1. Elektronički svijet

1.1. Informacijske i komunikacijske tehnologije

Nakon ove nastavne teme moći ćeš:

- opisati načine pristupa internetu
- razlikovati aktivnu i pasivnu mrežnu opremu
- provjeriti brzinu prijenosa podataka vlastitog internetskog priključka.

Danas je teško zamisliti svakodnevni život bez uvijek dostupnog voznog reda, kupovine putem interneta, orijentiranja s pomoću besplatnih digitalnih mrežnih karata, različitih komunikacijskih alata i društvenih mreža. Mnogim je uređajima moguće upravljati putem računalne mreže, brojne aplikacije znatno nam olakšavaju kućanske poslove, privatne i poslovne komunikacije, obrazovanje, liječenje, putovanje i dr. Gotovo su svi važni događaji praćeni društvenim mrežama, a računalne igre povezuju ljude sa svih kontinenata u realnom vremenu. Korištenjem interneta i društvenih mreža tvrtke komuniciraju s potrošačima i odgovaraju na sva njihova pitanja o proizvodu.

Ubrzani razvoj **komunikacijskih tehnologija** omogućio je stvaranje bezbroj novih komunikacijskih alata, uređaja i programske podrške. Procesi prenošenja poruka s uređaja na uređaj odvijaju se u našoj okolini u svakom trenutku, a da toga nismo ni svjesni. Uspostavljanje učinkovite komunikacije s kupcima povećava konkurentnost na tržištu i stvara jak javni imidž. Poslovi se danas ne obavljaju samo u tvrtkama, već se može poslovati putem interneta.

Internet je spoj različitih mreža računala u jedinstvenu javno dostupnu svjetsku računalnu mrežu koja nudi velik broj informacijskih i komunikacijskih usluga. Podatci se internetom prenose komutacijom paketa. Računala međusobno komuniciraju s pomoću protokola koji se naziva ”upravljački mrežni protokol/internetski protokol” (engl. *Transmission Control Protocol/Internet Protocol*, **TCP/IP**). S pomoću interneta korisnici mogu razmjenjivati **elektroničku poštu**, pronaći različite informacije, prenositi datoteke protokolom za prijenos datoteka (engl. *File Transfer Protocol*, **FTP**) te se koristiti nizom servisa i alata.

Kako bi računala mogla međusobno komunicirati, potrebno ih je povezati u **računalnu mrežu**. Računalnu mrežu čine **dva ili više povezanih računala**, a njome se prenose podatci i dijele uređaji (server, pisač, skener i dr.).

Za održavanje lokalne mreže u tvrtkama potreban je **mrežni administrator**, a za veće mreže i nekoliko njih. Računala u lokalnoj mreži (engl. *Local Area Network*, LAN) mogu dijeliti zajednički pristup internetu.

Za **pristup sadržajima na internetu** potrebno se s njime prethodno povezati. Za povezivanje s internetom potrebni su:

- **fizička veza**
- **logička veza**
- **programi**
- **usluga davatelja internetske usluge**, teleoperatera (engl. *Internet Service Provider*, **ISP**).

Fizičkom vezom smatraju se sklopovi, uređaji i pribor koji služe za prijenos signala između osobnog računala i uređaja u računalnoj mreži. U to se ubraja razna mrežna oprema. **Mrežna oprema** se prema primjeni u računalnoj mreži dijeli na **aktivnu** i **pasivnu**. **Aktivna mrežna oprema** obuhvaća uređaje koji koriste izvor električne energije i omogućuju aktivno upravljanje mrežnim prometom. Sastoji se od računala i servera koji stvaraju promet te preklopnika (engl. *switch*), usmjernika (engl. *router*), zvjezdišta (engl. *hub*), obnavljača (engl. *repeater*), pristupnih točaka (engl. *access point*), modema i drugih uređaja koji odašilju, usmjeravaju, primaju, pojačavaju električne signale koji se koriste za mrežnu komunikaciju ili na bilo koji način utječu na njihov protok. **Pasivna mrežna oprema** obuhvaća svu ostalu opremu koja ne zahtijeva električnu struju za rad, a koristi se pri izgradnji komunikacijske infrastrukture računalne mreže, na primjer za kabele, priključke, utičnice, ormare za smještaj mrežnih uređaja i dr.

Logička veza je skup protokola koji omogućuju komunikaciju u računalnoj mreži. **Protokol** je skup pravila koja se primjenjuju kod elektroničkog načina prijenosa podataka u nekoj mreži.

Programi interpretiraju podatke koji se prenose i prikazuju ih u razumljivom obliku.

Internetska usluga u velikoj će mjeri ovisiti o tome koji davatelji internetskih usluga pokrivaju vaše područje te o vrstama usluga koje nude.

S obzirom na vrstu medija postoje dva načina prijenosa podataka: **žični** i **bežični**. **Žični** se prijenos odvija **vodovima** (kabelima) koji mogu biti **bakreni** i **optički**. **Bežični** se prijenos podataka odvija **zrakom**.

1.1.1. Brzina prijenosa podataka

Svakim danom rastu potrebe za prijenosom sve većih količina podataka što većom brzinom. Radi postizanja i održavanja što kvalitetnije komunikacije postojeći se uređaji stalno poboljšavaju i nadograđuju. Danas su na raspolaganju različite vrste komunikacije u nepokretnim i pokretnim komunikacijskim mrežama. Odabir ovisi o tome gdje se korisnik nalazi, koliko vremena ima i koliko je novca u mogućnosti izdvojiti za komunikacijsku uslugu.

Različiti fizički mediji podržavaju prijenos bitova **različitim** brzinama. **Širina propusnog pojasa** (engl. *bandwidth*) u računalnim mrežama predstavlja kapacitet brzine prijenosa podataka nekog medija u digitalnom sustavu, a mjeri se u bitovima po sekundi, b/s (engl. *bits per second*, bps). Predstavlja **teorijsku mogućnost brzine** kojom bi se podatci u nekom digitalnom sustavu mogli prenijeti u idealnim uvjetima. **Digitalna propusnost** ili samo **propusnost** (engl. *throughput*) mjera je prijenosa bitova medijem tijekom određenog vremenskog razdoblja. Mjeri količinu podataka koja može prolaziti s jednog mjesta na drugo tijekom određenog vremena. To je **stvarna brzina** kojom se podatci mogu prenijeti u nekom digitalnom sustavu. Mjeri se također u bitovima po sekundi i obično je manja od propusne širine, a predstavlja omjer količine podataka koji se prenose mrežom i jedinice vremena. U računalnoj mreži propusnost ne može biti brža od najsporije veze na putu od izvora do odredišta. Čak i ako svi segmenti ili većina njih imaju veliku propusnost, dovoljan je samo jedan segment s malom propusnošću da stvori usko grlo propusnosti cijele mreže.

Propusnost je određena nizom faktora, a neki od njih su:

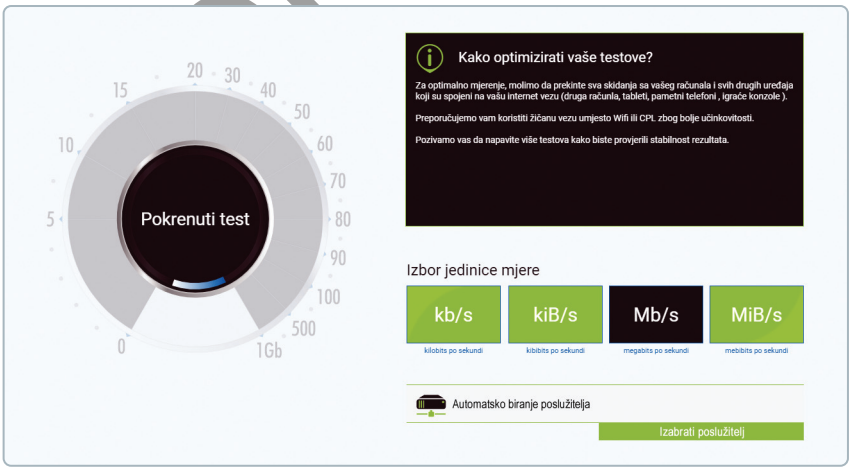
- tehnologije za signalizaciju i otkrivanje mrežnih signala
- svojstva medija
- trenutačne tehnologije
- količina prometa
- vrsta prometa
- kašnjenje signala do kojeg dolazi zbog prolaska kroz mrežne uređaje od izvora do odredišta.

Prilikom prijenosa bakrenim medijima signali su uzorci električnih impulsa. Optičkim se medijima prenose uzorci svjetlosti, a bežično se prenose radiovalovi. Najčešće korištene mjerne jedinice za propusnu širinu, digitalnu i korisnu propusnost prikazane su u tablici 1.1.

Tablica 1.1. Najčešće korištene mjerne jedinice za propusnu širinu, digitalnu i korisnu propusnost

mjerna jedinica za širinu propusnog pojasa i propusnost, digitalnu i korisnu	skraćenica		pretvaranje mjernih jedinica iz veće u manju
	engleski	općenito	
bitovi po sekundi	bps	bit/s	1 bit/s – osnovna mjerna jedinica propusne širine
kilobitovi po sekundi	kbps	kbit/s	1 kbit/s = 10^3 bit/s
megabitovi po sekundi	Mbps	Mbit/s	1 Mbit/s =10^3 kbit/s = 10^6 bit/s
gigabitovi po sekundi	Gbps	Gbit/s	1 Gbit/s = 10^3 Mbit/s = 10^6 kbit/s = 10^9 bit/s
terabitovi po sekundi	Tbps	Tbit/s	1 Tbit/s =10^3 Gbit/s = 10^6 Mbit/s = 10^9 kbit/s = 10^{12} bit/s

Korisnici na internetu mogu provjeriti brzinu prijenosa podataka vlastitog internetskog priključka pristupanju nekom od internetskih servisa koji se bave mjerenjem brzine prijenosa podataka na internetu. Uzmimo za primjer takav internetski servis kojem se pristupa s poveznice: https://www.nperf.com/hr/. Klikom na poveznicu pristupa se početnoj stranici servisa gdje se može odabrati mjerna jedinica u kojoj će se prikazati brzina prijenosa podataka ili ostaviti zadana – Mb/s (slika 1.1).

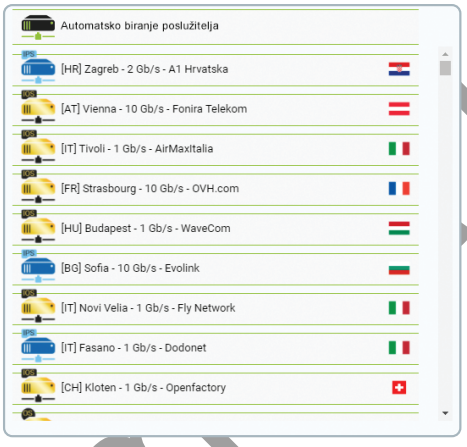


Slika 1.1. Početna stranica servisa koji se bavi mjerenjem brzine na internetu

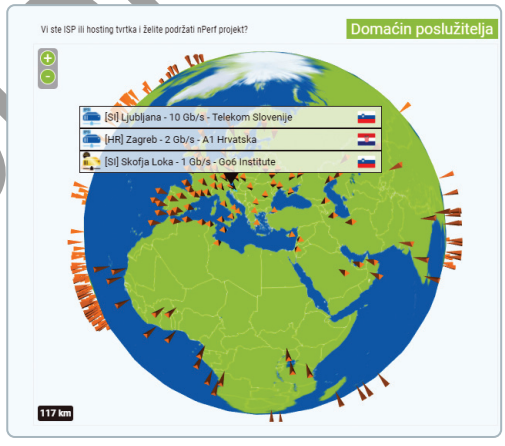
Nakon toga odabire se poslužitelj na izborniku u donjem dijelu stranice (slika 1.2).

Slika 1.2. Izbornik za odabir poslužitelja na stranici servisa

Postoji mogućnost odabira nekoliko desetaka poslužitelja iz cijelog svijeta (slika 1.3) koji su prikazani i na karti (slika 1.4). Klikom na lokaciju poslužitelja na karti svijeta ispisuje se naziv davatelja internetskih usluga koji je ujedno i vlasnik poslužitelja te njegova lokacija. Nakon odabira poslužitelja provjerena je brzina mreže u dva smjera.

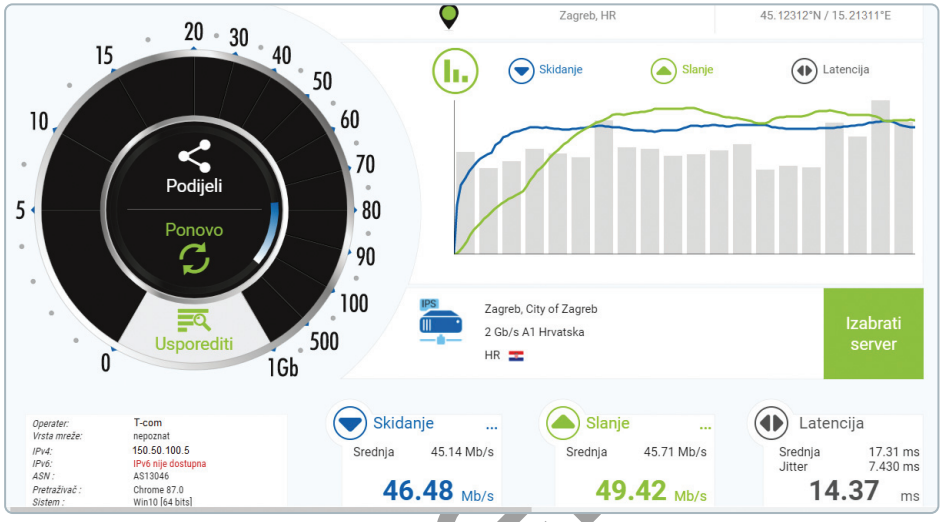


Slika 1.3. Dio popisa poslužitelja raspoloživih za provjeru brzine prijenosa podataka



Slika 1.4. Grafički prikaz poslužitelja raspoloživih za provjeru brzine prijenosa podataka

Nakon nekoliko trenutaka potrebnih da probni paket podataka prođe od poslužitelja do korisnika i nazad, na stranici servisa ispiše se brzina preuzimanja i brzina slanja podataka kao i kašnjenje njihova prijenosa, **latencija**.



Slika 1.5. Ispis brzine preuzimanja i brzine slanja, kašnjenje prijenosa i latencija

Pitanja za ponavljanje

1. Usporedi aktivnu i pasivnu mrežnu opremu.
2. Provjeri brzinu prijenosa podataka vlastitog internetskog priključka.

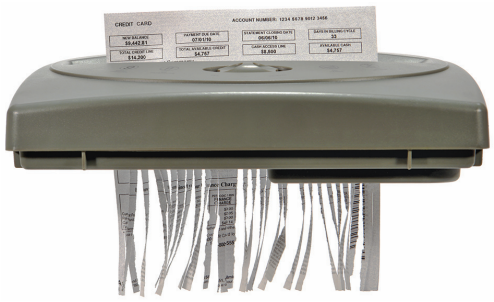
1.2. Sigurnost i računalni virusi

Nakon ove nastavne teme moći ćeš:

- objasniti pojam informacijske sigurnosti
- usporediti simetrično i asimetrično kriptiranje
- usporediti javni i privatni ključ
- navesti i objasniti značajke kriptografije
- opisati digitalni potpis
- navesti štetne programe i opisati njihovo djelovanje
- objasniti kako se svojim korisničkim navikama možemo zaštititi od djelovanja štetnih programa.

Internetom svakodnevno prolazi i pohranjuje se na računalima i poslužiteljima velika količina informacija. I tvrtke i građani kao privatne osobe upotrebljavaju veliku količinu informacija s interneta, a ujedno i šalju mnoge informacije o sebi i svojem poslovanju. Zbog toga je nužno da podatci na internetu budu odgovarajuće zaštićeni. Najjednostavniji primjer dostupnosti podataka je internetski servis Google karte koji nam pomaže u svakodnevnom snalaženju u prometu. Sjetite se samo na koliko mjesta upisujemo bez razmišljanja adresu stanovanja, a utipkavanjem adrese u tražilicu servisa jako se lako dozna gdje se nalazi nečiji dom, kako mu se prilazi i slično.

Informacijska sigurnost obuhvaća načine i sredstva za zaštitu tiskanog, elektroničkog ili bilo kojeg drugog oblika povjerljivih, privatnih i osjetljivih podataka od neovlaštenog pristupa, uporabe, zlouporabe, otkrivanja, uništavanja, preinake ili ometanja. Očuvanje sigurnosti podataka težak je zadatak jer se većina tvrtki i ustanova neprestano suočava s dinamičnim okruženjem koje utječe na njihovo poslovanje: promjena zakona i propisa, napredak tehnologije, otkrivanje novih ranjivosti, proširenje tržišta i dr. Na slici 1.6 prikazana je naprava za uništavanje rezanjem na trake papirnatih povjerljivih dokumenata kakva se primjenjuje u mnogim tvrtkama i ustanovama.



Slika 1.6. Naprava za uništavanje rezanjem na trake papirnatih povjerljivih dokumenata

1.2.1. Kriptografija

Stoljećima su se ljudi domišljali načinima kako zaštititi svoju pisanu komunikaciju od neželjenih pogleda. Prvi pronađeni tragovi šifriranja potječu iz davnine. Oko 1900. godine pr. Kr. u Egiptu je nastao natpis koji se danas smatra prvim dokumentiranim primjerom šifriranja. Rimski car Gaj Julije Cezar (100. pr. Kr. – 44. pr. Kr.) nije vjerovao glasnicima u komunikaciji sa svojim guvernerima i časnicima pa je stvorio sustav u kojem je zamijenio svako slovo razgovijetnoga teksta trećim slovom u abecednome slijedu iza njega. Na taj je način kriptirao sve poruke, pa i pisma Ciceronu i drugim prijateljima.

Uzmimo za primjer Cezarovo ime u potpisu. U tablici 1.2 prikazat ćemo njegov način šifriranja uz uporabu naših abecednih znakova. Cezarovo ime zapisano s pomoću njegova načina šifriranja i hrvatskih slova abecede izgledalo bi kao u četvrtom retku tablice 1.2.

Tablica 1.2. Primjer šifriranja Cezarova imena s pomoću njegova sustava hrvatskim abecednim znakovima

A B C Č Ć D Dž Đ E F G H I J K L LJ M N NJ O P R S Š T U V Z Ž	hrvatska abeceda
GAJ JULIJE CEZAR	originalni raspored slova u potpisu
D E F G H I J K L LJ M N NJ O P R S Š T U V Z Ž A B C	kriptirana abeceda
JDLJ LJŽNLLJH FHBDT	potpis prema Cezarovu načinu šifriranja

Praksa šifriranja nastavljala se tijekom povijesti, a u tu su svrhu razvijene različite naprave. Na slici 5.1 prikazan je starinski mehanički šifrarnik s pomičnim kotačima na kojima se nalaze slova. Korisnici su mogli odabrati po kojem će ključu pomicati slova prilikom zadavanja ili otkrivanja šifri.

Slika 1.7. Starinski mehanički šifrarnik

Kriptografija je znanstvena disciplina koja proučava metode zaštite informacija i komunikacije korištenjem kodova prevedenih tako da ih može pročitati samo onaj kome su namijenjeni.

Osnovni zadatak kriptografije je omogućiti pošiljatelju i primatelju poruke **sigurnu komunikaciju putem nesigurnog**

komunikacijskog kanala (npr. telefonska linija, dijelovi računalne mreže) tako da treća osoba ne razumije poruke. Pritom **pošiljatelj preoblikuje poruku** prema unaprijed dogovorenom **ključu** koji je poznat samo primatelju. Dogovoreni ključ prema kojem se preoblikuje poruka naziva se **šifra**, a sam postupak preoblikovanja poruke **šifriranje** ili **kriptiranje**. Obrnuti postupak, kojim se poruka vraća u prvobitni oblik, naziva se **dešifriranje** ili **dekriptiranje**. Kriptirana poruka naziva se **kriptogram**. Funkcije kriptiranja i dekriptiranja zajedno čine **kriptosustav**. Danas se kriptografija primjenjuje kad se želi osigurati privatnost ili tajnost poruka, npr. pri slanju naloga u elektroničkom bankarstvu.

Kriptografija se bavi podatcima u digitalnom obliku. Matematički postupci kriptiranja i dekriptiranja provode se automatski, uz pomoć računala. U internetskim uslugama i informacijskim tehnologijama općenito kriptografija se odnosi na sigurne informacijske i komunikacijske tehnike. Načelo njihovog rada temelji se na razvoju algoritama za generiranje kriptografskih ključeva, digitalno potpisivanje dokumenata, provjeru s ciljem zaštite podataka, pregledavanje interneta i povjerljivu komunikaciju poput transakcija kreditnom karticom i slanja elektroničke pošte. Na slici 1.8 prikazan je primjer šifriranja znakovima, na slici 1.9 primjer šifriranja binarnim kodom.

Slika 1.8. Primjer šifriranja znakovima

Slika 1.9. Primjer šifriranja binarnim kodom

Prilikom kriptiranja tekstualnih poruka dvije su **vrste šifri**:

- blokovne
- protočne.

Blokovnim se **šiframa** kriptira jedan po jedan blok elemenata poruke uz primjenu iste šifre. **Protočnim** se **šiframa** kriptira element po element uz primjenu različitih šifri. Kod zahtjevnijeg se kriptiranja u istoj poruci mogu koristiti obje vrste šifri.

Osnovne metode kriptiranja su:

- supstitucija
- transpozicija.