KRIPTOGRAFIJA U RAČUNALNOJ KOMUNIKACIJI

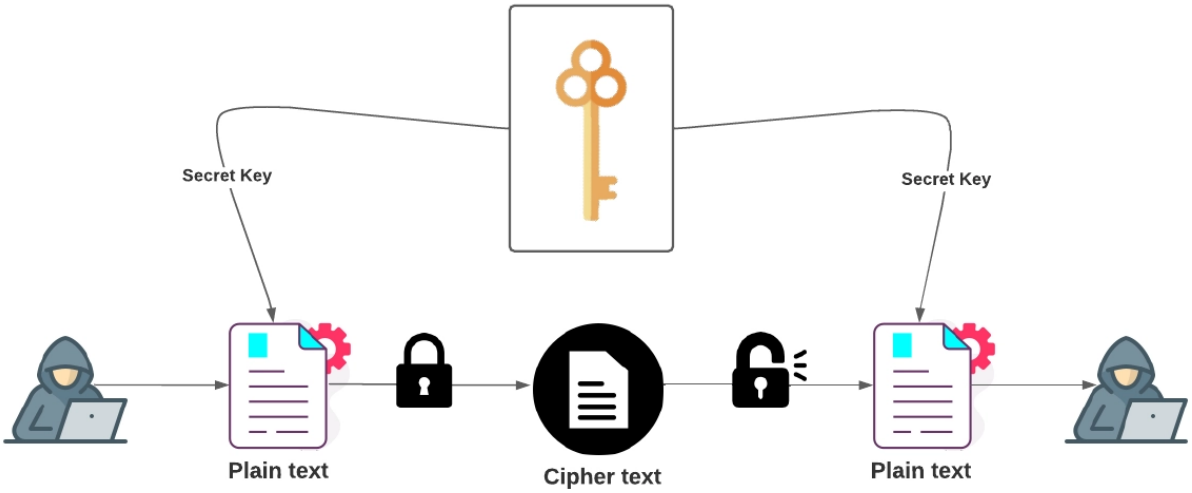
Barbara Kuharić, 3.G

6. SVIBNJA 2025.
TEHNIČKA ŠKOLA RUĐERA BOŠKOVIĆA

Uvod

U digitalnom dobu, sigurnost informacija postala je ključan aspekt svakodnevne komunikacije. Sve veća upotreba interneta i digitalnih tehnologija zahtijeva učinkovite metode zaštite podataka od neovlaštenog pristupa, krađe ili zloupotrebe. Kriptografija, kao znanost o šifriranju informacija, ima ključnu ulogu u zaštiti komunikacije između računala, uređaja i korisnika.

Kroz povijest, kriptografija se razvijala od jednostavnih šifri do složenih algoritama koji danas štite bankovne transakcije, elektroničku poštu, komunikaciju putem društvenih mreža i mnogo više. U ovom radu bit će prikazane osnovne vrste kriptografije, njena primjena u računalnoj komunikaciji, najvažniji alati te izazovi s kojima se suočava u suvremenom digitalnom okruženju.



Povijest kriptografije

Riječ "kriptografija" potječe od grčke riječi kriptos, što znači skriveno. Prefiks "crypt-" znači "skriven" , a sufiks "-graphy" znači "pisanje".

Podrijetlo kriptografije obično se datira oko 2000. godine prije Krista, s egipatskom praksom hijeroglifa. Oni su se sastojali od složenih piktograma, čije je puno značenje bilo poznato samo nekolicini elitnih ljudi.

Prva poznata uporaba moderne vrste šifre bila je Julije Cezar (100. pr. Kr. do 44. pr. Kr.), koji nije vjerovao svojim glasnicima kada je komunicirao sa svojim generalima. Iz tog je razloga stvorio sustav u kojemu je svaki znak u njegovim porukama zamijenjen znakom tri mjesta ispred njega u latinskom alfabetu.

Osnove kriptografije

Kriptografija je metoda za zaštitu komunikacije od neovlaštenih strana.

Osnovna ideja iza kriptografije je korištenje ključa za šifriranje informacija tako da ih mogu čitati samo oni koji im imaju pristup. Svi ostali ljudi vidjet će nasumična slova,brojeve,znakove umjesto izvorne poruke. Za dešifriranje poruke, sve što je potrebno je točan ključ.
Kriptografija omogućuje postizanje sljedeća 3 cilja:

1. Povjerljivost
   Kriptografija štiti tajnost informacija. Čak i ako je medij za prijenos ili pohranjivanje ugrožen, šifrirane informacije bit će beskorisne neovlaštenoj osobi.
2. Integritet
   Kriptografija osigurava da podaci nisu mijenjani metodom raspršivanja.
3. Autentičnost
   Kriptografija osigurava da su informacije poslane od namjeravanog, a ne lažnog pošiljatelja. To se postiže pomoću digitalnog certifikata, digitalnog potpisa i infrastrukture javnih ključeva (PKI).

Kriptografija se dalje može podijeliti na:

1.Simetričnu (ili tajni ključ) kriptografija i
2.Asimetričnu (ili javni ključ) kriptografija

Primjena u komunikaciji

U današnjem digitalnom svijetu, gotovo svaka vrsta mrežne komunikacije oslanja se na kriptografiju kako bi se osigurala privatnost i sigurnost podataka. Kriptografija omogućuje da podaci ostanu zaštićeni tijekom prijenosa putem interneta, gdje su potencijalno izloženi raznim oblicima presretanja ili manipulacije.

Najčešći primjer primjene je protokol HTTPS, koji štiti komunikaciju između korisnikovog preglednika i web poslužitelja. Osigurava da osjetljive informacije poput lozinki, brojeva kartica i osobnih podataka ne budu dostupne trećim stranama. Slično tome, protokoli SSL/TLS koriste se za enkripciju podataka u aplikacijama poput e-maila ili VoIP poziva.

Također, kriptografija omogućuje autentifikaciju, gdje sustav može potvrditi identitet korisnika pomoću digitalnih certifikata i ključeva. To je posebno važno u poslovnim sustavima, elektroničkom bankarstvu, e-upravi i mnogim drugim sigurnosno osjetljivim okruženjima.

Alati i tehnologije

Razvoj sigurnih komunikacijskih sustava ne bi bio moguć bez konkretnih alata i tehnologija koji implementiraju kriptografske metode. OpenSSL je jedan od najpoznatijih alata otvorenog koda, široko korišten u serverima za implementaciju SSL/TLS protokola. GnuPG (GPG) koristi se za šifriranje datoteka i elektroničke pošte, često u kombinaciji s digitalnim potpisima.

U novije vrijeme, kriptografija je postala temelj blockchain tehnologije. Ona omogućuje stvaranje decentraliziranih sustava, gdje se povjerenje ne temelji na jednoj instituciji, već na matematički zajamčenoj sigurnosti. Kriptovalute poput Bitcoina koriste kriptografske hash funkcije i digitalne potpise za zaštitu transakcija i stvaranje blokova podataka.

Također, u sigurnosno osjetljivim okruženjima koriste se hardverski sigurnosni moduli (HSM) – fizički uređaji koji upravljaju enkripcijskim ključevima i omogućuju visok stupanj zaštite.

Izazovi i budućnost

Unatoč svojoj snazi, kriptografija nije nepogrešiva. Sustavi su često ranjivi zbog loše implementacije, zastarjelih algoritama ili ljudskih pogrešaka. Napadi poput brute-force pokušaja, man-in-the-middle presretanja, te side-channel napadi mogu ugroziti sigurnost ako se ne koriste odgovarajuće zaštite.

Posebnu zabrinutost izaziva razvoj kvantnih računala, koja bi mogla s lakoćom razbiti današnje kriptografske sustave, osobito asimetrične algoritme poput RSA ili ECC. Zbog toga je u tijeku razvoj tzv. postkvantne kriptografije, koja bi trebala biti otporna na napade kvantnih strojeva.

Dodatni izazov čine i društveni aspekti – balans između zaštite privatnosti i potreba državnih institucija za nadzorom u kontekstu nacionalne sigurnosti.

Zaključak

Kriptografija igra ključnu ulogu u zaštiti računalne komunikacije i podataka u digitalnom okruženju. Omogućuje sigurnu razmjenu informacija, autentifikaciju korisnika i očuvanje privatnosti, što je od presudne važnosti u osobnom, poslovnom i državnom kontekstu.

Unatoč velikim prednostima, pred stručnjacima su brojni izazovi, uključujući kibernetičke prijetnje i nadolazeće kvantne tehnologije. Stoga je kontinuirano istraživanje, razvoj i edukacija o kriptografiji nužna za očuvanje sigurnosti u sve složenijem digitalnom svijetu.

Literatura

https://www.simplilearn.com/cryptography-techniques-article

https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html

https://medium.com/@tattwei46/basics-of-cryptography-18d01b952dde

https://www.fortinet.com/resources/cyberglossary/what-is-cryptography

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

https://www.geeksforgeeks.org/cryptography-tutorial/

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

https://www.rain.com/learn/whats-cryptography-and-how-it-functions

https://docs.oracle.com/cd/E19047-01/sunscreen151/806-5397/i996724/index.html

https://www.geeksforgeeks.org/difference-between-encryption-and-decryption/

https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:data-encryption-techniques/a/encryption-decryption-and-code-cracking