UPORABA IKT V NARAVOSLOVJU IN TEHNIKI

Predavanje 7

Komunikacije in internet

doc.dr. Mira Trebar

Vsebina

- Uvod
- Prenos informacije
- Omrežja in protokoli
- Povezovanje omrežij
- Komunikacija med procesi
- Internet
- Dostop do Interneta
- Internetne aplikacije
- Varnost

Uvod

- Komunikacije – proces prenosa informacij
- Komunikacijske poti: po zemlji, po vodi, sateliti
- Komunikacijski sistemi - Računalniško omrežje
  - med seboj povezani avtonomni računalniški sistemi,
    - prenašanje podatkov med računalniškimi sistemi in
    - delitev računalniških virov
  - komunikacijska oprema (strojno in programsko),
- Razlogi za razvoj računalniških omrežij
  - izmenjava podatkov med geografsko razpršenim organizacijami
  - preko omrežij imajo mnogi uporabniki dostop do
    - zmogljivih računalniških sistemov,
    - drage strojne ali programske opreme (barvni laserski tiskalniki,...),
    - razpršene podatkovne baze

Prenos informacije

- Informacija - fizikalna veličina (napetostni nivo)
- Telefonska linija – analognega signala - Modem

- Telefonski signali: DSL-Digital subscriber line (2Mb/s)
- Televizijski signali - kabelski modem (2Mb/s)
- Ethernet (sredi 70tih) – komercialno in pisarniško okolje
  - Koaksialni kabel (10Mb/s)
- Fast Ethernet (100Mb/s)
  - Koaksialni kabel ali optična vlakna
  - Sukana parica
- Gigabit Ethernet standard (1Gb/s,10Gb/s, 100gb/s)

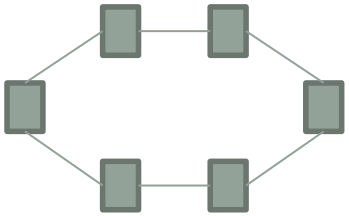
Delitev omrežij

- Velikost omrežja:
  - lokalno omrežje, LAN (ang. local area network)
    - sistemi v takem omrežju so si geografsko dokaj blizu
    - za tako omrežje običajno skrbi ena sama organizacija
  - mestna omrežja, MAN (ang. metropolian area network)
    - omrežje na nivoju velemesta
  - področna omrežja, WAN (ang. wide area network)
    - omrežja, ki se razprostirajo po širokem geografskem področju
- Javna (odprta) in zasebna (zaprta) omrežja
  - internet – javno omrežje
  - intranet – zasebno omrežje
- Glede na povezavo
  - fizična povezava,
  - brezžična povezava (WLAN)

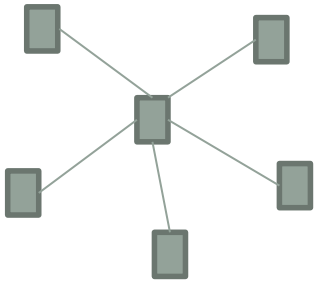
Topologija omrežij

- LAN
  - Vodilo

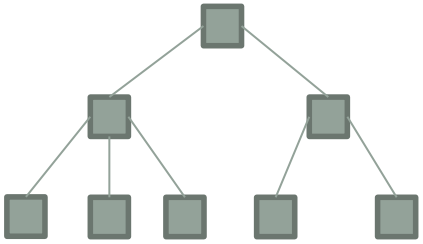
  - Zanka



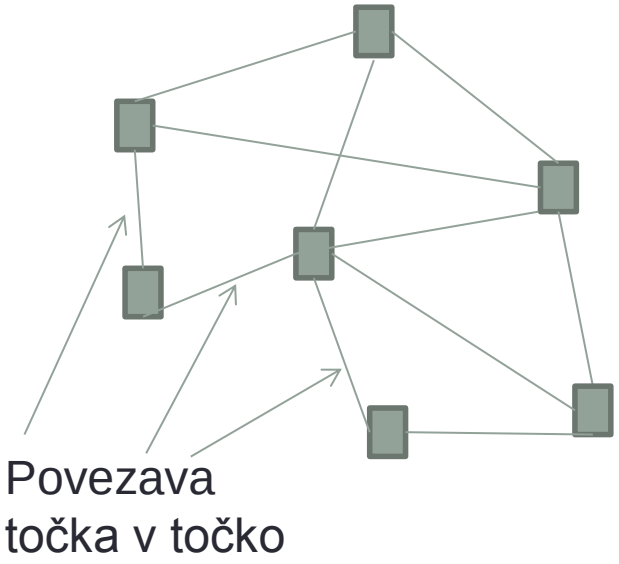
  - Zvezda



  - Drevo



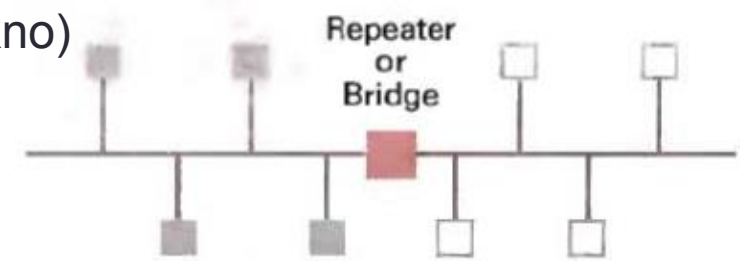
- WAN
  - Mreža



Povezovanje omrežij – naprave (1)

- Lokalna omrežja povezujemo v večja omrežja
- **Mrežna kartica**
  - Samostojna
  - integrirana na matično ploščo 10 / 100 / 1000 Mbit/s
  - Avtomatsko prilagajanje na hitrost omrežja

- **Ojačevalnik** (ang. repeater)
  - prenaša **vse** signale iz prvega omrežja v drugo in obratno
  - združevanje omrežij (žica in optično vlakno)
  - dolga omrežja, ojačenje signala

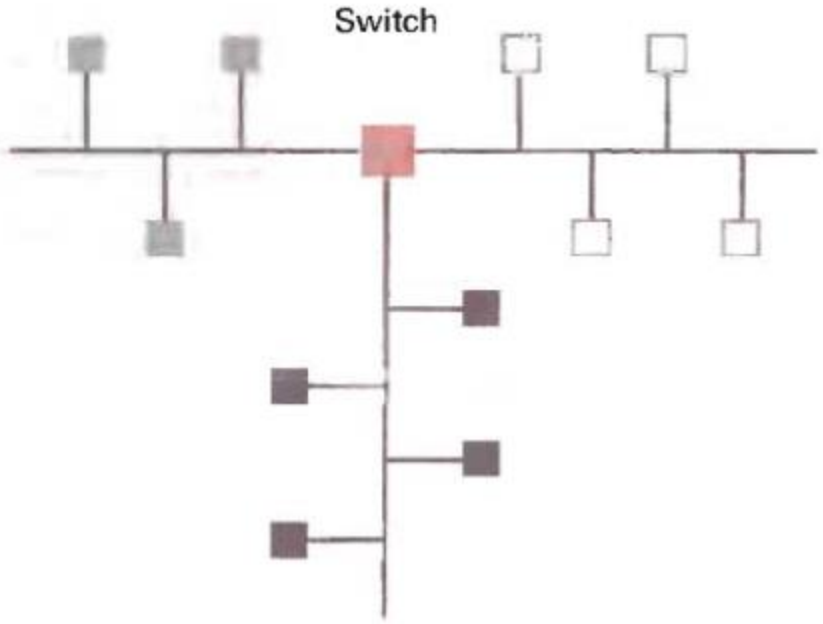


- **Most** (ang. bridge)
  - prenaša signale iz prvega omrežja v drugo in obratno
  - prenaša **samo** tiste signale, ki so namenjeni v sosednjeomrežje
    - promet znotraj omrežij lahko nemoteno poteka istočasno

Povezovanje omrežij – naprave (2)

- **zvezdišče** (ang. hub)
  - hkrati povezuje več omrežij
  - je ojačevalnik z več povezavami
  - med omrežji prenaša **vsa** sporočila

- **stikalo** (ang. switch)
  - hkrati lahko povezuje več omrežij
  - je most z več povezavami
  - med omrežji prenaša samo **potrebna** sporočila

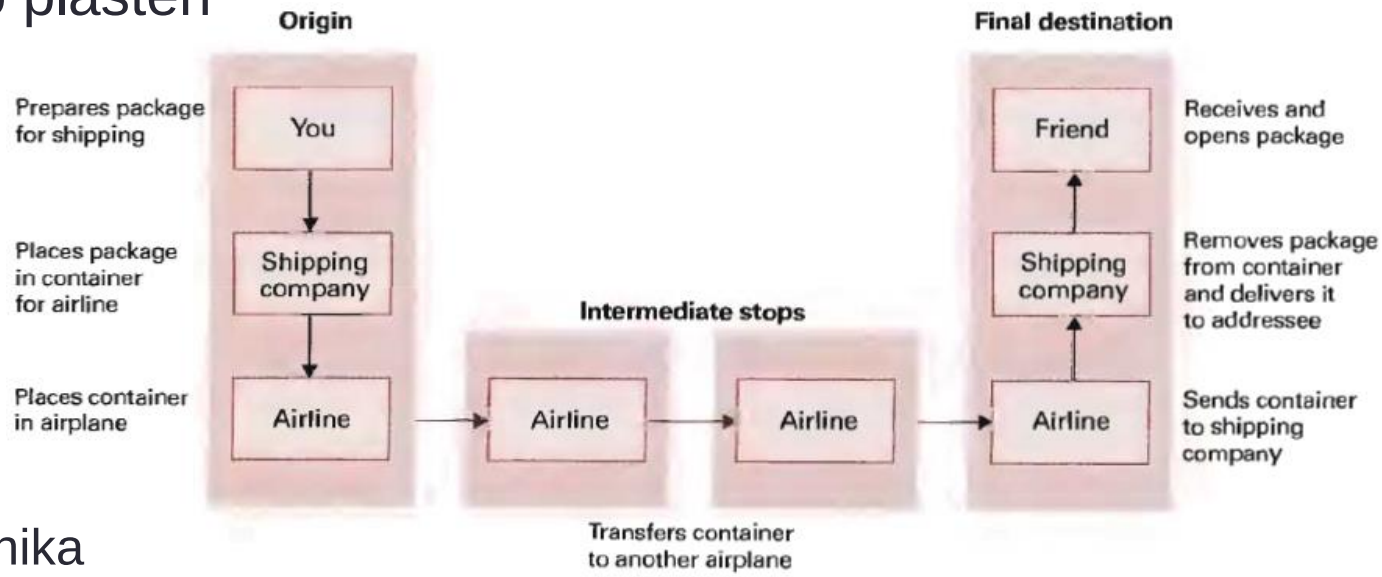


Povezovanje omrežij – naprave (2)

- **usmerjevalnik** (ang. router)
  - osnovna funkcija je enaka kot pri stikalu
  - povezovanje lokalnih (LAN) in področnih omrežij (WAN)
  - primeri
    - usmerjanje prometa med omrežji, ki uporabljajo različne naslovne sheme
    - povezava brezžičnega in žičnega omrežja
  - preko usmerjevalnika več računalnikov v omrežju LAN dostopa do interneta (WAN) preko enega naslova WAN
    - funkcija prehoda (ang. gateway)
    - vsak paket vsebuje naslov pošiljatelja (LAN) in naslov prejemnika,
    - usmerjevalnik si oba podatka zabeleži, nato zamenja naslov pošiljatelja (LAN) s svojim naslovom v omrežju WAN,
    - ko prejemnik odgovori in paket pripotuje do usmerjevalnika, le-ta glede na tabelo zamenja svoj naslov WAN z naslovom računalnika v LAN
  - zaradi usmerjevalnikov imamo lahko na tisoče omrežij LAN, v katerih imajo računalniki enake naslove

Modeli omrežij: uvod

- Pristojnosti komunikacijskih programov so razdeljene po plasteh



  - plast uporabnika
  - plast pošte
  - plast letalske družbe

  - uporabnik ne pozna podrobnosti delovanja pošte
  - pošta ne pozna podrobnosti delovanja letalske družbe

Modeli omrežij: standardi

- Standardi določajo
  - plasti komunikacijskega procesa in
  - protokole znotraj vsake plasti

- Komunikacija poteka v več plasteh
  - sprememba nižje plasti (na primer fizične povezave) ne vpliva na višje plasti (na primer brskalnik)
  - za komunikacijo v omrežju lahko uporabljamo enostavne naprave, ki podpirajo samo nižje plasti

  - modeli lahko uporabljajo poljubno število plasti
  - več plasti, večja modularnost, bolj počasna omrežja

Modeli omrežij - protokoli

- Protokol – vzajemno dogovorjena pravila, dogovori in sporazumi za uspešno izmenjavo informacij v omrežju.
  - Omrežni : IP (Internet Protocol)
  - Prenosni :
    - TCP (Transport Layer Protocol),
    - UDP (User Datagram Protocol)
  - Aplikacijski nivo:
    - HTTP (Hypertext Transfer Protocol)
    - SMTP (Simple Mail Transfer Protocol)
    - POP3 (Post Office Protocol)
    - IMAP (Internet Message Access protocol)
    - FTP (File Transfer Protocol)
    - TELNET (Terminal Emulation Protocol)
    - DNS (Domain Name System)

Aplikacija	Port
splet	80
e-pošta (pošiljanje)	25
e-pošta (sprejem)	110
e-pošta (sprejem)	143
datoteke	21
terminali	23
imena –IP	42

Modeli omrežij: ISO OSI referenčni model

- ISO – OSI (ang. International Standard Organization
  Open Systems Interconnection)
- fizična plast:
  - predpisuje prenosni medij preko katerega se prenašajo podatki,
  - definira nivo signala, hitrost prenosa, način zapisa podatkov,
- povezovalna plast:
  - skrbi za prenos podatkov po fizični plasti, vključuje detekcijo napak in sistem za ponovno pošiljanje pokvarjenih podatkov
- omrežna plast:
  - sporočila razdružuje v pakete, pakete usmerja po omrežju in jih sestavlja nazaj v sporočila
  - primer: internetni protokol (IP)

Modeli omrežij: ISO OSI referenčni model

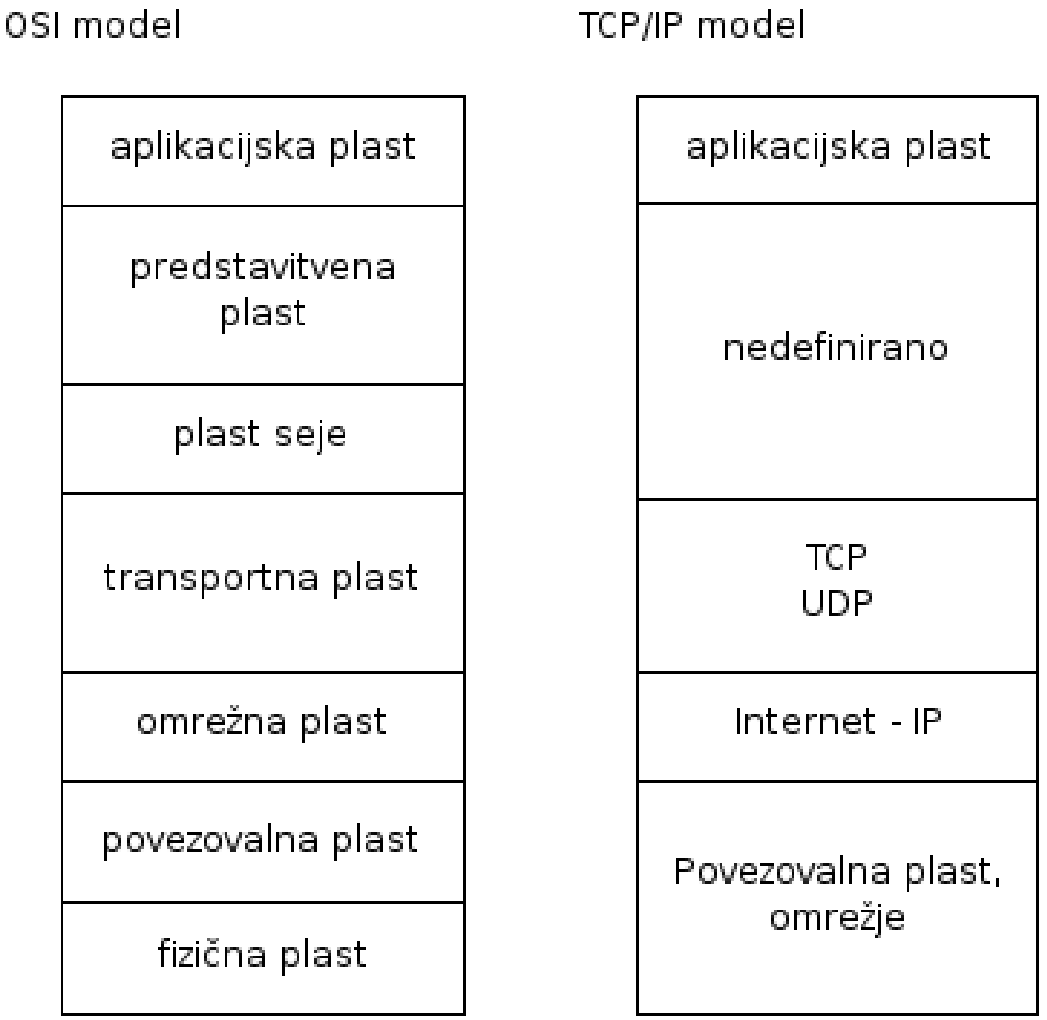
- transportna plast:
  - zakriva spodnje tri plasti pred zgornjimi – vsi protokoli so definirani samo na računalnikih, vpletenih v komunikacijo, ne pa na posrednikih
  - nadzor povezav in prenos podatkov
  - primera:
    - TCP (ang. Transmission Control Protocol),
      - počasnejši, bolj zanesljiv
      - obvesti sprejemnika o pošiljanju, po potrditvi začne s pošiljanjem
    - UDP (ang. User Datagram Protocol)
      - hitrejši, manj zanesljiv
      - pošlje sporočilo in pozabi nanj
- plast seje:
  - vzpostavlja, nadzira in prekinja logično povezavo med računalniki
- predstavitvena plast:
  - pretvarja podatke, poslane po omrežju, iz ene v drugo obliko, določa način zapisa, razdruževanje in sestavljanje podatkov

Modeli omrežij: ISO OSI referenčni model

- aplikacijska plast:
  - vmesnik med uporabnikom in modelom OSI
  - primeri:
    - protokoli za elektronsko pošto
      - SMTP (ang. Simple Mail Transfer Protocol)
      - POP (ang. Post Office Protocol)
      - IMAP (ang. Internet Message Access Protocol),
    - svetovni splet
      - HTTP(S) (ang. Hyper Text Transfer Protocol (Secure))
    - prenašanje datotek
      - FTP (ang. File Transfer protocol), …
      - SSH (ang. Secure SHell) ali SFTP (ang. Secure File Transfer Protocol)
    - oddaljeni dostop na računalnik
      - TELNET (ang. TELetype NETwork)
      - RDP (ang. Remote Desktop Connection)

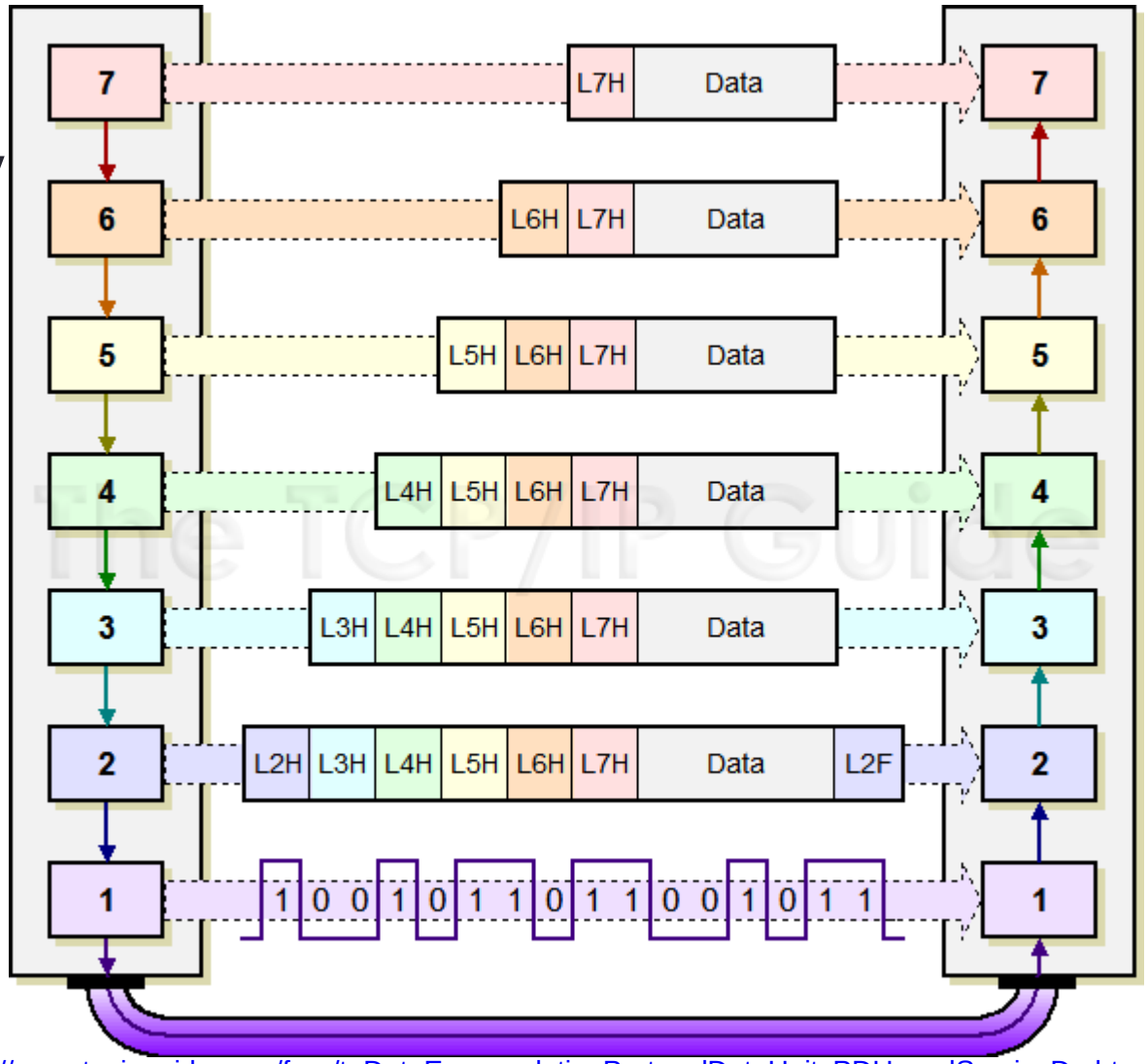
Modeli omrežij: TCP/IP

- ISO OSI referenčni model in model TCP/IP
  - aplikacijska plast
    - računalnik ima samo en internetni naslov
    - na njem lahko teče več procesov
    - da se ve kateremu procesu pripada kakšen paket jim dodelimo vrata (ang. port)
      - http: 80
      - ftp: 20, 21



Pošiljanje podatkov – TCP/IP

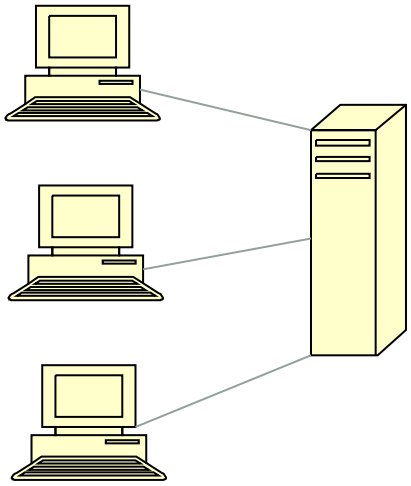
- Slojni protokoli
- ovijanje podatkov

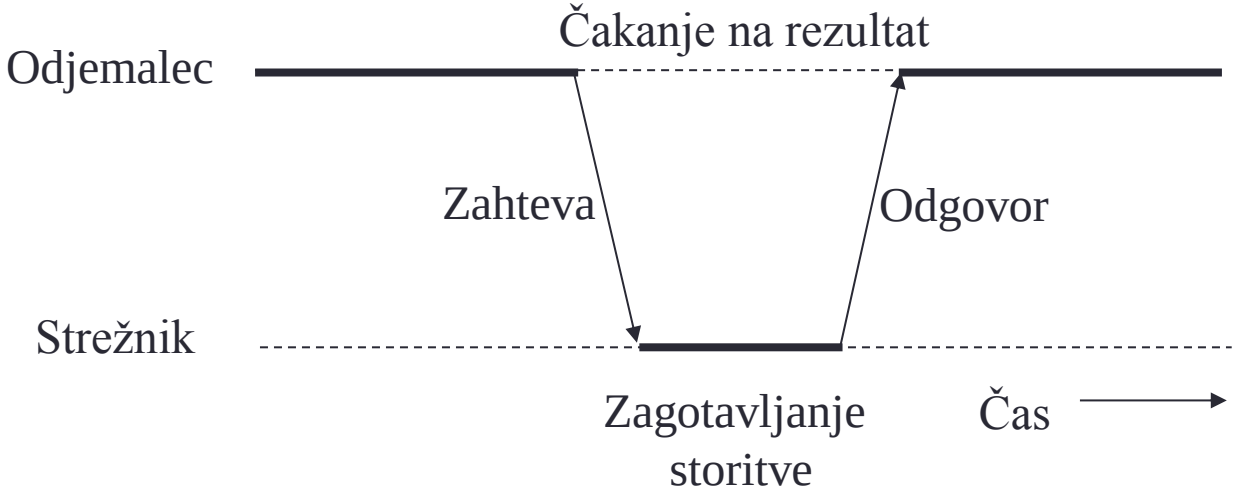


http://www.tcpipguide.com/free/t_DataEncapsulationProtocolDataUnitsPDUsandServiceDa.htm

Komunikacija med procesi (1)

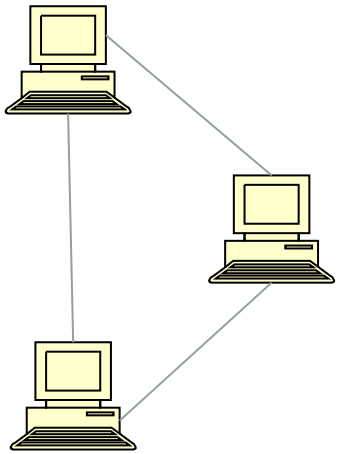
- Različni računalniki - koordiniranje akcij za izvajanje nalog
- odjemalec – strežnik (ang. client – server):
  - odjemalec podaja zahteve, strežnik jih izvršuje
    - strežnik – računalnik na katerega je priklopljen poseben tiskalnik
    - odjemalci – od strežnika zahtevajo izpis datotek, ..
  - Komunikacija poteka na osnovi pošiljanja sporočil.

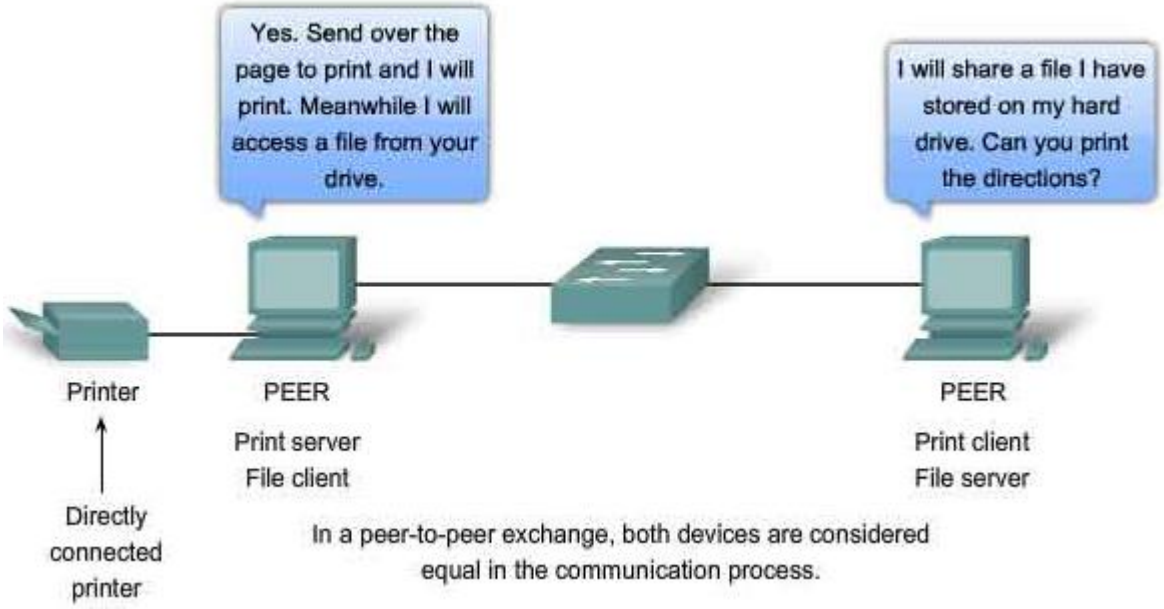




Komunikacija med procesi (2)

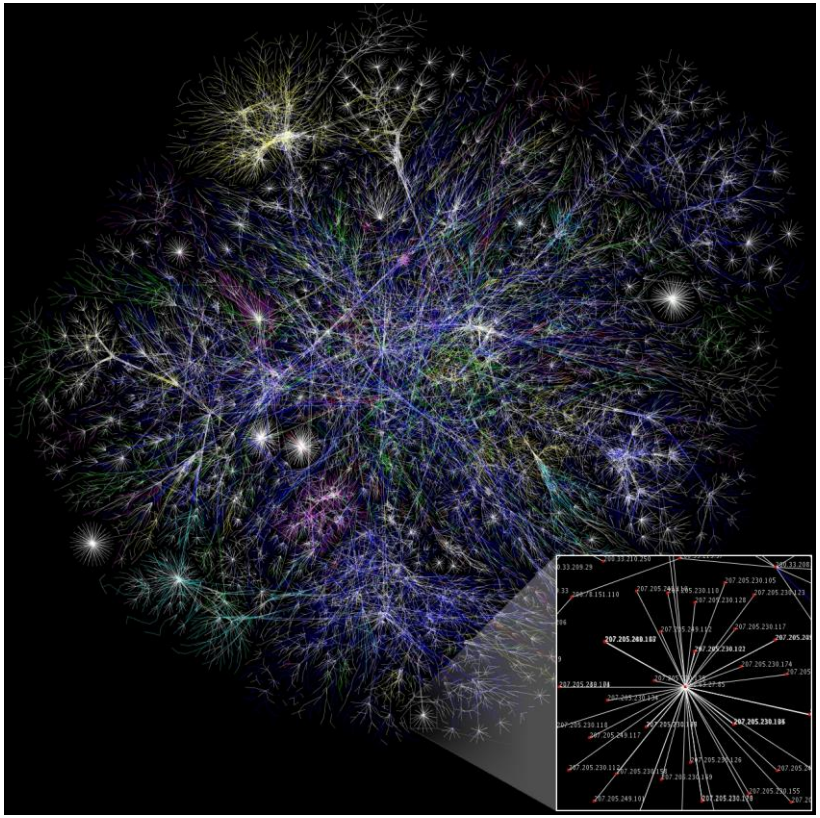
- brat – bratu (ang. peer to peer, P2P)
  - računalniki (procesi) so si enakovredni
  - vsak nastopa hkrati kot odjemalec in strežnik
    - orodja za sporočanje (Skype, Messanger),
    - internetne igre
    - skupna raba datotek (glasba, filmi)





Internet

- Omrežje računalniških omrežij - protokol TCP/IP (1983)
- Arhitektura - slika omrežja
  - domene in poddomene
  - **ucilnica.fktt.uni-lj.si**
    - domena: **si**
    - pod-domena: **uni-lj**
    - pod-pod-domena: **fkkt**
    - računalnik **ucilnica**
- Nad internetnimi domenami bedi ICANN (The Internet Corporation for Assigned Names and numbers) s tremi lokalnimi registrarji
  - RIPE (Evropa),
  - ARIN (Amerika),
  - APNIC (Azija)



Internet – uporabnik

- Modem
  - Kabel (Cable)
  - DSL – Digital Subscriber Line
- Usmerjevalnik (Router)
  - Fiksne povezave (wired)
  - Brezžične povezave (wireless)
- Računalnik
  - Namizni (Desktop)
  - Prenosni (Laptop)
- Strežnik
- Tiskalnik
- Žepni PC (iPaq-Pocket PC)
- ?

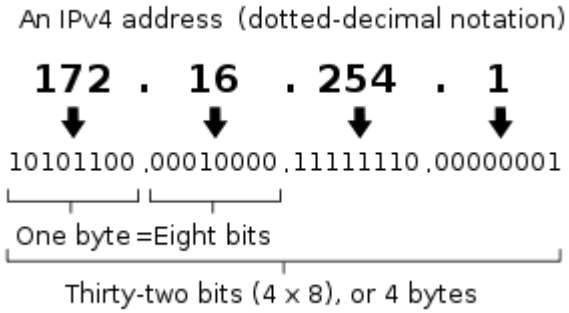
http://yourpctips.com/Computer-Tips-and-Tricks/what-is-wireless-network.html

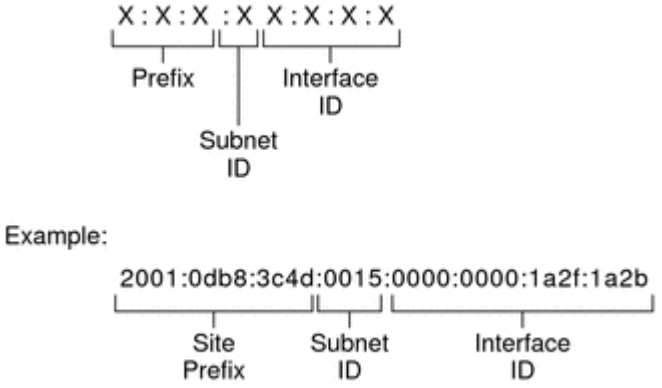
Internet – DNS

- Sistem domenskih imen - DNS (Domain Name Server)
  - Nabor postopkov, storitev, pravil in formatov za dodeljevanje imen posameznim lokacijam v internetnem omrežju.
  - Naloge:
    - Prevajanje imen v omrežne naslove–imenski strežnik (Name server).
    - Iskanje IP gostiteljskih računalnikov na oosnovi imen domenskih imen.
  - Domena:
    - Vzdrževanje baze podatkov imenskega strežnika
    - Vodi strežnik po katerem povprašujejo drugi sistemi
    - Sporočila, namenjena računalnikom v domeni, ostanejo znotraj domene.
  - Usmerjevalnik - prehod (ang. gateway) :
    - Povezovanje registrirane domene v internetnem omrežju -
    - Skrbi za sporočila, namenjena računalnikom v oblaku

Internet – Naslovi

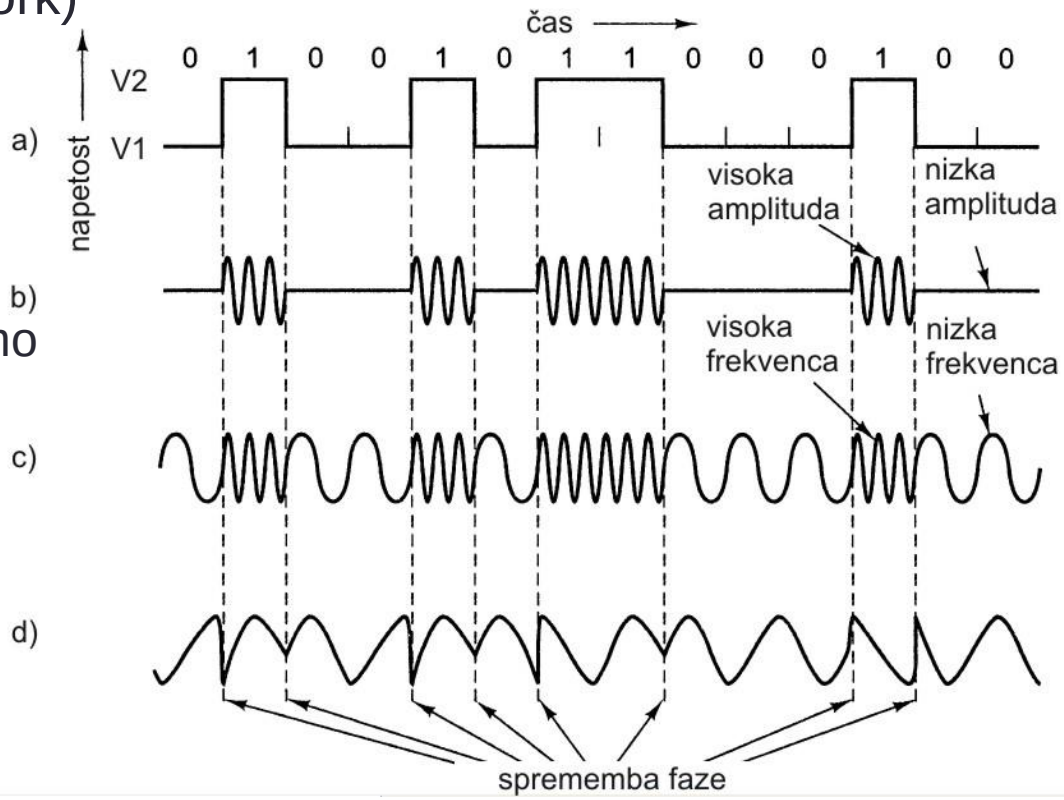
- **IPv4** - Internetni Protokol verzija 4
  - 32 bitov – 4 x 8 bitov (0..255) ali 4 decimalne številke
  - Primer: naslov: **193.2.110.197,** ime: **ucilnica.fkkt.uni-lj.si**
  - oznaka omrežja, ki jo poda lastnik nadrejene domene,
  - oznaka računalnika, ki jo poda operater domene
  - Različni razredi domen - vsaka ima svoj imenski strežnik
- **IPv6** – rešitev za pomanjkanje naslovov
  - 128 bitov → 3,4 x 10^{38} različnih naslovov





Dostop do Interneta (1)

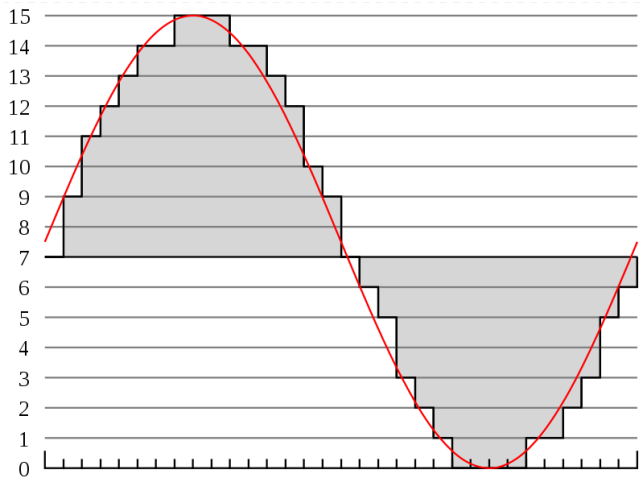
- Modem
  - MOdulator / DEModulator
  - prenos podatkov po klasični telefonski liniji PSTN (ang. Public Switched Telphone Network)
  - Digitalni signal (0,1) - napetost
    - Direktni prenos **a)**
      - prihaja do popačenj
    - Rešitev: signal moduliramo
      - amplitudno b),
      - frekvenčno c)
      - fazno d)
      - lahko tudi kombinacije



Dostop do Interneta (2)

- ISDN (ang. Integrated Services Digital Network)
  - medij je klasična telefonska linija (parici)
    - digitalen prenos podatkov mogoč z nadgradnjo infrastrukture

  - ponuja
    - dva kanala B po 64 kbit/s
      - prenos podatkov po enem ali obeh, prenos govora po enem ali po dveh
    - kanal D s 16 kbit/s
      - servisne storitve (vzpostavitev klica)
  - prenos govora v digitalni obliki



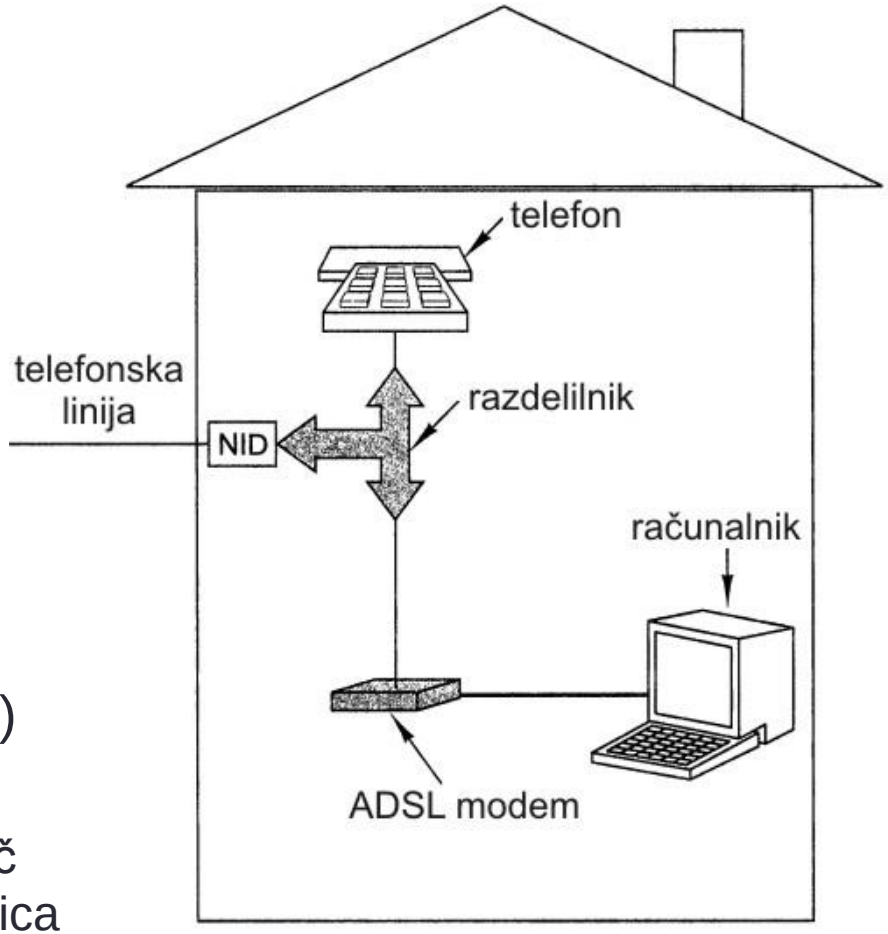
  - za priklop na računalnik potrebujemo pretvornik TA (ang. Terminal Adaptor)

Dostop do Interneta (3)

- **xDSL** (ang. Digital Subscriber Lines)
  - širokopasovni dostop do interneta (= več kot ISDN)
  - iz central odstranijo filtre frekvenc, višjih od 3000 Hz
  - za prenos podatkov na razdalji nekaj km je primeren 1,1 MHz pas, razdeljen na 256 pasov širokih po 4 kHz
    - 0 – prenos govora
    - zgornjih 250 namenjenih prenosu podatkov
      xDSL = 250 modemov

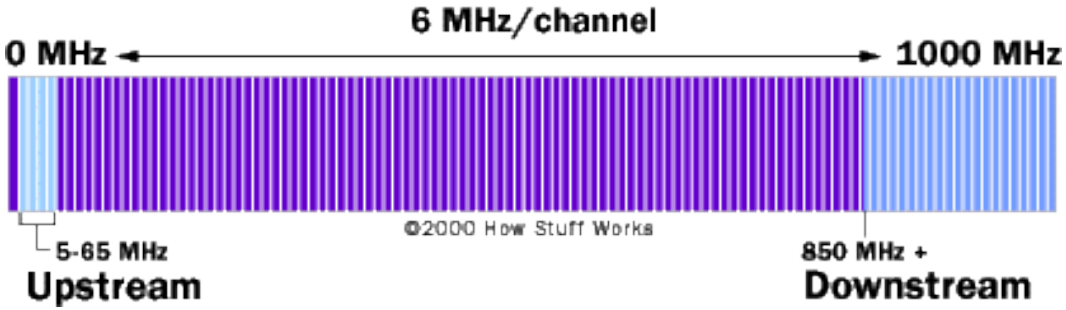
Dostop do Interneta (4)

- SDSL – število kanalov za prenos iz interneta in na internet je enako (simetrična razdelitev)
- ADSL – običajno 32 kanalov za prenos na internet, ostali za prenos iz interneta (asimetrična razdelitev)
- Zmogljivost
  - teoretična: 13,44 Mbit/s
  - realna: do 8 Mbit/s
- Tipična postavitev
- VDSL (ang. Very High Speed DSL)
  - razširitev ADSL za kratke razdalje
  - optična vlakna do vozlišč, od vozlišč do končnih porabnikov bakrena parica



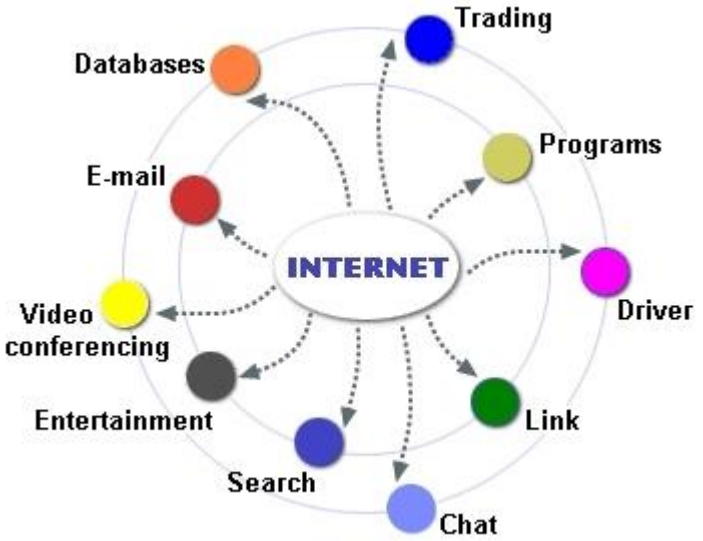
Dostop do Interneta (5)

- Kabelski internet
  - Ponudniki televizijskih programov
  - Medij:
    - širokopasovni kabli – pasovna širina 750 MHz,
    - optična vlakna – večje pasovne širine (ang. Fibre To The Building, FTTB)
  - televizijski programi zasedajo 65 - 850 MHz, 6 – 8 MHz za program
  - Za prenos podatkov ostane na voljo območje do 65 MHz in nad 850 MHz
  - Zaradi večje pasovne širine (predvsem pri optičnih kablih) so mogoče bistveno višje hitrosti – 100 Mbit/s in več
  - Za razliko od xDSL si kabel do vozlišča deli več uporabnikov, zato je potrebno šifriranje sporočil
  - Signal je moduliran – med računalnikom in omrežjem potrebujemo ustrezen modem



Internetne aplikacije

- Tradicionalne
  - elektronska pošta
  - prenos datotek
  - oddaljeni dostop do računalnikov
  - svetovni splet



http://www.astrosurf.com/luxorion/qsl-future-communications.htm

- Novejše
  - internetna telefonija
  - oddajanje radijskega signala in televizijske slike

Internetne aplikacije: elektronska pošta

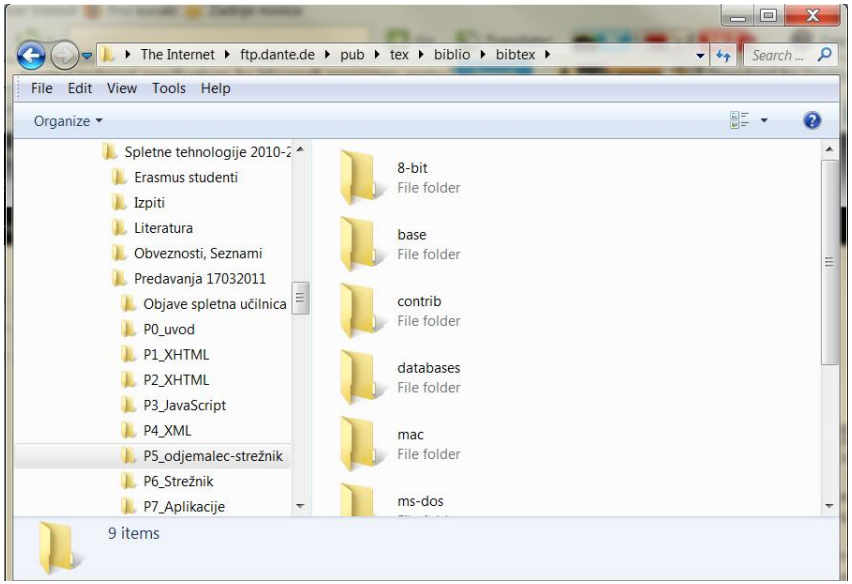
- ang. electronic mail, e-mail
- ena najbolj uporabljanih aplikacij
- v domeni za elektronsko pošto skrbi poštni strežnik
  - računalnik z namensko programsko opremo
  - računalniki v domeni pošto pošiljajo na poštni strežnik
  - poštni strežnik jo razpošilja v oblak
  - prejeta pošta je shranjena na poštnem strežniku dokler je uporabnik ne pobere
- Elektronski naslov:
  - Zgradba: oznaka_osebe@oznaka_strežnika
  - Primer: mira.trebar@fri.uni-lj.si

Internetne aplikacije: elektronska pošta

- Protokoli
  - SMTP (ang. Simple Mail Transfer Protocol)
    - Oddajanje pošte na strežnik
  - POP (ang. Post Office Protocol)
    - POP3
    - pošta se pretoči na lokalni računalnik, kjer jo preberemo
    - primerno, če za branje pošte uporabljamo en sam računalnik
  - IMAP (ang. Internet Message Access Protocol),
    - pošta se hrani na strežniku
    - na strežniku rabimo veliko prostora
    - primerno, če za branje uporabljamo več računalnikov
  - Exchange – podrobnejše specifikacije za Microsoftove lastniške protokole

Internetne aplikacije: prenos datotek

- aplikacija tipa odjemalec - strežnik
  - poseben program,
  - delno vključen tudi v brskalnike
- protokol
  - FTP (ang. File Transfer protocol),
  - SFTP (ang. Secure FTP)
  - shrambe za datoteke
  - primer: ftp://ftp.dante.de



Internetne aplikacije: oddaljeni dostop

- TELNET (ang. TELetype NETwork)
  - dostop na oddaljeni sistem v obliki ukazne vrstice: **telnet** *hostname* [*port*]
  - komunikacija ni šifrirana
    - prenašanje uporabniških imen in gesel ni varno
- SSH (ang. Secure Shell)
  - dostop v obliki ukazne vrstice,
  - rešen problem s šifriranjem sporočil
  - PuTTY program za uporabo z Windows OS
- RDP (ang. Remote Desktop Connection)
  - Microsoftov protokol za dostop do namizja oddaljenega računalnika:
  - Teamviewer pogram

Varnost (1)

Varnost računalnika
Varnost osebnih podatkov

Omrežna varnost
Varna izmenjava sporočil

Varnost gostitelja

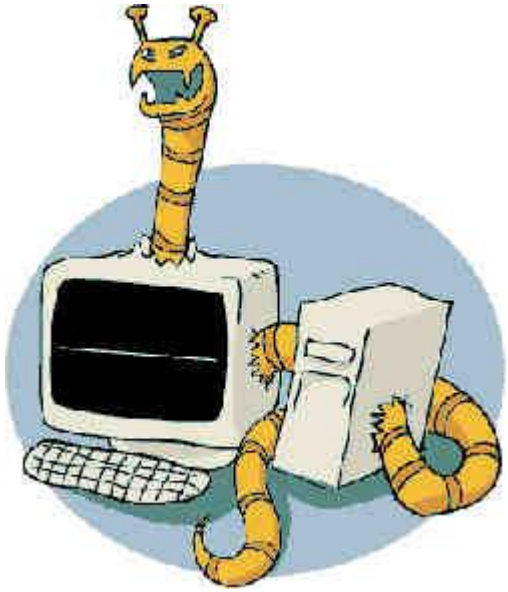
- Zavarovati odjemalca in njegove osebne podatke
- Varovanje podatkov ob prenosu
- Varovanje strežnika in tam shranjenih podatkov

Varnost (2)

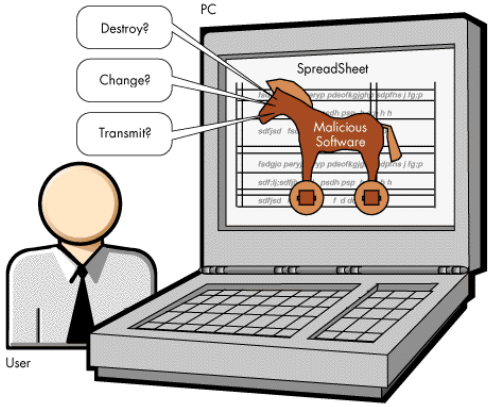
- Računalniki v omrežju so ogroženi
  - nepooblaščeni dostop, vandalizem
- Oblike napadov
  - Zlonamerna programska oprema (ang. malware)
    - lahko jo prenesemo na računalnik kjer se izvaja
      - virusi, črvi, Trojanski konji, vohljači, ribarjenje
    - računalnik lahko napade iz drugega računalnika
      - odpoved storitve, DOS (ang. denial of service)
      - neželena elektronska pošta
- Pogostost napadov
  - Računalnik - priključen v Internet
    ocenjujejo, da je napaden vsakih 20 minut

Varnost: oblike napadov (1)

- **Virus**
  - integrira se v programe, ki so že na računalniku
  - pri izvajanju programa gostitelja se izvede tudi virus
  - namen izvajanja virusa je,
    - da se razširi še na druge programe v računalniku
    - zmanjša zmogljivosti računalnika
    - onemogoči izvajanje programov, pobriše podatke, …
- **Črv**
  - avtonomen program, ki se zna sam razpošiljati po omrežju
  - namen črva je lahko
    - samo razpošiljanje in s tem obremenjevanje omrežja
    - tudi bolj zlonamerne operacije



Varnost: oblike napadov (2)



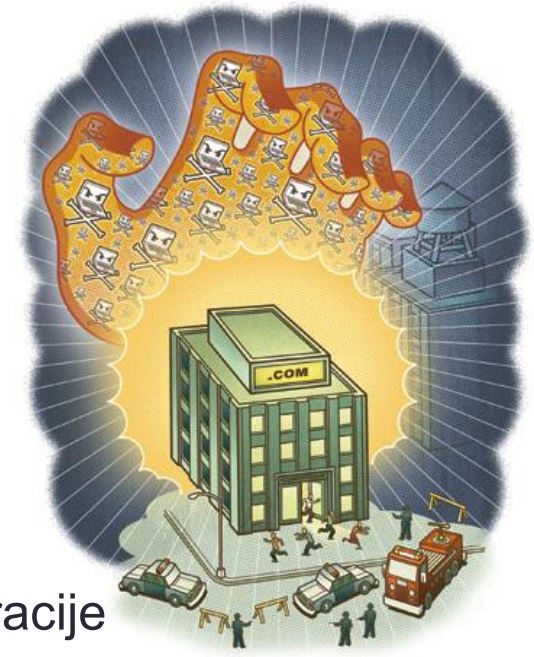
- **Trojanski konj**
  - v računalnik ga namestimo sami kot sestavni del želenega programa (igra, orodje)
  - poleg osnovnih opravlja še dodatne funkcije, ki imajo lahko boleče posledice
  - izvajati se lahko začnejo takoj ali pa šele na točno določen dogodek (izbrani datum, …)
  - pogosto so sestavni del priponk v elektronskih sporočilih → **ne odpirajte priponk iz neznanih virov (exe, com, tudi doc, xls)**
- **Vohljač**
  - zbira podatke o aktivnostih, ki se izvajajo na računalniku
  - podatke pošilja pobudniku napada
  - kraja uporabniških imen, gesel, številk kreditnih kartic, …

Varnost: oblike napadov (3)

- **Tehnika ribarjenja**
  - podatke pridobivajo tako, da jih zahtevajo
  - uporabnika zavedejo s podobno vsebino in upajo, da bo prijel za vabo
  - vabe se pošiljajo:
    - po elektronski pošti,
    - v sporočilu povezava na stran s podobnim izgledom in podobno vsebino
  - ang. fishing in phishing
  - primer: bančne prevare
    - “banka” zahteva:
      - naložite certifikat in
      - vtipkate geslo!!!

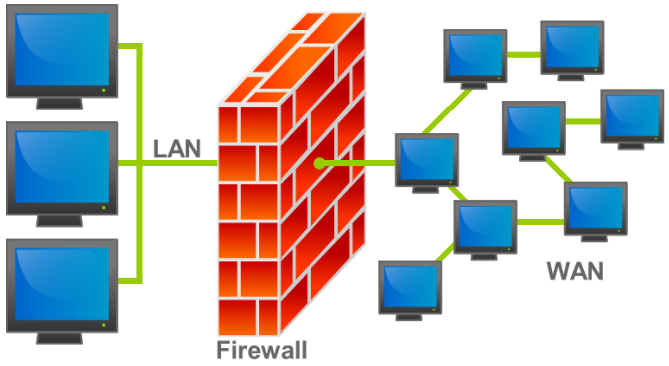
Varnost: oblike napadov (4)

- Odpoved storitve – DOS
  - ang. Denial Of Sevice
  - napadalec računalnik preobremeni
    - veliko število zahtev v kratkem času
    - Najprej okuži veliko računalnikov z ostalimi oblikami (črv, Trojanski konj)
    - Ob določenem dogodku vsi okuženi računalniki zahtevajo servisiranje s strani napadenega strežnika
  - pogosto so napadene velike računalniške korporacije
- Neželena elektronska pošta
  - ang. junk mail, spam
  - zloraba elektronskih sistemov za razpošiljanje pošte
  - neuporabna za bralca elektronskih sporočil
  - pogosto izhodišče za ostale oblike napadov



Varnost: zaščita in zdravljenje (1)

- Preventiva je najboljša kurativa!
- Nadzor prometa v omrežju
  - **požarni zid** (ang. firewall) na domenskem prehodu
    - blokiranje odhodnih sporočil z določenimi ciljnimi naslovi
      - uporabnikom onemogočimo dostop do strani s potencialno nevarno vsebino
    - blokiranje dohodnih sporočil iz določenih naslovov
      - obstajajo seznami nevarnih strežnikov,
      - sporočila, ki jih pošiljajo nevarni strežniki zavrne
    - blokirajo vsa dohodna sporočila, pri katerih je naslov pošiljatelja enak enemu od naslovov v notranjem omrežju
      - v tem primeru se napadalec pretvarja, da je običajni uporabnik (ang. spoofing)
  - **požarni zid** na računalniku
    - program, ki blokira sporočila, ki jih ne potrebujejo nobeden od programov
    - če so zaprte vse “luknje”, napad ni mogoč,
    - primer: če na računalniku nimamo nameščenega spletnega strežnika lahko vsa sporočila na vratih 80 zavrne



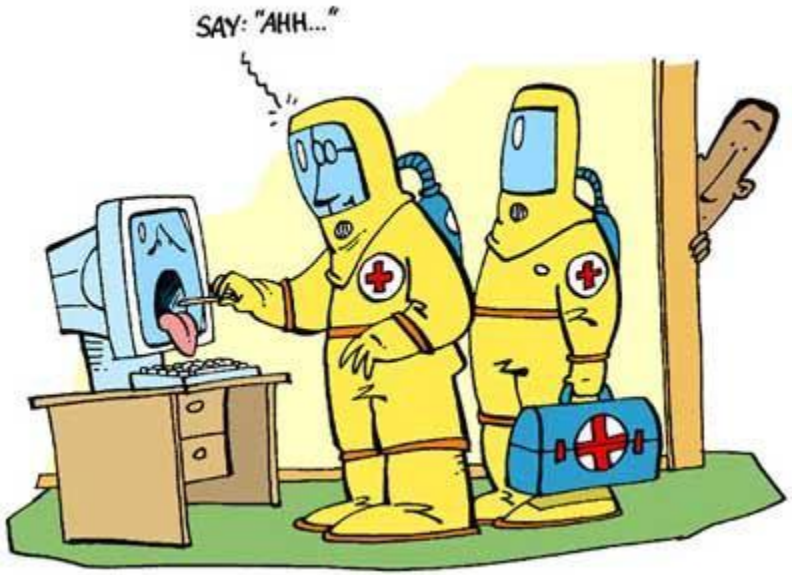
Varnost: zaščita in zdravljenje (2)

- **Filtri za neželeno pošto**
  - nameščeni na strežniku ali na odjemalcu
  - uporabljajo zapletene postopke za ločevanje želenih in neželenih sporočil
    - iskanje značilnih nizov znakov,
    - verjetnostna teorija,
    - umetna inteligenca

- **Strežnik proxy**
  - varuje odjemalce pred zlonamernimi posegi strežnika
  - zlonamerni strežnik lahko analizira akcije odjemalcev in se tako seznani s strukturo omrežja, nato pripravi napad
  - med odjemalce in strežnik postavimo strežnik proxy
    - odjemalec komunicira s strežnikom proxy
    - strežnik proxy se do pravega strežnika obnaša kot odjemalec
    - pravi strežnik vedno vidi enega samega odjemalca

Varnost: zaščita in zdravljenje (3)

- Orodja za nadzor omrežja
  - specialna programska orodja, ki spremljajo aktivnost v omrežju
  - alarmiranje v primeru močno povečane aktivnost
  - poročanje o dogajanju na požarnih zidovih
- **Protivirusni programi**
  - namenjeni so zaznavanju in odstranjevanju najrazličnejših oblik napadov
  - podatkovne baze s podpisi virusov, črvov, Trojanskih konjev
  - nujno vzdrževanje podatkovnih baz s stalnim posodabljanjem
  - primeri:
    - AVG, NOD, Norton Antivirus, …



Varnost: zaščita in zdravljenje (4)

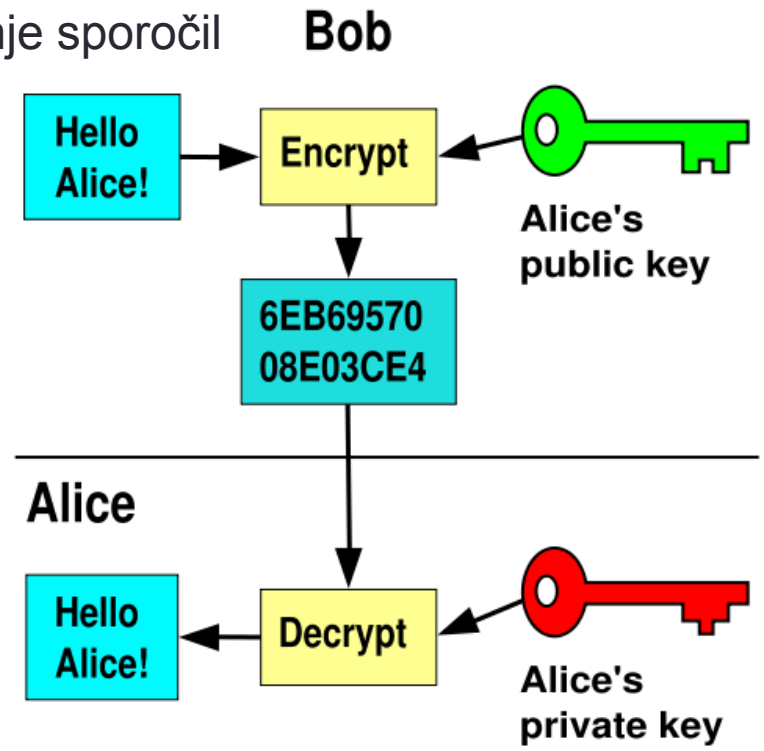
- Osnovni napotki
  - ne odpiramo priponk v elektronskih sporočilih nepoznanih pošiljateljev
  - z Interneta ne nalagamo programov katerih izvora ne poznamo,
  - ne odzivamo se na sporočila pop-up
  - računalnik po uporabi izklopimo iz Interneta

Varnost: šifriranje sporočil (1)

- Cilj napadalcev je velikokrat dostop do podatkov na našem računalniku in okoriščanje z njimi
- Običajna zaščita:
  - uporabniško ime in geslo
  - z vohljanjem napadalec enostavno pride do obeh
  - potrebna je zaščita → šifriranje
- Internetne aplikacije
  - HTTP → HTTPS
  - FTP → SFTP
  - Telnet → SSH

Varnost: šifriranje sporočil (2)

- Zaščita sporočil z javnim ključem
  - Čeprav vemo kako je sporočilo šifrirano, ga ne moremo odšifrirati.
  - Sistem je zasnovan na dveh številčnih vrednostih (ključih)
    - javni ključ je namenjen šifriranju sporočil
    - zasebni ključ je namenjen za odšifriranje sporočil
  - Postopek
    - javni ključ razpošljemo vsem, ki želijo poslati sporočilo na ciljni sistem
    - pošiljatelj sporočilo šifrira z javnim ključem
    - morebitni napadalec ga ne more odšifrirati kljub temu, da pozna javni ključ
    - edini, ki sporočilo lahko odšifrira je ciljni sistem, ker ima zasebni ključ.

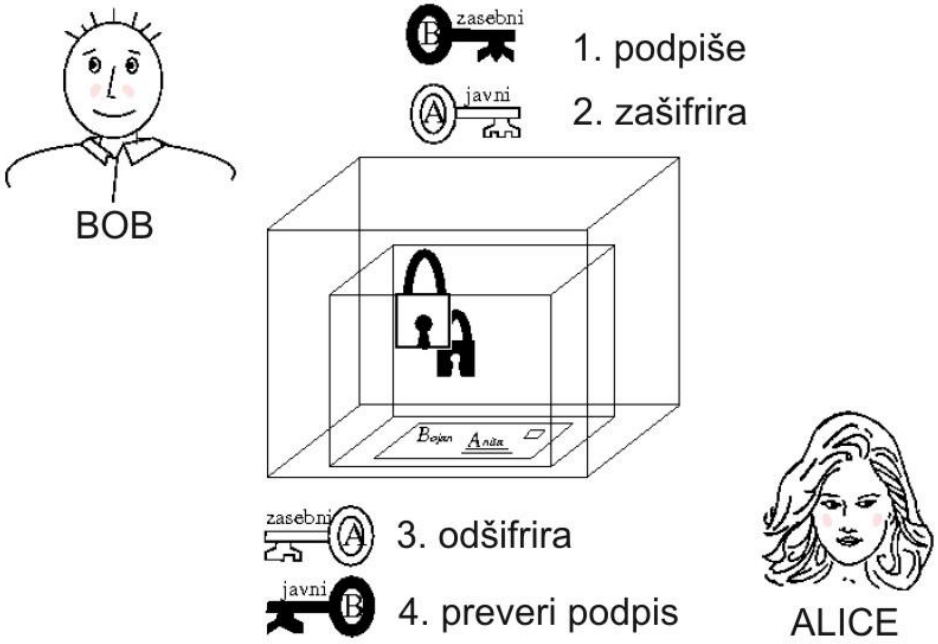


Varnost: šifriranje sporočil (3)

- Kako zagotoviti, da imamo pravi javni in zasebni ključ?
  certifikatni uradi
  - vzdržujejo liste certifikatov
  - certifikat je datoteka, ki vključuje ime stranke in njen javni ključ
  - organizacije zaradi večjega nadzora večinoma same izdajajo certifikate
- Kako zagotoviti, da je pošiljatelj res pravi?
  avtentikacija sporočil
  - digitalni podpis
  - pošiljatelj sporočilo šifrira z zasebnim ključem
  - sprejemnik ga odšifrira z javnim ključem
  - odšifriranje je uspešno samo v primeru, ko javni ključ ustreza zasebnemu ključu

Varnost: šifriranje sporočil (4)

- Primer: Bob pošlje Alice podpisano zasebno pismo
  1. **podpiše** ga s svojim zasebnim ključem
  2. **zašifrira** ga z javnim ključem
  3. Alice ga **odšifrira** s svojim zasebnim ključem
  4. z Bobovim javnim ključem **preveri podpis**



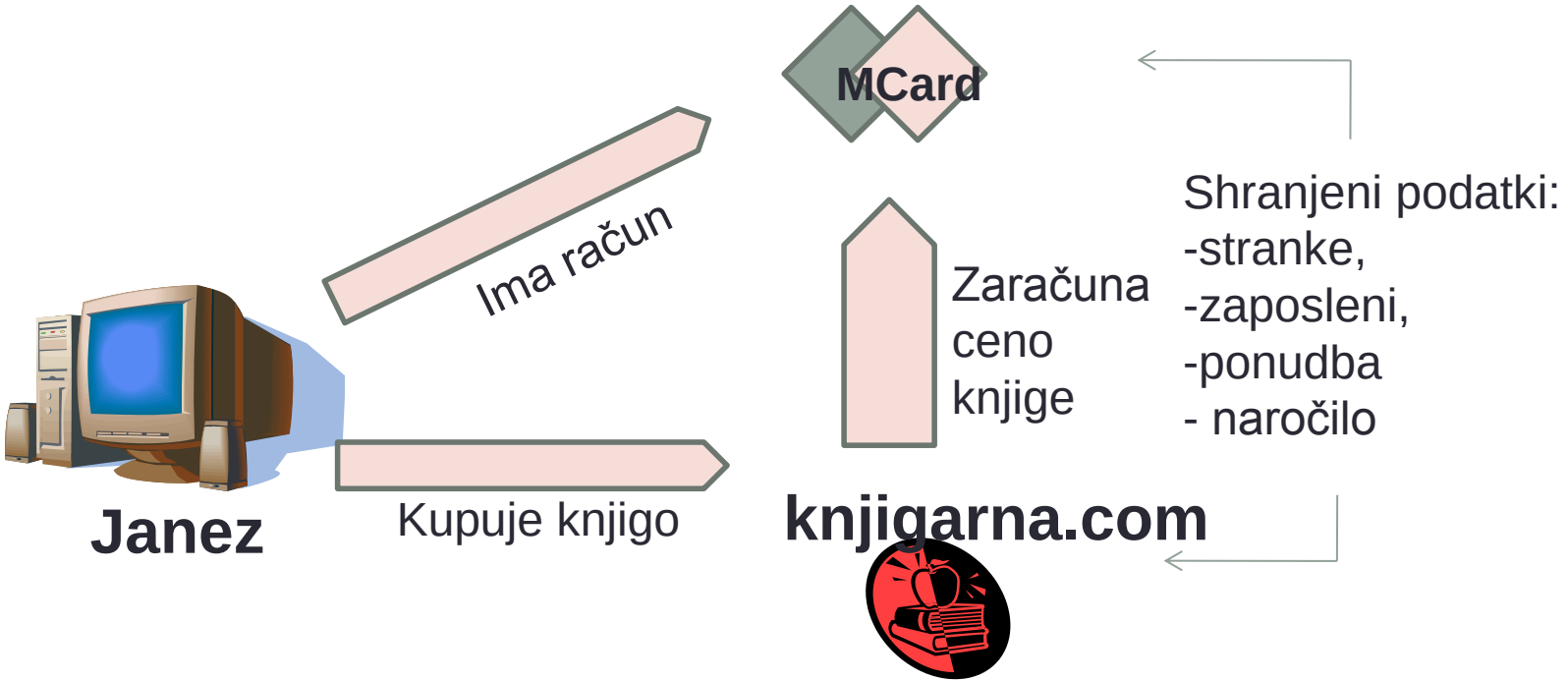
Varnost: šifriranje sporočil (5)

- Najbolj priljubljeni sistemi šifriranja z javnimi in zasebnimi ključi temeljijo na algoritmu RSA (avtorji River, Shamir, Adleman, MIT)

  Asimetrični algoritem šifriranja/dešifriranja, razvit na MIT
- PGP Corporation (ang. Pretty Good Privacy)
  - izdelava programskih modulov, ki uporabljajo RSA algoritme
  - kompatibilni so z večino programov za elektronsko pošto
  - zastonj za osebno in neprofitno rabo
  - Uporabnik lahko sam pripravi svoj zasebni in javni ključ
  - http://www.pgp.com

Varnost – Primer (1)

- Janez kupuje knjigo v spletni trgovini.
- Plačilo se izvede z uporabo plačilne kartice.



Varnost – Primer (2)

- Uporabljeni so različni ključi (par ključev):
  - Privatni ključ in javni ključ, ki je splošno dostopen
  - Janez uporabi za šifriranje sporočila m javni ključ E
  - Knjigarna uporabi javni in privatni ključ za dešifriranje (E,D)