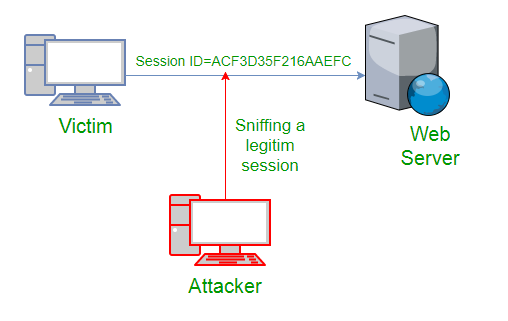
# Uvod

Računarske mreže predstavljaju ključni dio modernog svijeta, omogućavajući komunikaciju i razmjenu informacija na globalnoj razini. Međutim, ova povezanost također nosi rizike sigurnosti. Kriptografija, kao grana informatike koja se bavi zaštitom podataka, igra ključnu ulogu u osiguravanju povjerljivosti, integriteta i autentičnosti podataka u računarskim mrežama. U ovom radu, istražit ćemo osnovne pojmove kriptografije u kontekstu računarskih mreža, s fokusom na razmjenu ključeva, simetričnu i asimetričnu kriptografiju.

# Razmjena ključeva

-Problem razmjene ključeva  
Razmjena ključeva predstavlja ključni korak u sigurnoj komunikaciji u računarskim mrežama. Kada dvije strane žele uspostaviti sigurnu komunikaciju, potrebno je da svaka strana posjeduje zajednički tajni ključ koji se koristi za šifriranje i dešifriranje poruka. Međutim, glavni problem s kojim se susrećemo je kako sigurno razmijeniti ključeve između tih strana, posebno u situacijama kada prethodno nisu razmijenile nikakve informacije i nisu imale mogućnost dogovaranja o uspostavljanju nekog specifičnog ključa.

Glavna prijetnja u razmjeni ključeva je mogućnost prisluškivanja i manipulacije podacima koje je moguće ostvariti u računarskim mrežama. Ako se ključevi razmjenjuju na nezaštićen način, postoji rizik da zlonamjerni ljudi presretnu ključeve i koristi ih za dešifriranje ili čak lažiranje komunikacije.



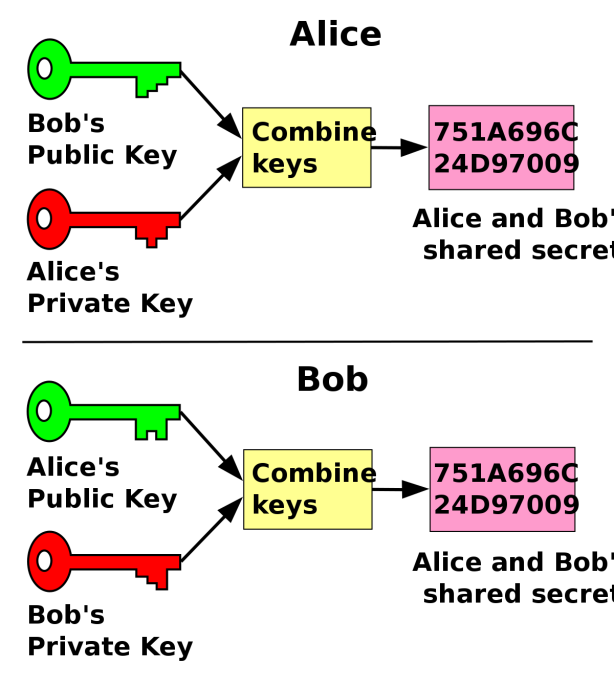
-Protokoli razmjene ključeva  
Kako bismo riješili problem razmjene ključeva na siguran način, razvijeni su razni protokoli koji osiguravaju sigurnu razmjenu ključeva između dvije strane. Ti protokoli obično koriste matematičke algoritme i tehnike kriptografije kako bi osigurali tajnost ključeva prilikom razmjene.

Jedan od najpoznatijih protokola razmjene ključeva je Diffie-Hellman protokol. Diffie-Hellman protokol je algoritam koji omogućuje dva korisnika da sigurno razmjene ključeve preko nesigurne komunikacijske mreže. Radi na osnovi matematičkog problema diskretnog logaritma.

Koraci Diffie-Hellman protokola su sljedeći:

-Odabir parametara: Sudionici dogovore zajednički prosti broj p i generator g. Oba parametra su javno poznata.  
-Generiranje privatnih ključeva: Svaki sudionik generira svoj slučajan privatni ključ. Privatni ključ je broj između 1 i (p-1).  
-Izračunavanje javnih ključeva: Koristeći privatne ključeve i parametre p i g, svaki sudionik izračunava svoj javni ključ. Javni ključ se dobiva kao g^(privatni ključ) mod p.  
-Razmjena javnih ključeva: Sudionici razmjenjuju svoje javne ključeve putem nesigurne komunikacije.  
-Izračunavanje zajedničkog tajnog ključa: Nakon što sudionici dobiju javne ključeve, koriste ih zajedno sa svojim privatnim ključevima kako bi izračunali zajednički tajni ključ. Taj ključ se računa kao (javni ključ suparnika)^(privatni ključ) mod p.  
-Korištenje zajedničkog ključa: Sudionici koriste zajednički tajni ključ za šifriranje i dešifriranje poruka koje razmjenjuju.

Diffie-Hellman protokol je siguran zbog računske složenosti problema diskretnog logaritma. Čak i ako napadač prisluškuje komunikaciju i zna javne ključeve, teško mu je izračunati privatne ključeve ili zajednički tajni ključ bez rješavanja tog problema. Protokol se koristi u raznim kriptografskim sustavima za sigurnu komunikaciju, ali se često kombinira s mehanizmima autentičnosti kako bi se spriječili napadi "man-in-the-middle".



Drugi popularan protokol razmjene ključeva je RSA protokol. RSA (Rivest-Shamir-Adleman) je kriptografski protokol koji se koristi za razmjenu ključeva, digitalno potpisivanje i šifriranje podataka. Temelji se na matematičkom problemu faktorizacije velikih brojeva.

Koraci RSA protokola su sljedeći:

-Generiranje ključeva: Prvo, sudionik generira par ključeva - javni ključ i privatni ključ. Javni ključ je dostupan svima i koristi se za šifriranje podataka, dok je privatni ključ poznat samo vlasniku i koristi se za dešifriranje podataka.  
Odabir prostih brojeva: drugi član bira dva velika različita prosta broja, obično označena kao p i q.  
-Izračunavanje modula: Izračunava se modul n kao proizvod p i q, tj. n = p \* q. Modul n je dio javnog ključa.  
-Izračunavanje Eulerove funkcije: Izračunava se Eulerova funkcija φ(n), koja predstavlja broj prirodnih brojeva manjih od n koji su relativno prosti s n. Za prost broj p, φ(p) = p - 1.  
-Odabir javnog ključa: drugi član bira broj e koji je relativno prost s φ(n) i manji od n. Broj e je dio javnog ključa.

-Izračunavanje privatnog ključa: Izračunava se broj d koji zadovoljava uvjet (e \* d) mod φ(n) = 1. Broj d je privatni ključ.  
-Razmjena javnih ključeva: Sudionici razmjenjuju svoje javne ključeve.

Nakon generiranja ključeva, RSA se može koristiti na sljedeći način:

Šifriranje: Osoba koja želi poslati šifriranu poruku koristi javni ključ primatelja kako bi šifrirala podatke.

Dešifriranje: Primatelj koristi svoj privatni ključ kako bi dešifrirao primljenu poruku.

RSA protokol je siguran jer faktorizacija velikih brojeva, koja je potrebna za otkrivanje privatnog ključa, trenutno nije izvediva u razumnom vremenu.

Internet Key Exchange (IKE) je protokol koji se koristi za uspostavljanje sigurne veze i razmjenu ključeva u IPsec (Internet Protocol Security) VPN (Virtual Private Network) komunikaciji. IKE se sastoji od dvije glavne faze: IKE faza 1 i IKE faza 2.

Koraci IKE protokola su sljedeći:

IKE faza 1 je odgovorna za sigurnu razmjenu ključeva za uspostavu sigurne veze. U ovoj fazi se događa sljedeće:  
-Dogovor o parametrima: Sudionici dogovaraju sigurnosne parametre, uključujući algoritme za šifriranje, autentifikaciju i razmjenu ključeva.  
-Razmjena identiteta: Sudionici razmjenjuju identitete, obično putem digitalnih certifikata ili predjeljivanjem pre-shared ključeva.  
-Izračunavanje zajedničkog tajnog ključa: Koristeći Diffie-Hellman protokol, sudionici izračunavaju zajednički tajni ključ koji će se koristiti za simetrično šifriranje podataka u fazi 2.

IKE faza 2 je odgovorna za sigurno razmjenjivanje podataka između dvije strane koje su uspostavile sigurnu vezu. U ovoj fazi se događa sljedeće:  
-Dogovor o sigurnosnom udruživanju: Sudionici dogovaraju sigurnosne parametre, uključujući algoritme za šifriranje i integritet podataka.  
-Razmjena ključeva za šifriranje: Koristeći prethodno uspostavljene ključeve iz faze 1, sudionici razmjenjuju ključeve koji će se koristiti za šifriranje podataka.  
-IKE se koristi za automatizaciju procesa uspostave sigurne komunikacije i razmjene ključeva između dvije strane u IPsec VPN-u. Ovaj protokol osigurava povjerljivost, integritet i autentičnost podataka koji se prenose preko javne mreže, pružajući sigurno okruženje za privatnu komunikaciju.

Primjeri primjene protokola razmjene ključeva

Postoji veliki broj primjena protokola za razmjenu ključeva i zavisno od nivoa potrebne sigurnosti, raspoloživih hardverskih resursa i samog tipa konekcije, biramo protokol koji će postići najbolji rezultat u datoj situaciji.

SSL i SLT

Secure Socket Layer (SSL) i njegova nasljednica Transport Layer Security (TLS) su kriptografski protokoli koji pružaju sigurnu komunikaciju preko nesigurne mreže, kao što je internet. Ovi protokoli osiguravaju šifriranje podataka, autentičnost sudionika i integritet podataka tijekom prijenosa.

SSL/TLS protokoli rade na osnovi asimetrične (javnog ključa) i simetrične kriptografije te digitalnih certifikata. Njihov glavni cilj je osigurati povjerljivost, integritet i autentičnost podataka koji se prenose između klijenta i poslužitelja.

Klučne faze SSL/TLS protokola su:

1.Handshake: Inicijalna faza u kojoj se uspostavlja veza između klijenta i poslužitelja. Uključuje sljedeće korake:

a. Dogovor o kriptografskim algoritmima: Klijent i poslužitelj biraju zajedničke algoritme za šifriranje, autentičnost i razmjenu ključeva.

b. Razmjena i provjera digitalnih certifikata: Poslužitelj pruža svoj digitalni certifikat koji sadrži javni ključ. Klijent provjerava vjerodostojnost certifikata.

c. Razmjena tajnih ključeva: Klijent i poslužitelj koriste javne i privatne ključeve za generiranje zajedničkog tajnog ključa koji će se koristiti za simetrično šifriranje podataka.

2.Šifriranje podataka: Nakon uspješnog završetka rukovanja, klijent i poslužitelj koriste zajednički tajni ključ za šifriranje i dešifriranje podataka koji se prenose. Simetrična kriptografija se obično koristi za brže šifriranje velike količine podataka.

3.Integritet podataka: SSL/TLS protokoli koriste hash funkcije i digitalne potpise kako bi osigurali da se podaci nisu mijenjali tijekom prijenosa. Prilikom dešifriranja, provjerava se integritet podataka kako bi se spriječile neovlaštene promjene.

4.Autentičnost: SSL/TLS protokoli osiguravaju autentičnost poslužitelja i, po potrebi, klijenta. Klijent može zahtjevati da poslužitelj pruži valjani digitalni certifikat kako bi se osigurala identifikacija poslužitelja.

SSL/TLS protokoli su široko korišteni za sigurnu komunikaciju na webu, kao što je HTTPS (HTTP Secure). Ovi protokoli pružaju zaštitu korisničkih podataka, poput lozinki, financijskih transakcija i povjerljivih informacija. Redovito se ažuriraju kako bi se riješile sigurnosne slabosti i podržali najnoviji kriptografski standardi.

Ukratko, SSL/TLS protokoli osiguravaju sigurnu komunikaciju šifriranjem podataka, provjerom autentičnosti sudionika i osiguravanjem integriteta podataka. Oni igraju ključnu ulogu u održavanju privatnosti i sigurnosti na internetu.

Virtual Private Network (VPN)

VPN koristi protokole razmjene ključeva kako bi uspostavio sigurnu vezu između korisnika i privatne mreže. Protokoli kao što su Internet Key Exchange (IKE) omogućuju sigurnu razmjenu ključeva za šifriranje podataka koji se prenose putem VPN-a. VPN se najčešće koristi kao dodatni sloj sigurnosti online te se s njim postiže virtuelna anonimnost online zbog implementiranih slojeva sigurnosti u VPN servisima.

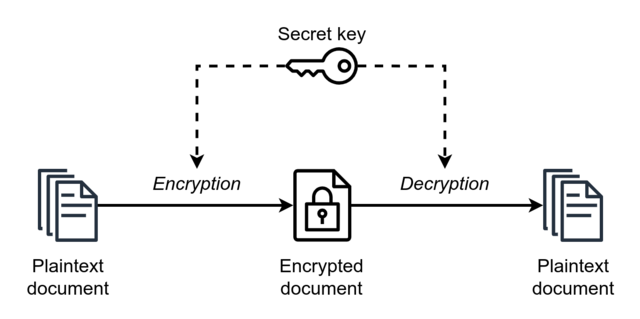
Bežične mreže

Wireless Networks: U bežičnim mrežama, protokoli razmjene ključeva koriste se za sigurnu autentifikaciju korisnika i osiguravanje povjerljivosti podataka. Na primjer, Wi-Fi Protected Access (WPA) protokol koristi razne protokole razmjene ključeva za sigurnu vezu između bežičnih uređaja i pristupne tačke.

Ovi primjeri ilustriraju važnost protokola razmjene ključeva u osiguravanju sigurnosti i povjerljivosti komunikacije u različitim kontekstima računarskih mreža. Korištenjem tih protokola, korisnici mogu sigurno razmijeniti ključeve i osigurati povjerljivost i integritet podataka koji se prenose u mreži.

# Simetrična kriptografija

Simetrična kriptografija je vrsta kriptografskog sustava u kojem se isti ključ koristi za šifriranje i dešifriranje podataka. Ovaj ključ se naziva tajni ključ ili simetrični ključ. Simetrična kriptografija je jednostavna i brza, ali postoji izazov kako sigurno razmijeniti tajni ključ između dvije komunikacijske strane.



Algoritmi simetrične kriptografije

Simetrični algoritmi su matematičke funkcije koje se koriste za šifriranje i dešifriranje poruka koristeći isti tajni ključ. Primjeri popularnih simetričnih algoritama su Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Standard (3DES) i Blowfish. Ovi algoritmi koriste različite tehnike, kao što su zamjena znakova, permutacija i XOR operacije, kako bi osigurali sigurnost podataka.

AES je najčešće korišteni simetrični kriptografski algoritam. Koristi ključeve dužine 128, 192 ili 256 bitova i koristi se za šifriranje i dešifriranje podataka. AES je brz, siguran i otporan na napade “Battery draining attack”.  
DES je stariji simetrični kriptografski algoritam koji koristi ključ dužine 56 bitova. Uprkos svojoj popularnosti u prošlosti, DES je sada manje siguran zbog ograničene dužine ključa i naprednih računarskih mogućnosti.  
3DES je poboljšanje DES-a koje koristi isti algoritam, ali primjenjuje ga tri puta s različitim ključevima. Kombinacija tri puta DES-a povećava sigurnost, ali naravno usporava performanse.

Prednosti i nedostaci simetrične kriptografije

Simetrična kriptografija ima nekoliko prednosti. Prvo, simetrični algoritmi su brzi i učinkoviti jer koriste isti ključ za šifriranje i dešifriranje, što čini proces enkripcije i dekripcije brzim. Također, simetrična kriptografija je jednostavna za implementaciju i zahtijeva manje kompjuterskih resursa.  
Međutim, glavni nedostatak simetrične kriptografije je izazov razmjene tajnog ključa između dvije komunikacijske strane. Tajni ključ mora biti sigurno razmijenjen kako bi se osigurala povjerljivost podataka. Ako se ključ ne razmijeni sigurno, postoji rizik od napada presretanjem ključa i kompromitiranja sigurnosti podataka.

Primjena simetriče kriptografije

Simetrična kriptografija ima široku primjenu u zaštiti podataka i sigurnoj komunikaciji. Primjeri primjene simetrične kriptografije uključuju:

-Zaštita podataka na mrežnom sloju: Simetrična kriptografija se često koristi za šifriranje podataka koji se prenose preko računarskih mreža, kao što su IP paketi. To osigurava da samo primatelj može dešifrirati i pristupiti tim podacima.  
-Disk enkripcija: Simetrična kriptografija se koristi za šifriranje podataka na hard diskovima kako bi se osigurala njihova povjerljivost u slučaju gubitka ili krađe uređaja.  
-Sigurna komunikacija: Simetrična kriptografija se koristi za sigurnu komunikaciju između korisnika putem različitih kanala, kao što su chat aplikacije, e-mailovi i VoIP usluge.

Simetrična kriptografija je ključna tehnologija u sigurnosti podataka i računarskih mreža. Uprkos izazovima vezanim za razmjenu ključeva, simetrična kriptografija pruža učinkovit način zaštite podataka i osiguravanje povjerljivosti u komunikaciji.

# Asimetrična kriptografija

Asimetrična kriptografija, također poznata kao javni ključ kriptografija, je vrsta kriptografskog sustava u kojem se koriste dva različita ključa - javni ključ i privatni ključ. Javni ključ se dijeli s drugima, dok privatni ključ ostaje tajna. Ovi ključevi su međusobno povezani matematičkim funkcijama, što omogućuje šifriranje podataka s jednim ključem i dešifriranje s drugim ključem.

Algoritmi asimetrične kriptografije

Asimetrični algoritmi koriste matematičke funkcije poput faktorizacije brojeva ili problematike diskretnog logaritma kako bi osigurali sigurnost podataka. Primjeri popularnih asimetričnih algoritama su RSA (Rivest-Shamir-Adleman), Diffie-Hellman, ElGamal i ECC (Elliptic Curve Cryptography).

Prednosti i nedostaci asimetrične kriptografije

Asimetrična kriptografija pruža nekoliko prednosti u odnosu na simetričnu kriptografiju. Prvo, nema potrebe za razmjenom tajnog ključa između dvije strane. Svaka strana generira svoj par ključeva - javni i privatni, čime se eliminira izazov razmjene tajnog ključa. Drugo, asimetrična kriptografija omogućuje digitalno potpisivanje, što omogućuje provjeru autentičnosti podataka.

Međutim, asimetrična kriptografija je složenija i sporija u odnosu na simetričnu kriptografiju. Matematički algoritmi koji se koriste u asimetričnoj kriptografiji zahtijevaju više računarske snage i resursa. Stoga se često koristi kombinacija simetrične i asimetrične kriptografije, gdje se asimetrična kriptografija koristi za razmjenu tajnih ključeva, a simetrična kriptografija za šifriranje podataka.

Primjena asimetrične kriptografije

Sigurna komunikacija: Asimetrična kriptografija se koristi za sigurnu komunikaciju između korisnika putem kanala kao što su e-mailovi, SSL/TLS za web komunikaciju i VPN veze. Javni ključ se koristi za šifriranje podataka koje samo primatelj može dešifrirati pomoću svog privatnog ključa.

Digitalni potpis: Asimetrična kriptografija omogućuje digitalno potpisivanje dokumenata i poruka kako bi se osigurala njihova autentičnost i integritet. Pošiljatelj koristi svoj privatni ključ za stvaranje digitalnog potpisa, a primatelj koristi javni ključ pošiljatelja za provjeru potpisa.  
Enkripcija podataka na mirovanju: Javni ključ kriptografija se koristi za šifriranje podataka koji su pohranjeni na medijima ili u bazi podataka, čime se osigurava njihova povjerljivost i sprječava neovlašteni pristup.

Asimetrična kriptografija igra ključnu ulogu u sigurnosti podataka i osigurava sigurnu komunikaciju i zaštitu podataka u računarskim mrežama.

# Zaključak

Simetrična kriptografija, koja koristi isti ključ za šifriranje i dešifriranje podataka, pruža brz i učinkovit način zaštite podataka. Međutim, izazov leži u sigurnoj razmjeni tajnog ključa između dvije komunikacijske strane. Protokoli razmjene ključeva pomažu u rješavanju tog problema, osiguravajući sigurnu razmjenu ključeva kako bi se osigurala povjerljivost podataka.

S druge strane, asimetrična kriptografija koristi dva različita ključa - javni ključ i privatni ključ. To omogućuje sigurnu komunikaciju bez potrebe za sigurnom razmjenom tajnog ključa. Asimetrična kriptografija također omogućuje digitalno potpisivanje i provjeru autentičnosti podataka.

U zaključku se može primijetiti da i simetrična i asimetrična kriptografija imaju svoje prednosti i nedostatke. Simetrična kriptografija je brza i učinkovita, ali zahtijeva sigurnu razmjenu tajnog ključa. Asimetrična kriptografija eliminira taj izazov, ali je složenija i sporija u usporedbi s simetričnom kriptografijom.

Kriptografija je neprestano evoluirajuće područije, a protokoli razmjene ključeva i kriptografski algoritmi se neprestano poboljšavaju kako bi se osigurala sigurnost i zaštita podataka. Razumijevanje osnova kriptografije ključno je za stručnjake za računarske mreže i sigurnost kako bi uspješno implementirali sigurnost podataka u mrežne sisteme.

U zaključku, kriptografija igra vitalnu ulogu u sigurnosti računarskih mreža. Kombinacija simetrične i asimetrične kriptografije, uz korištenje protokola razmjene ključeva, omogućuje sigurnu komunikaciju, zaštitu podataka i osigurava povjerljivost, autentičnost i integritet informacija koje se prenose putem mreže. Kriptografija je temeljni alat za održavanje sigurnosti u digitalnom dobu i nastavit će se razvijati kako bi se suočila s novim izazovima i prijetnjama.