# Telekomunikacijska omrežja

Zapiski predavanj – 2013/14

Anton Umek
anton.umek@fe.uni-lj.si

## 1. UVOD V TELEKOMUNIKACIJE

- Električne komunikacije, signali in informacija
- Delitev elektromagnetnega spektra
- Glavni mejniki v razvoju telekomunikacij
  - Telegraf in telefon
  - Radio in televizija
  - Satelitske komunikacije
  - Mobilni celična omrežja
  - Paketna omrežja in Internet

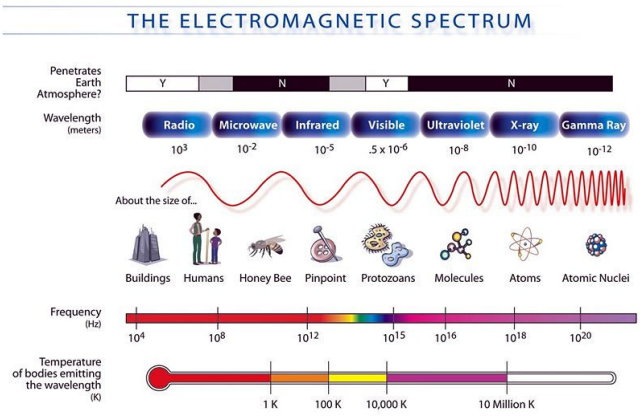
## Električne komunikacije

- Komunikacija med napravami poteka s pomočjo električnih signalov. Glede na vrsto prenosnega medija ločimo vrvične in brezvrvične komunikacije.
  - Vrvične komunikacije zahtevajo instalacijo prenosnega medija. Medij je lahko električni žični kabel ali pa optično vlakno. Elektromagnetno valovanje razširja usmerjeno v omejenem prostoru. Zaradi fizične povezave terminali niso mobilni.
  - Brezvrvične komunikacije lahko potekajo po zraku ali v praznem prostoru, pri zelo nizkih frekvencah pa tudi v vodi. Prenosni medij je omejen zato predstavlja dragocen naravni vir. Zaradi skupnega prenosnega medija lahko prihaja do motenj med različnimi uporabniki.



## Delitev elektromagnetnega spektra

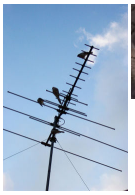
- Elektromagnetno valovanje se prosto razširja v zraku ali v praznem prostoru. Komunikacijo v frekvenčnem prostoru do 300Ghz imenujemo tudi radijska komunikacija.



## Radijski frekvenčni prostor

- Območje radijskih frekvenc je razdeljeno na območja nizkih, srednjih in visokih frekvenc s predponami (Very, Ultra, Super, Extremely):
  - ELF (3Hz-30Hz), SLF(30Hz-300Hz), ULF(300Hz-3kHz),VLF(3-30kHz)
  - LF (30kHz-300kHz), MF (300kHz-3MHz), HF(3MHz-30MHz), VHF(30MHz-300MHz),
  - UHF (300MHz-3GHz), SHF(3-30GHz), EHF(30-300GHz)
- Zadnjo skupino (300MHz-300GHz) imenujemo tudi mikrovalovi.
- Dimenzije oddajnih anten so primerljive z valovno dolžino !!

VLF

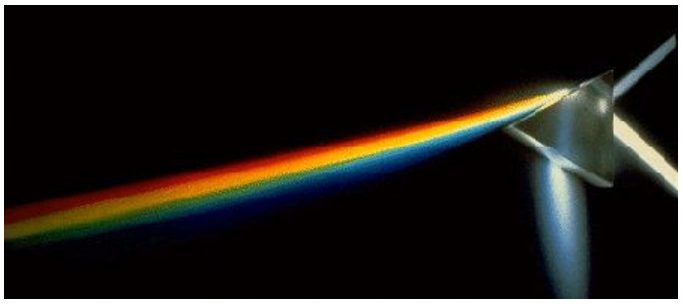


UHF



## Svetlobni spekter

- Pri frekvencah nad 300Ghz običajno navajamo podatek o valovni dolžini.
- Za človeško oko vidni del svetlobnega **spektra** je v območju od 400 do 700nm.
- Svelobna komunikacija po optičnih vlaknih poteka v nevidnem delu spektra v območjih med 1200nm in 1700nm.
- Območje X žarkov je od 10nm do 10pm, območje gama žarkov pa določajo valovne dolžine od 10pm do 1pm.



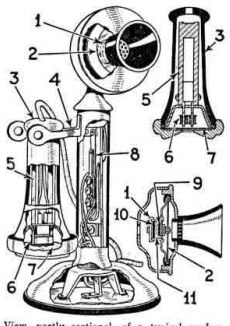
## Prve znakovne komunikacije in telegraf

- Znakovne komunikacije so se že uporabljale pred iznajdbo prvih električnih naprav (bobni, dimni signali, kresovi, ogledala…)
- V 18. stoletju so uporabljali teleskopske relejne sisteme svetlobnih semaforjev na stolpih, največ po Franciji.
- 1839: telegraf (Cooke, Wheatstone , Morse)
- Po ameriški državljanski vojni je leta 1866 položen prvi telegrafski kabel med Evropo in Ameriko.



## Telefon

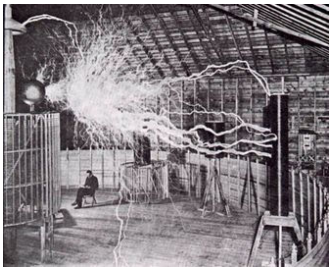
- 1876, A.G. Bell , Elisha Gray

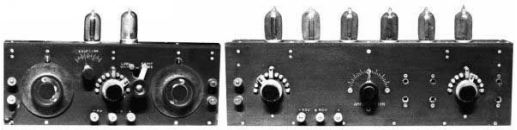



View, partly sectional, of a typical modern Telephone, with cross-sectional views of Transmitter and Receiver. 1, 1 Transmitter Button (containing 9, 10, and 11); 2, 2 Transmitter Diaphragm; 3, 3 Receiver; 4 Receiver Hook; 5, 5 Permanent Magnet; 6, 6 Receiver Coil; 7, 7 Receiver Diaphragm; 8 Contact Springs which close the circuit when the receiver is lifted from the hook; 9 Front Carbon Electrode; 10 Rear Carbon Electrode; 11 Carbon Granules.

## Začetek radijskih komunikacij

- 1888, Heinrich Hertz eksperimentalno potrdi obstoj elektromagnetnih valov,
- 1897, Nikola Tesla: US patent za radijski prenos informacije,
- 1901, Guglielmo Marconi: radijski prenos informacije čez Atlantik, Nobelova nagrada.
- 1906, Fessenden: prvo oddajanje govora in glasbe
- 1920: prvo oddajanje radijskih novic







## Televizija

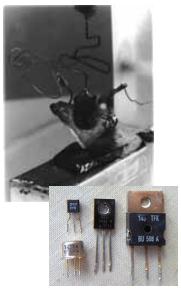
- 1926, John Baird, prenos gibljive slike, mehanski TV!
- 1929: prva oddajanja TV signala v ZDA in v Evropi
- 1951, CBS: prvi komercialni TV program v barvah
- TV aparati :

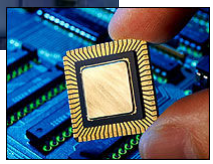


1938 DuMont Model 180
America's First Commercial Electronic TV Set

## Razvoj elektronike

- Leta 1947 je bil v Bell Labs izdelan prvi transistor,
- leta 1961 je patentirano prvo integrirano vezje (IC)
- število transistorjev v pomnilnikih narašča eksponentno:
  - 1970>100
  - 1989>1.000.000
  - 2005>1.000.000.000
  - 2007>10.000.000.000

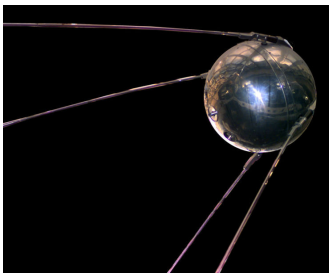


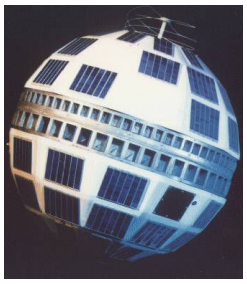




## Satelitske komunikacije

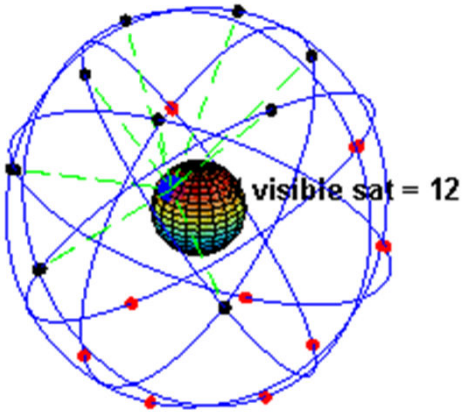
- Doba vesoljskih komunikacij se začne leta 1957 z izstrelitvijo Sputnika.
- Leta 1961 AT&T lansira prvi telekomunikacijski satelit Telstar za telefonijo in TV.





## Sistem satelitske navigacije

- navigacija GPS





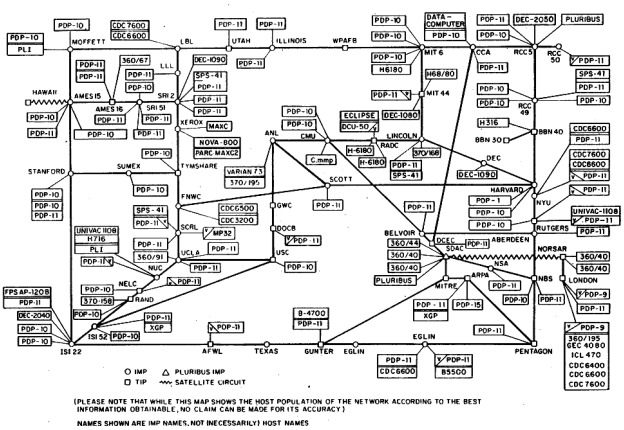

## Mobilna celična omrežja

- Leta 1981 začne delovati prva generacija mobilne telefonije v Skandinaviji NMT (Nordic Mobile Telecommunication).
- Deset let kasneje začne delovati prvo GSM omrežje.
- Leta 2001 začne delovati prvo UMTS omrežje, in leta 2003 tudi v Sloveniji.
- 2010 se začenjajo postavljati prva omrežja LTE,
- razvija pa se že četrto generacijo (4G) mobilnih sistemov LTE-Advanced

# Začetki Interneta

- 1961 je L. Cleinrock iz ameriške univerze MIT predstavil koncept paketnega omrežja.
- V letu 1969 je začela raziskovalna agencija ARPA (Advanced Research Project Agency) razvoj paketnega omrežja in leta 1972 je kot rezultat teh raziskav začelo delovati geografsko porazdeljeno omrežje ARPANET.

ARPANET LOGICAL MAP, MARCH 1977




(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES



# Začetki Interneta

- Zaradi nepovezljivosti različnih fizičnih omrežij se je v letu 1973 začel razvoj TCP/IP protokolnega sklada, ki naj bo neodvisen od fizičnega medija. IP verzija 4 je bila končana 1978, ARPANET pa je na IP protokol prešel leta 1982.
- ARPANET je bil v začetku vojaško omrežje, zaradi obsežnega sodelovanja ameriške vojske z univerzami pa se je razširilo najprej na ameriške in nato tudi druge univerze.
- K popularizaciji in komercializaciji interneta je v največji meri pripomogel razvoj jezika HTML in protokola HTTP, ki ju je razvil T. B. Lee na švicarskem inštitutu za fiziko CERN.

## Primeri internetnih aplikacij

| | |
|---|---|
| **Elektronska pošta** | Program, ki omogoča pošiljanje, sprejemanje in urejanje elektronske pošte. Uporablja protokole SMTP, IMAP, POP3,... |
| **Spletni brskalnik** | Poleg brskanja po spletnih straneh omogočajo brskalniki še prenos datotek (download in upload). Uporablja protokole HTTP, FTP, HTML, ... |
| **MIRC** | Program za "on-line" pogovor po internetu. Omogoča pisni pogovor dveh ali več udeležencev, ki so prijavljeni na isti strežnik. |
| **Dostop do podatkovnih zbirk** | Večino podatkovnih aplikacij omogoča tudi dostop do oddaljenih podatkovnih strežnikov. Večinoma so to strežniki zasnovani na SQL jeziku. |
| Gopher | Program, ki se je pred pojavom HTTP protokola največ uporabljal za iskanje podatkov po internetu. |



## Rast števila uporabnikov svetovnega spleta

| leto | brskljalnik | število uporabnikov |
|---|---|---|
| 1993 | Mosaic | |
| 1995 | IE, NN2.0 | 16m |
| 1996 | IE3,NN3.0 | 36m |
| 1997 | IE4,NN4.0 | 70m |
| 1998 | IE5, | 147m |
| 2002 | NN7 | 587m |
| 2005 | IE7, FF2.0 | 1,1M |
| 2007 | | 1,25M |
| 2010 | IE8 ,FF4.0 | 2M |
| 2013 | Crome, IE, FF, Safari .. | 2.4M (34% prebivalstva) |

- strmo narašča uporaba mobilnih naprav: pametni telefoni in tablice

## Kratka zgodovina storitev na spletu

- 1994 spletna trgovina **Amazon**
- 1998 je ustanovljen **Google**
- 1998 začne delovati **eBay**,
  - 2002 postane lastnik PayPal-a (1.5M$)
  - 2006 je dodana še spletna trgovina ebay express
- 2003 Skype, septembra 2005 postane lastnik eBay (2.6M$)
- 2003 MySpace, 2004 **Facebook**, danes 500M uporabnikov!
- 2005 YouTube, naslednje leto (2006) postane lastnik Google (1,65M$)

Ostajajo največji v 2013: Amazon, Google, .. E-bay, ..Facebook..



## 2. OSNOVE SIGNALOV

- Signali kot nosilci informacije
- Vrste signalov v fiziki, akustični in električni signali
  - Periodični signali, harmonični akustični signali
  - Aperiodični signali, impulzi v znakovnih komunikacijah
  - Naključni signali, šum v akustiki in v telekomunikacijah
- Matematični opis signalov
  - časovni potek signala
  - moč signala, logaritemska mera [dB]
  - frekvenčni spekter signala
  - zgledi
- Filtriranje električnih signalov na zgledih:
  - grafični audio izravnalnik
  - popačitve pri prenosu telekomunikacijskih signalov

## Signali in informacija

- **Signali** so nosilci informacije v komunikaciji.
- Oblike signalov določajo informacijsko vsebino.

- V **analogni** komunikaciji je izvorni signal zvok ali pa vzorčena slika. Človek prepozna informacijsko vsebino signalov, ki jih je sprejel preko čutnih organov (sluh, vid). Pri človeškem zaznavanju ni vsa informacija enako pomembna (relevantna). Človeško zaznavanje je zelo kompleksno in subjektivno. Pri prenosu analognih signalov so lahko tudi majhne popačitve opazne. Primer je audio-HiFi.



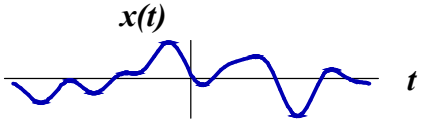
## Signali in informacija

- **Signali** so nosilci informacije v komunikaciji.
- Oblike signalov določajo informacijsko vsebino.

- V znakovni (**digitalni**) komunikaciji je informacijska vsebina signalov popolnoma merljiva. Znakovni signali so lahko pridobljeni direktno iz digitalnih izvorov, ali pa so pridobljeni s kodiranjem analognih izvorov. Primer direktne znakovne komunikacije med človekom in strojem je tipkanje po tastaturi. Znakovne komunikacije lahko potekajo praktično brez napak in s tem brez izgube informacije.

## Kaj so signali?

- Signali so s časom se spreminjajoče fizikalne veličine, kot je to zračni pritisk, električna napetost, električni tok, električno polje magnetno polje in podobno.
- Signale predstavimo kot funkcije časa:
  - $p(t)$ - *pritisk*
  - $u(t)$ - napetost
  - $i(t)$ - tok
  - $x(t)$, $y(t)$ - splošni signali (kadar ni pomembno katero fizikalno veličino predstavljajo)
- Signale lahko predstavimo tudi grafično:






## Vrste signalov

- Periodični signali
  - Periodični so signali, pri katerih se začne oblika signala po določenem času ponavljati:

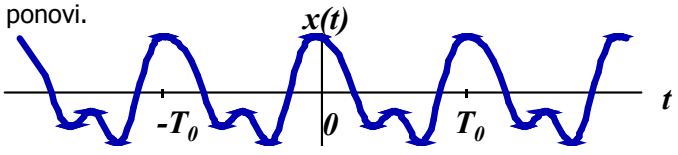
$$x(t) = x(t + T_0)$$

$T_0$ - perioda signala

  - Inverzno vrednost periode signala imenujemo osnovna frekvenca:

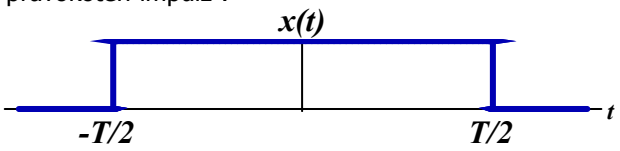
$$f_0 = \frac{1}{T_0}$$

  - Osnovna frekvenca pove, kolikokrat na sekundo se signal ponovi.

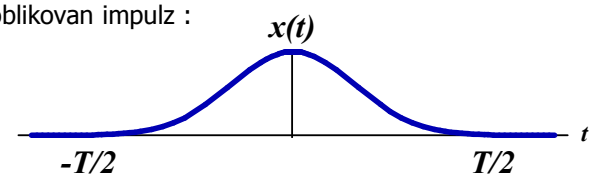


## Vrste signalov

- Aperiodični signali
  - Aperiodični signali se ne ponavljajo.
  - Večinoma so to časovno omejeni signali.
  - Časovno omejene signale imenujemo tudi impulzi.
  - pravokoten impulz :



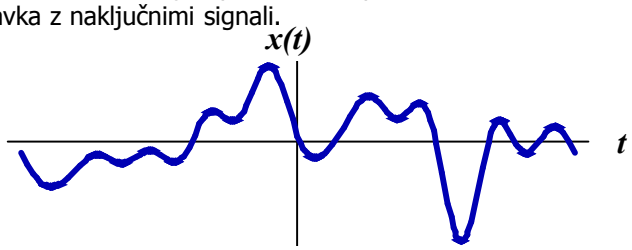

  - oblikovan impulz :






## Vrste signalov

- Naključni signali
  - Naključni signali so signali, pri katerih ne poznamo vnaprej njihove oblike
  - Glede na izvor signala ali glede na opazovanje podobnih signalov lahko sklepamo na določene lastnosti. Poznamo lahko torej statistiko signala.
  - Ko v telekomunikacijah prenašamo sporočila imamo vedno opravka z naključnimi signali.



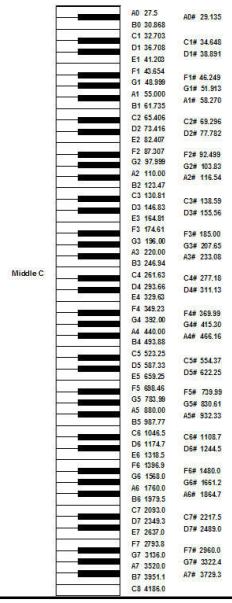
## Periodični signali

- Osnovna lastnost periodičnih signalov je njihova osnovna frekvenca $f_o$.
- Elektromagnetni signali
  - Frekvence so do 300 GHz (300.000.000.000 Hz).
- Optični signali
  - Frekvence so med $10^{14}$ in $10^{15}$ Hz (1.000.000.000.000.000 Hz).
  - Od frekvence je odvisna barva svetlobe.
  - Barve, ki jih vidimo, so običajno iz več frekvenc.
- Akustični signali
  - Frekvence so med 20 Hz in 20 kHz (20.000 HZ).
  - Te frekvence sliši človeško uho.
  - Od frekvence je odvisna višina zvoka.
  - Glasnost je odvisna od moči signala.



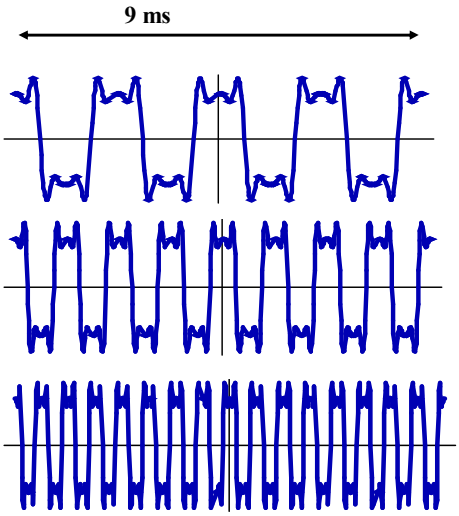
## Primer: nihanje strune

- lastna **frekvenca** strune je odvisna od dolžine in od debeline strune
- dvakrat daljša struna niha na dvakrat nižji frekvenci, ali eno oktavo nižje
- premik za osem tonov višje (oktava) pomeni na klaviaturi podvojitev frekvence:



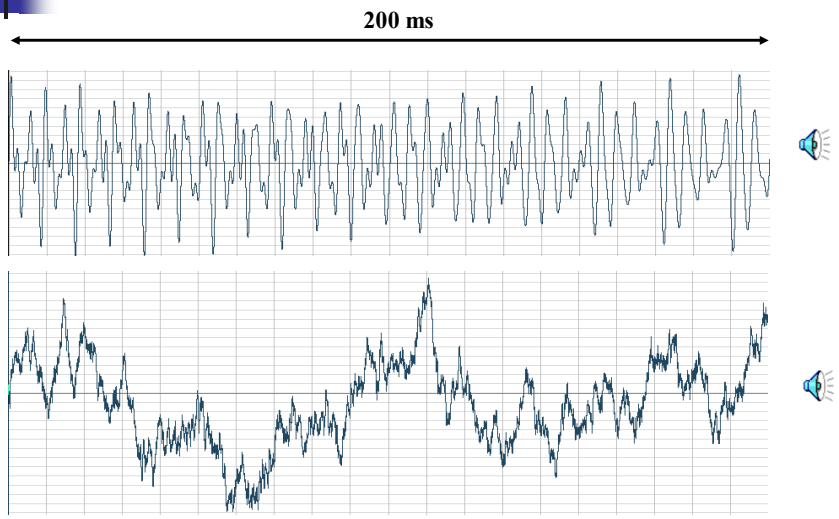
## Primeri akustičnih signalov

- Ton A - 440Hz
- Ton A’ - 880 Hz
- Ton A” 1760 Hz






## Drugi zvoki



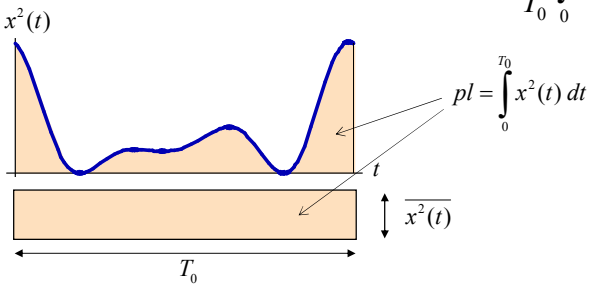
## Moč signala

- Pri vseh fizikalnih signalih moč narašča s kvadratom amplitude. Zato definiramo trenutno moč kar kot:

$$p(t) = x^2(t)$$

- Povprečna moč:

$$P = \overline{p(t)} = \overline{x^2(t)} = \frac{1}{T_0}\int_0^{T_0} x^2(t)\,dt$$






## Logaritemska mera moči

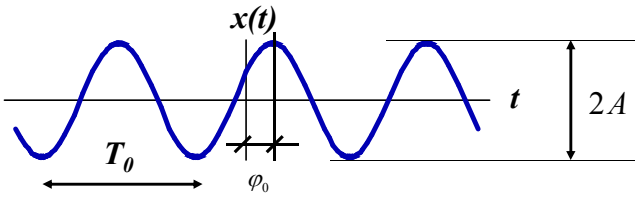
- Na različnih področjih tehnike (akustika, telekomunikacije,..) izražamo moč relativno glede na referenčni nivo P0.
  - referenčna moč v akustiki $P_0$= 1pW
  - referenčna moč v telefoniji $P_0$= 1mW
- decibel [dB] je logaritemska mera razmerij moči:

$$L_P = 10 \cdot \log\left(\frac{P}{P_0}\right)$$

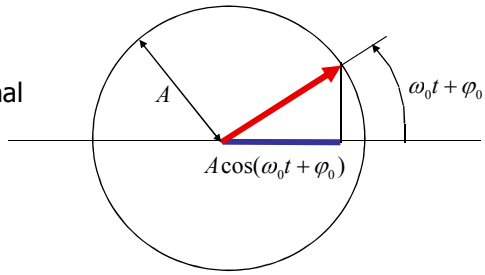
- primer izražave razmerij moči v decibelih
  - akustična moč P=1W, L=120dB
  - električna moč P=1W, L=30dB

## Harmonični signali

- Grafični prikaz harmoničnega signala




- Harmonični signal in kroženje






## Harmonični signali

- Harmonični so signali, ki jih lahko zapišemo v obliki:

$$x(t) = A\cos(\omega_0 t + \varphi_0)$$

| | |
|---|---|
| $A$ | amplituda signala |
| $\omega_0 = 2\pi f_0$ | frekvenca signala |
| $\varphi_0$ | fazni zasuk |

- Sinusna in kosinusna funkcija se razlikujeta samo po faznem zasuku:

$$A \cdot \cos(\omega_0 t - \pi/2) = A\sin(\omega_0 t)$$

zadošča torej, da imamo samo kosinuse z različnimi faznimi zasuki.

## Vsota dveh harmoničnih signalov

$$x_1(t) = A_1 \cdot \cos(\omega \cdot t + \phi_1)$$

$$x_2(t) = A_2 \cdot \cos(\omega \cdot t + \phi_2)$$

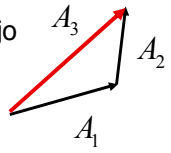
$$\omega = 2 \cdot \pi \cdot f$$

$$x_3(t) = x_1(t) + x_2(t)$$

- Vsota dveh harmoničnih signalov enakih frekvenc *f* je harmonični signal z isto frekvenco *f*.

$$x_3(t) = A_3 \cdot \cos(\omega \cdot t + \phi_3)$$

- Vsoto najlažje ponazorimo s kazalci, ki vsebujejo informacije o amplitudah in fazah signalov:






## Produkt dveh harmoničnih signalov

$$x_1(t) = A_1 \cdot \cos(\omega_1 \cdot t)$$

$$x_2(t) = A_2 \cdot \cos(\omega_2 \cdot t)$$

$$\omega_1 = 2 \cdot \pi \cdot f_1$$
$$\omega_2 = 2 \cdot \pi \cdot f_2$$

$$x_3(t) = x_1(t) \cdot x_2(t)$$

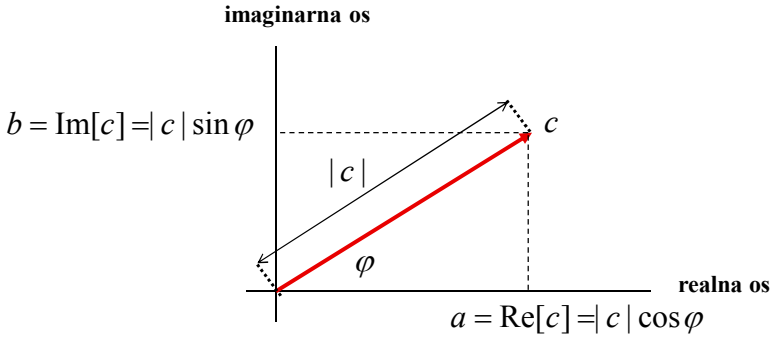
- Signal produkta vsebuje dve frekvenci - vsoto in razliko:

$$x_4(t) = \frac{1}{2} A_1 \cdot A_2 \left(\cos(\omega_1 + \omega_2)t + \cos(\omega_1 - \omega_2)t\right)$$

- Primer: množimo signala s frekvencami 1000Hz in 1200Hz.
  - Rezultat množenja sta frekvenci 2200Hz in 200Hz !

## Kompleksna ravnina

- Kompleksna števila predstavljajo vektor (kazalec) v kompleksni ravnini





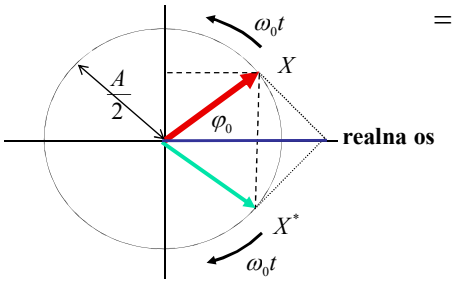

## Kompleksen zapis harmoničnega signala

- Harmonični signal lahko sedaj zapišemo kot:

$$A\cos(\omega_0 t + \varphi_0) = \frac{A}{2} e^{j(\omega_0 t + \varphi_0)} + \frac{A}{2} e^{-j(\omega_0 t + \varphi_0)} =$$

$$= \frac{A}{2} e^{j\varphi_0} e^{j\omega_0 t} + \frac{A}{2} e^{-j\varphi_0} e^{-j\omega_0 t} =$$

$$= X e^{j\omega_0 t} + X^* e^{-j\omega_0 t}$$



## Spekter periodičnega signala

- Vsak periodičen signal lahko sestavimo kot vsoto harmoničnih signalov.

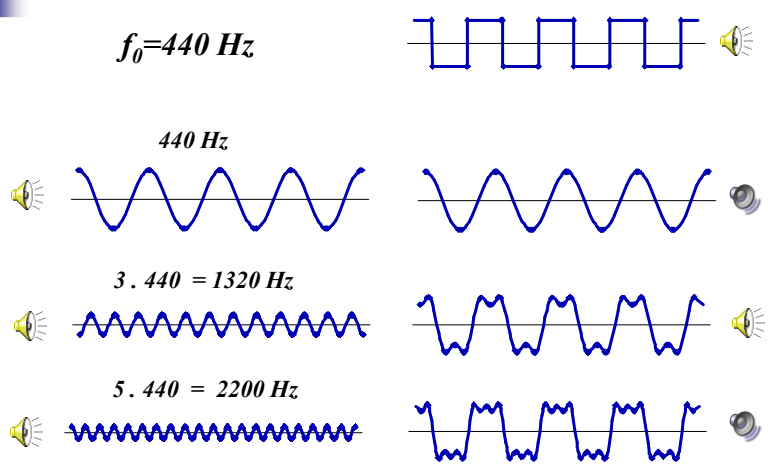
$$x(t) = A_0 + A_1\cos(\omega_0 t + \varphi_1) + A_2\cos(2\omega_0 t + \varphi_2) + A_3\cos(3\omega_0 t + \varphi_3) + \ldots =$$
$$= X_0 + X_1 e^{j\omega_0 t} + X_1^* e^{-j\omega_0 t} + X_2 e^{2j\omega_0 t} + X_2^* e^{-2j\omega_0 t} + \ldots$$

- Frekvence posameznih harmoničnih signalov so mnogokratniki osnovne frekvence.
- Signale pri mnogokratnikih osnovne frekvence imenujemo višje harmonske komponente.
- Koeficiente $A_k$ *imenujemo amplitudni spekter signala.*
- *Koeficiente* $\varphi_k$ *imenujemo fazni spekter signala.*
- *Koeficiente* $X_k$ *imenujemo kompleksni spekter signala*

$$X_k = \frac{A_k}{2} e^{j\varphi_k}$$

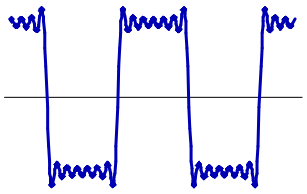


## Spekter pravokotnega signala

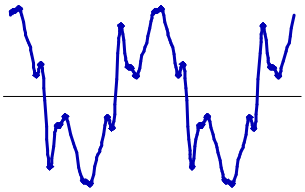


## Fazni zamik komponent

Pravokotni signal sestavljen iz sedmih sodih harmonskih komponent



Tretja harmonska komponenta je fazno zamaknjena za kot $\pi/2$





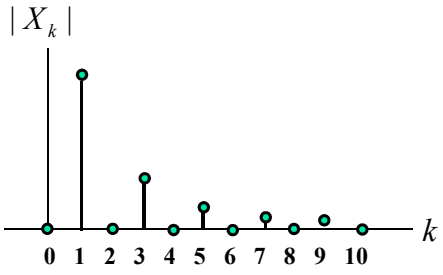
## Izračun spektra periodičnega signala

- Koeficiente $X_k$ lahko izračunamo po enačbi:

$$X_k = \frac{1}{T}\int_{-T/2}^{T/2} x(t)e^{-jk\omega_0 t}dt$$

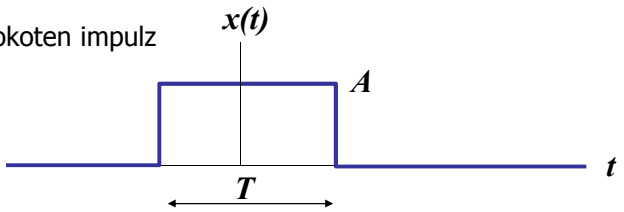
- Za pravokotni signal v prejšnjem primeru dobimo:

$$X_0 = 0$$
$$X_1 = 1{,}27$$
$$X_2 = 0$$
$$X_3 = -0{,}42$$
$$X_4 = 0$$
$$X_5 = 0{,}25$$



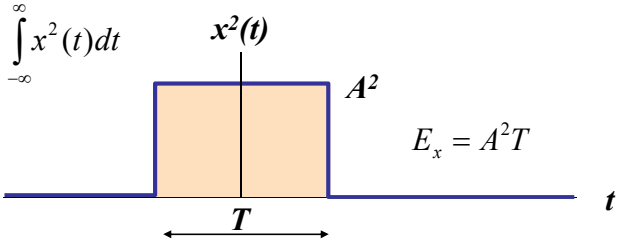
## Aperiodični signali

- Pravokoten impulz




- Aperiodični signali imajo definirano energijo:

$$E_x = \int_{-\infty}^{\infty} x^2(t)\,dt$$




$$E_x = A^2 T$$



## Izračun spektra

- Periodičen signal

$$TX_k = \int_{-T/2}^{T/2} x(t) e^{-jk\omega_0 t}\,dt$$

- Aperiodičen signal

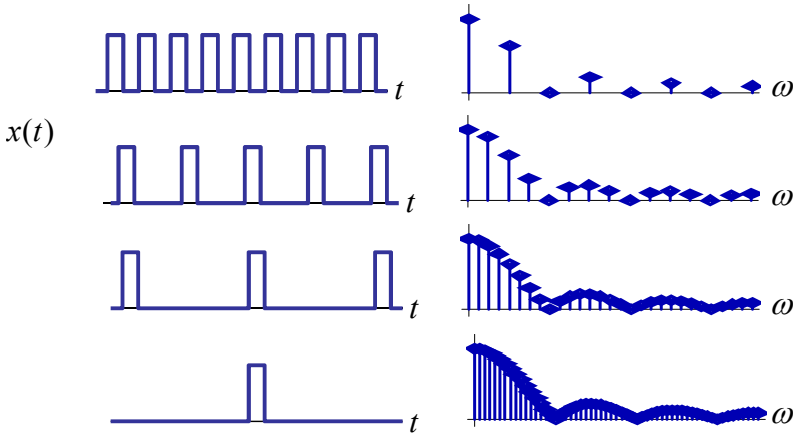
$$T \to \infty \qquad \omega_0 = \frac{2\pi}{T} \to 0 \qquad k\omega_0 \to \omega$$

**Fourierov transform:**

$$X(\omega) = \int_{-\infty}^{\infty} x(t) e^{-j\omega t}\,dt$$

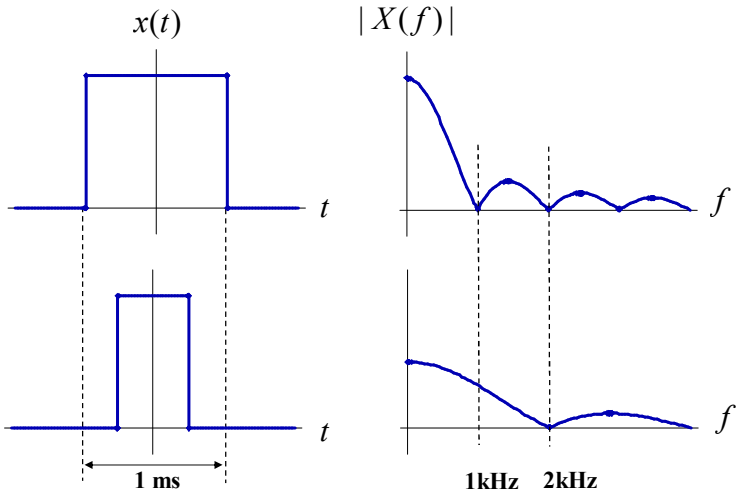
## Spekter aperiodičnih signalov

**Aperiodičen signal lahko nastane iz periodičnega, tako da večamo periodo signala:**



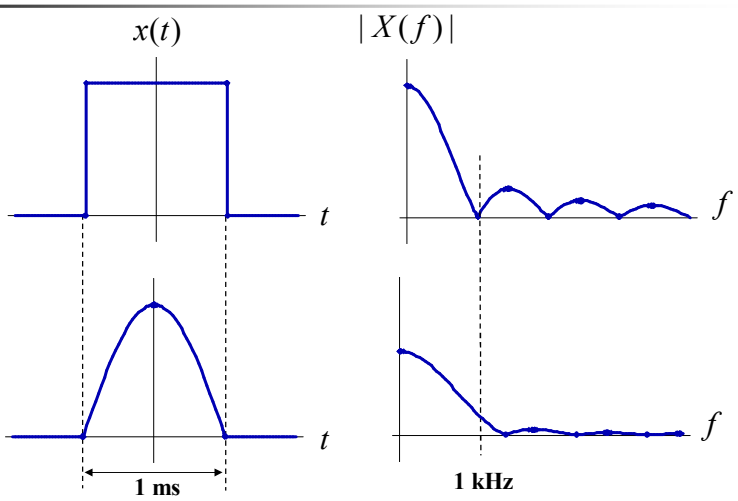



## Primeri spektrov




**širina spektra je odvisna od trajanja signala !**

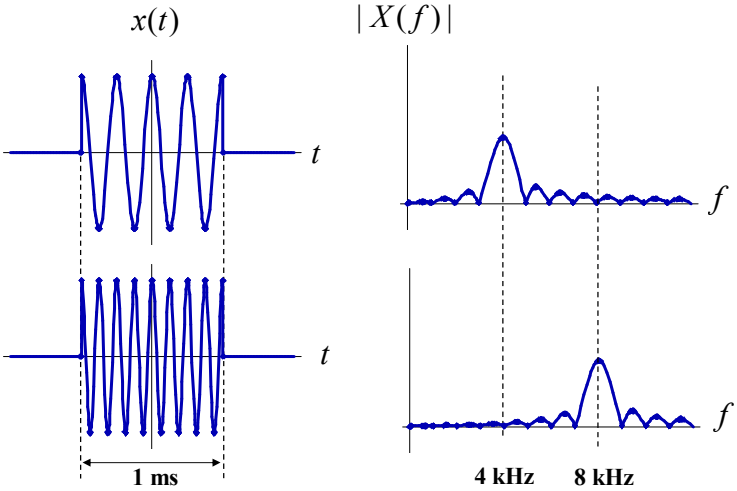
## Primeri spektrov




**širina spektra je odvisna tudi od oblike signala !**

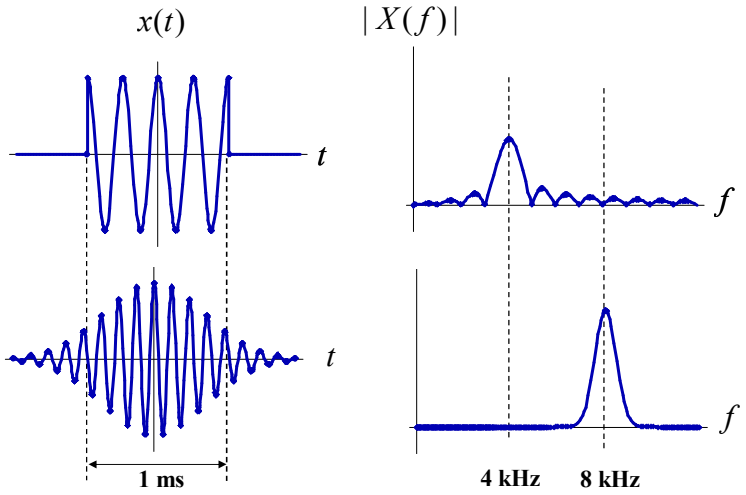


## Primeri spektrov




**Spekter moduliranega impulza (kratek pisk 4kHz, 8kHz ).**

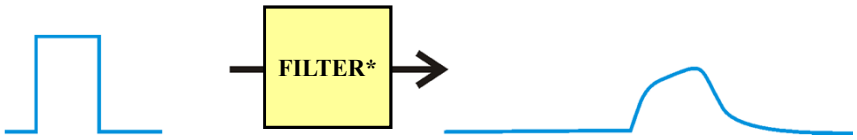
## Primeri spektrov






## Filtriranje signalov

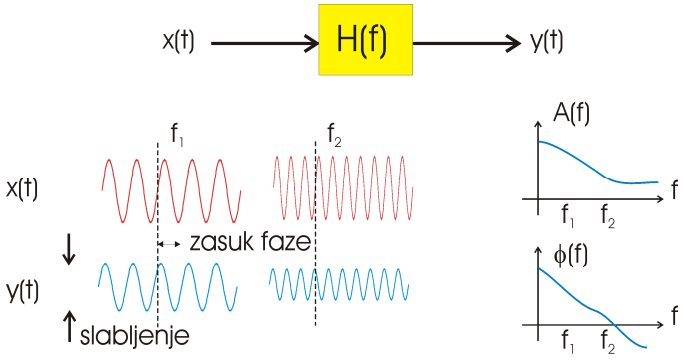
- Signal pri prehajanju skozi filter spremeni svojo obliko.




- **Signal vsebuje različne frekvenčne komponente. Frekvenčna vsebina je razvidna v spektru signala.**
- **Sprememba oblike je posledica razlik v slabljenju in razlik v zakasnitvah med različnimi spektralnimi komponentami signala.**

## Filtriranje harmoničnega signala

- Sito ne prepušča enako vseh frekvenc enako!
  - razlike so v ojačenju ali slabljenju
  - razlike so v zakasnitvah in faznem zasuku



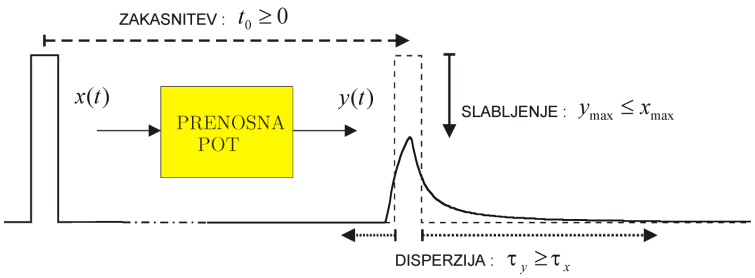



## Primer filtriranja signala

- graphic equalizer (grafični izravnalnik) je namenjen filtriranju audio signalov.
- primer na sliki:
  - 4 frekvenčni pasovi na oktavo; 31 frekvenčnih pasov (ang.: band),
  - ločeno nastavljanje ojačenj za vsak frekvenčni pas: +/- 12dB

## Filtriranje pri prenosu komunikacijskih signalov

Zgled: popačitev električnega impulza na bakrenem kablu



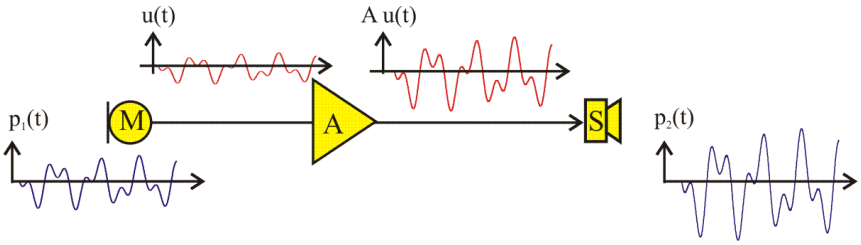



## 3. ANALOGNE IN DIGITALNE KOMUNIKACIJE

- Prenos analognih signalov
  - Pretvorba akustičnega v električni signal
  - Prenos zvokovnega signala po žicah
  - Radijski prenos analognih signalov
  - Model prenosnega komunikacijskega kanala
  - Popačitve analognih signalov in kriterij kvalitete
  - Omejitve pri prenosu analognih signalov
- Prenos digitalnih signalov
  - Kriterij kvalitete
  - Prednosti digitalnega zapisa signalov
- Analogno-digitalna pretvorba signalov
  - Vzorčenje signalov
  - Kvantizacija in kodiranje vzorcev
  - Popačitve in kvaliteta digitaliziranega signala

## Prenos analognih signalov

- prenos analognih signalov na kratki razdalji:
  - mikrofon pretvori akustični signal v podoben – analogen električni signal ,
  - ojačevalnik poveča napetost električnega signala za faktor A,
  - zvočnik pretvori električni signal v podoben akustični signal.

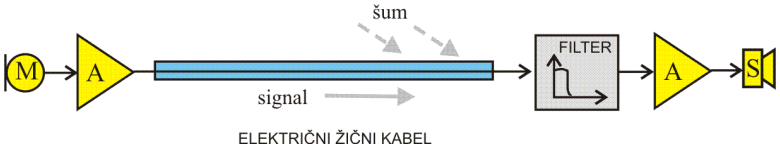



- **podobnost obeh akustičnih signalov je odvisna od kvalitete mikrofona in zvočnika.**



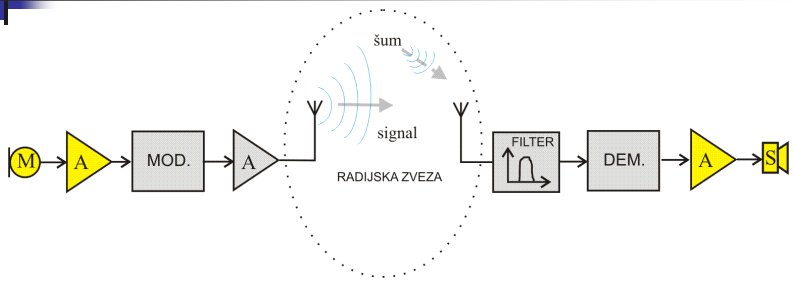
## Prenos v osnovnem frekvenčnem pasu

- žična komunikacija:




- **žični kabel zakasni, slabi in popači električni signal ,**
- **kabel "sprejema" tudi neželene tuje signale,**
- **na kvaliteto signala za zvočnikom vpliva nastavitev filtra:**
  - **filter naj je naravnan tako, da prepusti čim več signala in čim manj šuma,**
  - **optimalna nastavitev filtra je odvisna od frekvenčnega spektra signala in od frekvenčnega spektra šuma**
  - **tudi z optimalnim filtrom ni mogoče popolnoma izločiti šuma!**

## Radijski prenos analognih signalov

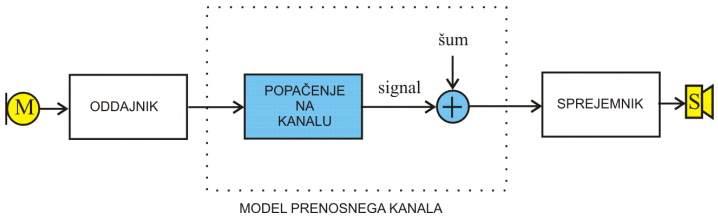



- **Modulator "premakne" nizkofrekvenčni analogni signal v višjo frekvenčno lego, ki je primerna za prenos po radijskem kanalu.**
- **Filter v sprejemniku je "naravnan" tako, da prepušča spekter oddanega signala. V istem frekvenčnem pasu se delno nahajajo tudi motilni signali – šum.**
- **Demodulator v sprejemniku premakne modulirani visokofrekvenčni signal nazaj v osnovno frekvenčno lego.**
- **Reproducirani akustični signal je popačen predvsem zaradi motenj na radijski zvezi.**



## Prenos analognih signalov

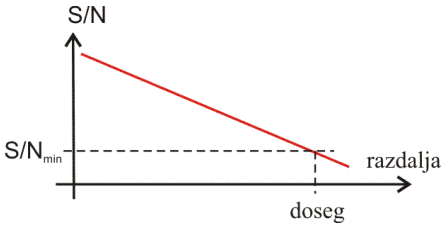
- model prenosnega sistema

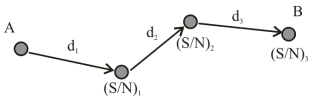



- **Par oddajnik in sprejemnik ne prispevata bistveno k popačenju signala.**
- **Popačenje signalov nastopi na fizičnem kanalu:**
  - **prenosni medij popači električne signale (filtriranje: slabljenje, fazno popačenje)**
  - **prištevajo se tuji motilni signali – šum**

## Omejitve pri analogni komunikaciji

- Kvaliteto analognega signala izraža razmerje med signalom in šumom:
  - slabljenje narašča z razdaljo, zato moč signala (**S**ignal) upada,
  - moč šuma (**N**oise) narašča z razdaljo



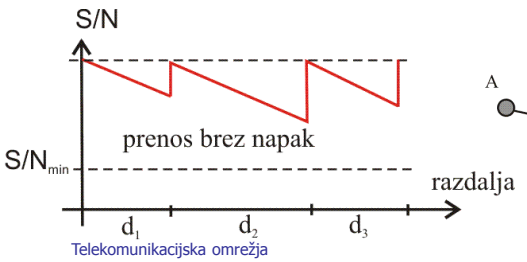



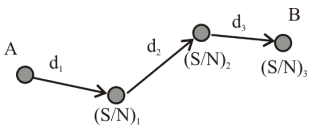

- **Kvalitete analognih signalov na večji razdalji ni mogoče ohraniti !**
- **Povezava v omrežju je sestavljena iz množice poti med vmesnimi vozlišči. Razmerje med signalom in šumom se na poti med oddajnikom A in sprejemnikom B lahko samo zmanjšuje!**
- **Najnižje dopustno razmerje S/N določa doseg zveze.**



## Prednost znakovnih komunikacij

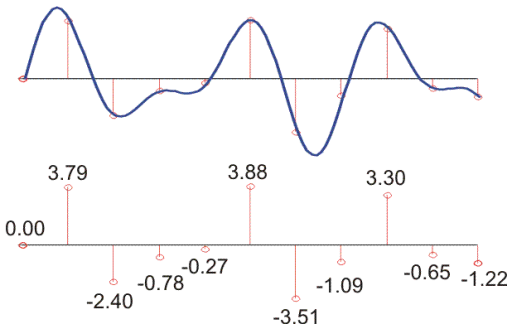
- Tudi pri znakovni – digitalni komunikaciji se signali popačijo in na kanalu se tudi prišteva šum.
- Kvaliteto znakovne komunikacije določa število napačno prenešenih znakov.
- Znakovni signal je do določene mere neobčutljiv na šum:
  - šum ne vpliva na kvaliteto vse dokler ne povzroči napake pri prenosu
  - znakovni signal lahko obnovimo in šum se ne akumulira na celotni poti po omrežju.



## Analogno-digitalna pretvorba signalov

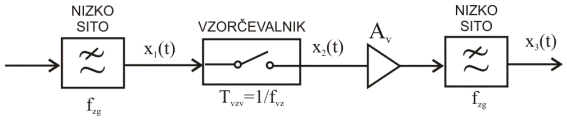
- Postopek A/D pretvorbe poteka v dveh fazah:
  1. časovno zvezni signal najprej enakomerno vzorčimo,
  2. vzorce signala kodiramo z omejenim številom bitov.

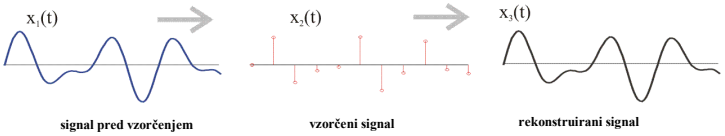





## Vzorčenje analognega signala

- Signal mora biti pred vzorčenjem frekvenčno omejen.
- Vzorčeni signal sestavljajo vzorci, ki so razmaknjeni za čas $T_{vz}$ :

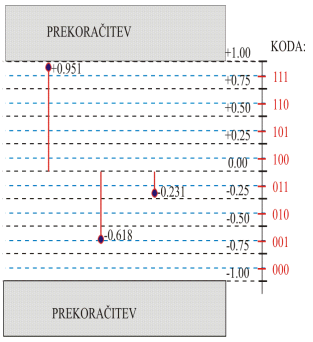



- **Da lahko iz vzorcev popolnoma rekonstruiramo prvotni signal, mora biti vzorčevalna frekvenca vsaj dvakrat višja od najvišje frekvence v spektru analognega signala:** $f_{vz} \geq 2 f_{zg}$

# Kvantizacija vzorcev

- Vzorce lahko kodiramo v omejenem območju vrednosti, ki ga imenujemo dinamično območje kvantizatorja. Če je vrednost vzorca večja od meje dinamičnega območja nastopi napaka zaradi prekoračitve.
- Vrednosti vzorcev lahko kodiramo s končno natančnostjo, ki je omejena z dolžino zapisa. Postopek zaokroževanja po vrednosti imenujemo kvantizacija.
- Napaka pri zaokroževanju povzroči popačitev signala. Učinek je enak, kot če bi signalu dodali šum. Napako pri kvantizaciji zato imenujemo kvantizacijski šum.






# Kvaliteta A/D pretvorbe

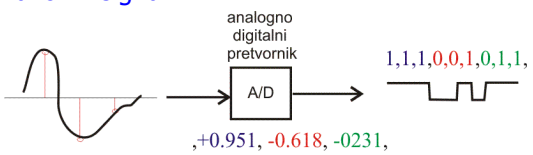
- Kvaliteto pretvorbe izraža razmerje med močjo signala in močjo kvantizacijskega šuma. Razmerje se podaja z logaritemsko mero v decibelih:
  - b: število bitov A/D pretvorbe
  - $X_{eff}^2$: povprečna moč signala
  - D: meja dinamičnega območja kvantizatorja

$$SNR_{AD} \approx 6 \cdot b + 10 \log \frac{3 \cdot x_{eff}^{\ 2}}{D^2}$$

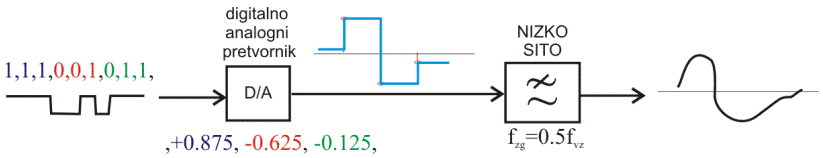
- **primer:**
  - **dinamično območje kvantizatorja je med –D=-4 in D=4,**
  - **območje je enakomerno razdeljeno na 256 korakov (kvantov),**
  - **vsak vzorec na izhodu kvantizatorja je zapisan z b=8 biti**
  - **povprečna moč signala je $X_{eff}^2$ =10**
  - **Izračunani SNR=6*8+10log(30/16)=50.73dB**

## Analogno-digitalni in digitalno-analogni pretvornik

- Na vhodu A/D pretvornika je analogni signal.
- Na izhodu A/D je zaporedje števil v binarni obliki – digitalni ali znakovni signal.




- **Na vhodu D/A pretvornika je digitalni signal.**
- **Na izhodu D/A je stopničasti signal, ki se preblikuje na rekonstrukcijskem situ.**



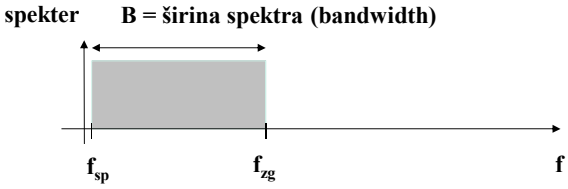



## 4. MODULACIJE

- Osnovni frekvenčni pas analognega signala
- Zakaj potrebujemo modulacijo ?
- Analogni modulacijski postopki
  - Amplitudna modulacija
  - Fazna modulacija
  - Frekvenčna modulacija
- Primerjava spektrov analogno moduliranih signalov: AM in FM

## Osnovni frekvenčni pas signala

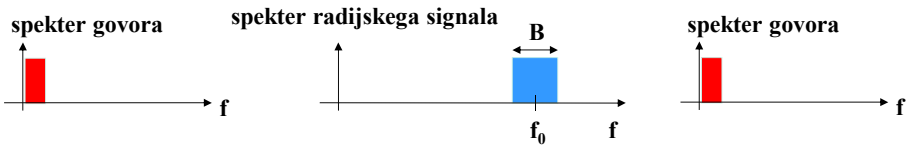
- Analogni signal na izvoru zaseda omejen frekvenčni pas, ki ga imenujemo tudi **osnovni frekvenčni pas** (ang.: baseband).
  - akustične signale lahko omejimo na slišno območje med 20Hz in 20kHz,
  - govorni signal ostaja razumljiv če spekter omejimo na območje od 300Hz do 3400 Hz.
- Če želimo prenašati signale v njihovem osnovnem pasu, moramo imeti na razpolago **prenosni medij**, ki to omogoča.
  - telefonsko naročniško omrežje je zasnovano na žičnih povezavah,
  - bakrene žične povezave so kvaliteten prenosni medij za povezavo analognih naprav na zelo kratki razdalji.






## Pomen modulacije

- Radijski medij ni primeren za prenos govornega signala v osnovnem pasu.
- **Modulacija** je postopek, ki povzroči premik signala v višjo frekvenčno lego. Takšen signal je mogoče tudi brezžično prenašati po prostoru.
- V sprejemniku se signal demodulira in s tem prestavi v osnovni frekvenčni pas.

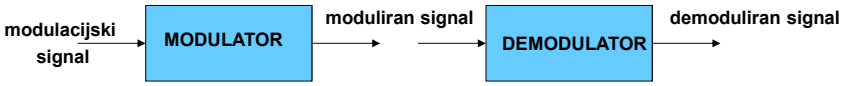
## Modulacija in demodulacija

**Modulacija** je postopek, pri katerem modulacijski (informacijski) signal spreminja lastnosti pomožnega signala (nosilca).

- **modulacijski signal** je signal na vhodu modulatorja, ki nosi informacijo
- **nosilec** je pomožni signal sinusne oblike,
- **moduliran signal** na izhodu modulatorja nosi vso informacijo signala na vhodu modulatorja
- **modulator** je gradnik (HW ali SW), ki izvaja modulacijo

**Demodulacija** je obratni postopek modulaciji.

- **demodulator** je gradnik (HW ali SW), ki izvaja demodulacijo
- **demoduliran signal** v sprejemniku je v idealnem primeru enak modulacijskemu signalu v oddajniku.

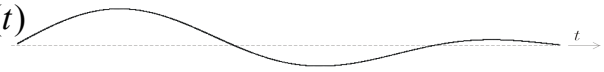




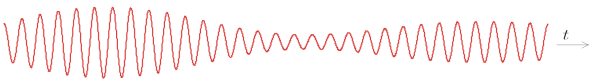

## Zgledi moduliranih signalov: AM, FM in PM

nosilec: $A \cdot \cos(\omega \cdot t + \phi)$

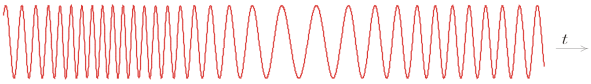

modulacijski signal: $m(t)$



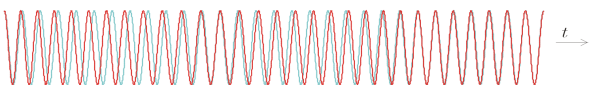

- AM




- FM

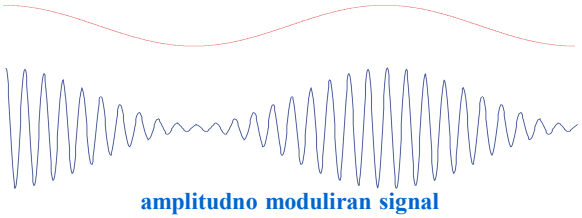



- PM



## Amplitudna modulacija - AM

- Amplituda nosilca je sorazmerna modulacijskemu signalu.
- Ločimo več vrst analognih AM, ki se razlikujejo po širini spektra:
  - AM-DSB-LC (Double Side Band , Large Carrier)
  - AM-DSB-SC (Double Side Band, Suppressed Carrier)=dvobočni AM
  - AM-SSB (Single side band)= enobočni AM
- Na kvaliteto zveze močno vplivata šum in nelinearno popačenje!

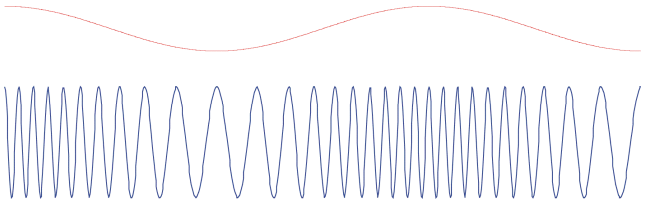


amplitudno moduliran signal



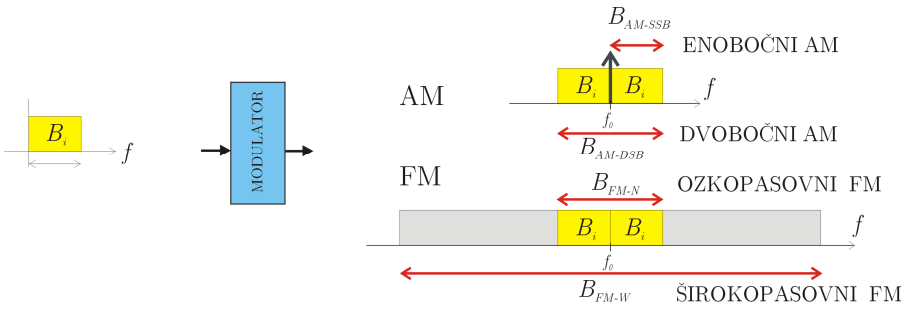
## Frekvenčna modulacija - FM

- Trenutna frekvenca FM signala je sorazmerna modulacijskemu signalu.
- Amplituda FM signala se ne spreminja.
- FM signal ni občutljiv na amplitudna popačenja



frekvenčno moduliran signal

## Spektri analognih moduliranih signalov




- Spekter moduliranega signala ne more biti ožji od spektra modulacijskega signala.



## 5. OSNOVE INFORMACIJ

- Definicija informacije, C.E. Shannon
  - Informacija o dogodku in verjetnost dogodka
- Entropija informacijskega izvora
- Kodiranje simbolov
  - Morsejeva koda
  - Redundanca in irelevanca
  - Brezizgubno kodiranje
    - Huffmanova koda

## Informacija

Kaj je informacija ?

Na kaj vežemo informacijo ?

Kako je informacija merljiva ?

---

začetek informatike:
C.E. Shannon, Matematična teorija komunikacij, 1948



## Informacija o dogodku in verjetnost dogodka

Izhodišča:

- Informacija je vezana na verjetnost dogodka.
- Verjetnost dogodka merimo med 0 in 1:
  - p(neverjeten dogodek)=0
  - p(gotov dogodek)=1
- Gotovi dogodki ne nosijo informacije.
- Manj verjetni dogodki nosijo več informacije kot bolj verjetni dogodki.
- **Informacija o dogodku je obratno sorazmerna verjetnosti dogodka:**

$$I(A) \propto \frac{1}{p(A)}$$

## Merjenje informacije

- Verjetnost dveh neodvisnih dogodkov je enaka produktu verjetnosti dogodkov:
  - verjetnost dogodka A: p(A)
  - verjetnost dogodka B: p(B)
  - verjetnost dogodka A in B: p(A B)=p(A) p(B)
- Informacije o neodvisnih dogodkih se morajo seštevati.

- Naštete zahteve izpolnjuje **logaritemska mera**:

$$I(A) = \log_2 \frac{1}{p(A)} = -\log_2 p(A)$$

- Informacijo merimo v bitih: bit, kbit, Mbit, ...
- več bitov je združenih v besede: 8 bit =1 byte,



## Povprečna infomacija izvora

- Izvor je generator množice N različnih znakov.
- Verjetnosti nastopanja posamičnih znakov lahko ugotovimo z merjenjem frekvenc dogodkov.
- Povprečna informacija je vsota informacij, ki so utežene z verjetnostjo dogodkov. Povprečno informacijo na izvoru imenujemo entropija izvora:

$$H = \sum_{i=1}^{N} p(A_i) I(A_i) = -\sum_{i=1}^{N} p(A_i) \log_2 p(A_i)$$

- Entropija je največja, če so vsi dogodki enako verjetni:

$$H_{\max} = \log_2(N)$$

## Met kocke

- Izvor je generator množice 6 različnih znakov.
  - K=1, K=2, K=3, K=4, K=5, K=6
- Vsi dogodki so enako verjetni: verjetnosti nastopanja posamičnih znakov so enake 1/6.
- Povprečna informacija pri metu kocke je približno 2,58 bita.

$$H = H_{\max} = \log_2(6) \approx 2,58$$



## Kodiranje znakov

Vsakemu znaku priredimo določeno lastno binarno kodo.

- Dolžina kode je lahko enaka za vse znake.
  - 7bit ASCII tabela znakov (128 znakov) " a b c "= 1100001 1100010 110011
- Če imajo kode znakov različne dolžine da krajše kode niso enake okrajšanim začetkom daljših kod: (npr: A=1011, B=10111).

## Morsejeva koda

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A | .- | M | -- | Y | -.-- | 6 | -.... |
| B | -... | N | -. | Z | --.. | 7 | --... |
| C | -.-. | O | --- | Ä | .-.- | 8 | ---.. |
| D | -.. | P | .--. | Ö | ---. | 9 | ----. |
| E | . | Q | --.- | Ü | ..-- | . | .-.-.- |
| F | ..-. | R | .-. | Ch | ---- | , | --..-- |
| G | --. | S | ... | 0 | ----- | ? | ..--.. |
| H | .... | T | - | 1 | .---- | ! | ··—· |
| I | .. | U | ..- | 2 | ..--- | : | ---... |
| J | .--- | V | ...- | 3 | ...-- | " | .-..-. |
| K | -.- | W | .-- | 4 | ....- | ' | .----. |
| L | .-.. | X | -..- | 5 | ..... | = | -...- |

- Samuel Morse, električni telegraf, 1836
- Morsejeva koda ni binarna, saj poleg kratkega znaka . in dolgega znaka _ vsebuje še presledke različnih dolžin:
  - zelo kratek presledek med pikami in črtami v znaku, kratek presledek med znaki, presledek med besedami, dolg presledek med stavki.
  - brez presledkov kode zato ni mogoče dekodirati.
- . . . _ _ _ . . . ?



## Učinkovito brezizgubno kodiranje znakov

- Ravnanje "po občutku" :
  - Znakom ki pogosto nastopajo priredimo krajšo kodo.
  - Znakom ki redko nastopajo lahko priredimo daljšo kodo.
- Znanstvena utemeljitev: Znaki z veliko verjetnostjo nastopanja nosijo manj informacije, zato jih kodiramo z manj biti.

$$I(A) \propto \frac{1}{p(A)}$$

## Omejitve pri kodiranju ?

Dolžina kode je odvisna od števila znakov.

- Za kodiranje N znakov potrebujemo največ $\log_2(N)$ bitov.
- Povprečna dolžina kode je lahko tudi manjša !

- Če ne želimo izgubiti dela informacije, potem povprečna dolžina kode na izhodu kodirnika ne sme biti manjša od entropije izvora. Takšno kodiranje zato imenujemo tudi brezizgubno kodiranje. Primer brezizgubnega kodiranja je stiskanje datotek (zip).

- Pri kodiranju govora upoštevamo dejstvo, da vsa informacija ni enako pomembna (relevantna). Učinkoviti kodirniki za govor izločajo nepomemben del informacije, ki za poslušalca ni zaznavna. Izgubljeni nepomemben del informacije imenujemo irelevanca. Takšno kodiranje imenujemo izgubno kodiranje.



## Primer izvora

- Izvor je generator množice 4 različnih znakov: **a**,**b**,**c** in **d**
- Po štetju 1000 znakov ugotovimo, da :
  - znak **a** nastopa 500 krat ,
  - znak **b** nastopa 250 krat ,
  - znak **c** nastopa 125 krat in
  - znak **d** nastopa 125 krat.
- Verjetnosti nastopanja znakov so:
  p(a)=0.5, p(b)=0.25, p(c)=0.125 in p(d)=0.125
- Informacije o dogodkih so:
  I(a)=1, I(b)=2 , I(c)=3 in I(d)=3
- Povprečna informacija je enaka:
  H=0.5*1+0.25*2+0.125*3+0.125*3=1.75 [bit]
- Če bi vsi znaki nastopali z enako verjetnostjo, bi bila entropija izvora 2 bita.

## Redundanca

- Če ne poznamo verjetnosti nastopanja znakov, je povprečna dolžina kode odvisna samo od števila znakov:
  - štiri znake kodiramo z dvemi biti,
  - za kodiranje 128 znakov potrebujemo 7 bitov,
  - za kodiranje 1024 različnih znakov potrebujemo 10 bitov...
- Povprečna dolžina kode je pogosto daljša od povprečne informacije.
- Relativno število "odvečnih" bitov imenujemo redundanca.
- Uporabimo že navedeni primer izvora s štirimi znaki (a,b,c,d)
  - Izvor generira štiri znake, vsak znak kodiramo z dvemi biti.
  - Entropija izvora je enaka 1.75 bit.
  - Za 1000 znakov uporabimo 2000 bitov potrebujemo pa le 1750 bitov.
  - Razlika 250 bitov je "odvečna" informacija.
  - Vsak osmi bit je v povprečju odveč.
  - Redundanca je po definiciji enaka R=1-H/Hmax=1-1.75/2=0.125



## Entopijsko kodiranje izvora

- Za prej navedeni primer izvora lahko generiramo kodo, ki ima v povprečju manj kot dva bita na znak.
  - Verjetnosti nastopanja znakov so:
    p(a)=0.5, p(b)=0.25, p(c)=0.125 in p(d)=0.125
- Kode znakov (Huffmanove kode):
  - *a : 0*
  - *b : 10*
  - *c : 1 1 0*
  - *d: 1 1 1*
- Povprečna dolžina kode je večja ali enaka entropiji izvora:
  L=0.5*1+0.25*2+0.125*3+0.125*3=1.75 [bit]
- Zaporedje bitov lahko dekodiramo v niz znakov brez izgube informacije: *..01010111.. = ..a,b,b,d..*

## 6. OSNOVE DIGITALNIH KOMUNIKACIJ

- Komunikacija s simboli, znaki, števili ...
- Hitrost komunikacije, simbolna frekvenca
- Binarni informacijski signal, kodiranje pri signalov za prenos
- Informacijski pretok
- Omejitve pri prenosu informacije
  - Popačitve signalov pri prenosu
  - Omejitve zaradi intersimbolne interferenca
  - Omejitve zaradi šuma
- Zaščita informacij za prenos, kanalno kodiranje

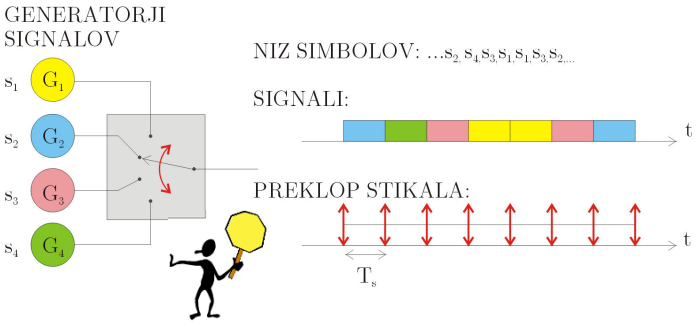


## Nabor dogovorjenih simbolov

- **Informacijo** prenašamo v obliki zaporedja dogovorjenih znakov ali simbolov.
- **M** znakov izberemo tako, da so med seboj čim bolj ločljivi !
- en znak lahko nosi v povprečju največ $b_s = \log_2(M)$ bitov informacije
- eden od starejših načinov znakovnih komunikacij ☺ :

## Simbolna frekvenca

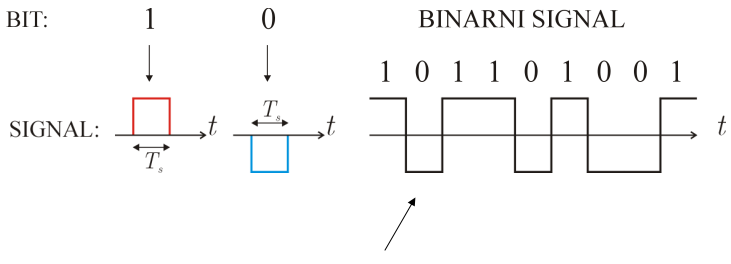
- Vsak znak predstavlja določeni električni signal, ki ima omejen čas trajanja $\mathbf{T_s}$
- Zaporedje simbolov se prenaša po komunikacijskem mediju kot zaporedje električnih signalov.
- **Simbolna frekvenca $f_s$** (ang: baud-rate) določa število simbolov, ki jih prenašamo v eni sekundi: $\mathbf{f_s = 1/T_s}$






## Binarni signal

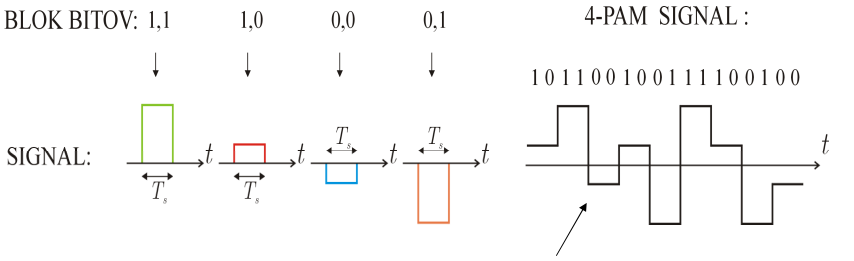
- Binarni signal vsebuje dva različna znaka.
- Koda znaka je zapisana z enim bitom: 0, 1




**zaporedje znakov=zaporedje bitov**

## Primer komunikacije s štirimi znaki

- V enakem času lahko prenesemo dvakrat več bitov informacije:




**zaporedje znakov=zaporedje blokov (parov) bitov**

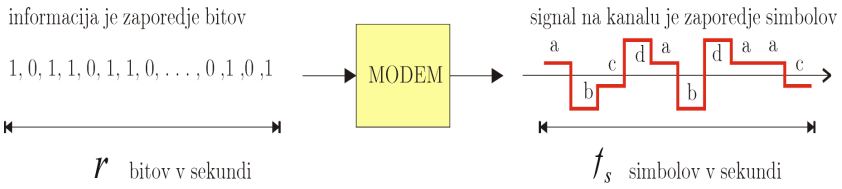
- **Grayevo kodiranje znakov: "sosedni" znaki se razlikujejo samo za en bit.**



## Informacijski pretok

- **Informacijski pretok ali hitrost prenosa informacije** (information transfer rate) je produkt znakovne frekvence s povprečnim številom bitov informacije, ki jih nosi en znak:

$$r = b_s \cdot f_s$$




- **Informacijski pretok merimo v bitih na sekundo: bit/s, kbit/s, Mbit/s**

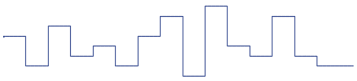
## Omejitve pri prenosu informacije

- **Kako povečamo hitrost prenosa informacije ?**

$$r = b_s \cdot f_s$$

**r=r$_1$ b$_s$=1, f$_s$=f$_1$**

**r=4 r$_1$ b$_s$=1, f$_s$=4 f$_1$**



**r=3 r$_1$ b$_s$=3, M=8, f$_s$=f$_1$**

**r=12 r$_1$ b$_s$=3, M=8, f$_s$=4 f$_1$**

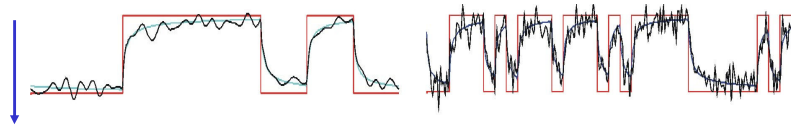
- Če povečamo znakovno hitrost, razširimo spekter signala.
- Če povečamo število znakov M, se ob nespremenjeni moči signala zmanjša razlika med znaki.



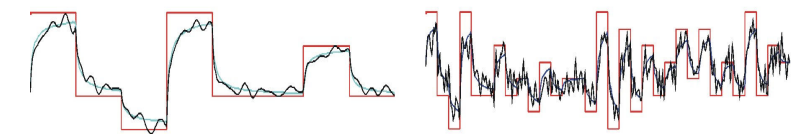
## Popačitve na fizikalnem kanalu

- popačenje signala in šum zmanjšujeta prepoznavnost znakov:

**b$_s$ , f$_s$** → **b$_s$ , 4 f$_s$**

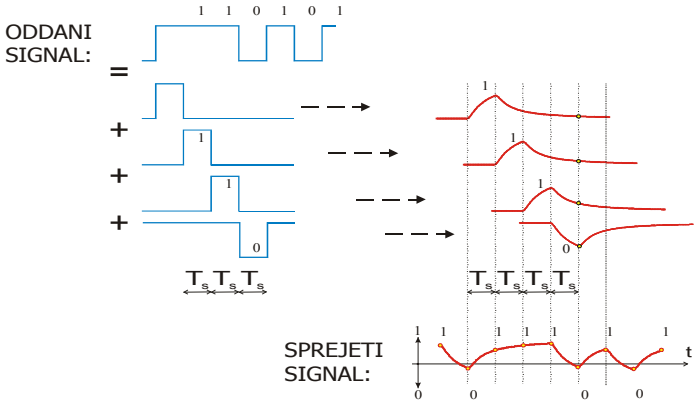


**3 b$_s$ , f$_s$** **3 b$_s$ , 4 f$_s$**



## Disperzija impulzov in interferenca

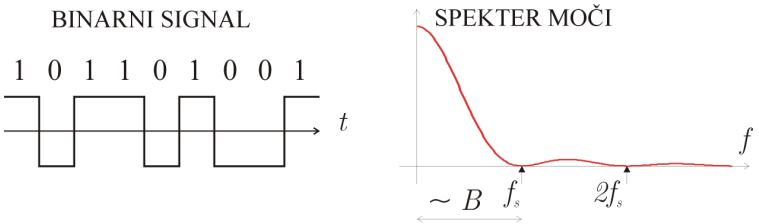
- Zaradi disperzije se impulzi v sprejemniku med seboj prekrivajo :





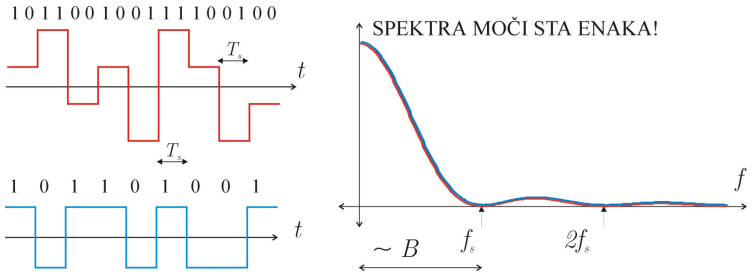

## Spekter binarnega signala

- Za prenos potrebujemo frekvenčni pas v katerem se nahaja večji del moči signala.
- Več kot 90% moči binarnega signala se nahaja do znakovne frekvence $f_s$:



## Spekter zaporedja impulzov

- Povečanje števila amplitud impulzov ne vpliva na spekter signala:

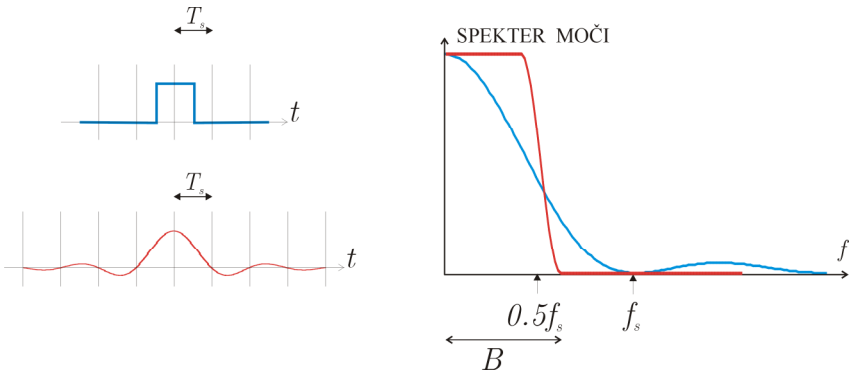



- **Širina spektra je odvisna od trajanja impulzov in tudi od oblike impulzov.**



## Oblika impulzov in spekter

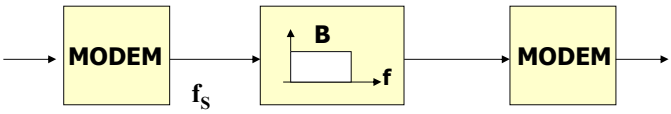
- Širina spektra signala je najmanj polovica znakovne frekvence:



## Omejitve s pasovno širino

- "Na frekvenčno omejenem kanalu s pasovno širino B lahko prenašamo največ 2B znakov v sekundi".
  (H. Nyquist, 1927)
- Če je znakovna frekvenca večja od 2B, ne moremo preprečiti interference zaradi prekrivanja znakov.

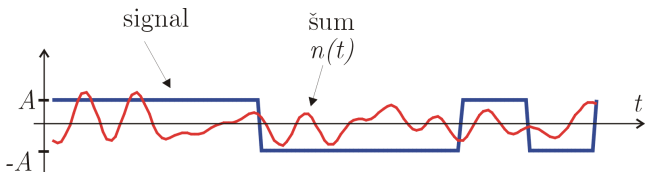
- Primer:
  - Po kanalu s pasovno širino B=1MHz lahko prenašamo največ 2 milijona znakov v sekundi. (2Mbaud)






## Omejitve zaradi šuma

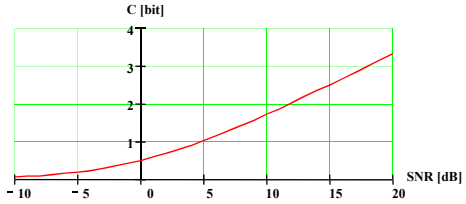
- Zaradi šuma so znaki v sprejemniku manj prepoznavni.
- Če je moč šuma prevelika v primerjavi z močjo signala, nastopijo napake pri prepoznavanju znakov v sprejemniku.
- Verjetnost napake je odvisna od razmerja med močjo signala in močjo šuma.



## Kapaciteta kanala

- Kapaciteta kanala nam pove teoretično maksimalno število bitov, ki jih lahko v enem znaku prenesemo po šumnem kanalu brez izgube informacije. Odvisna je od razmerja med močjo signala in močjo šuma:

$$C = \frac{1}{2}\log_2(1+\frac{P_s}{P_n})$$

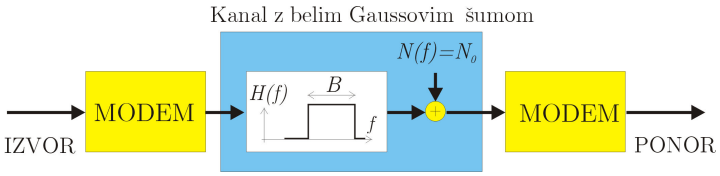



$$SNR = 10\log(\frac{P_s}{P_n})$$



## Omejitev s šumom in pasovno širino

- Količina informacije , ki jo lahko v eni sekundi prenesemo po komunikacijskem kanalu je omejena z:
  - močjo signala Ps,
  - močjo šuma Pn in
  - širino frekvenčnega pasu B.




$$r_{\max} = B \cdot \log_2(1+\frac{P_s}{P_n})$$

## Zgled:

- Koliko bitov v sekundi lahko teoretično prenašamo po frekvenčno omejenem kanalu z belim Gaussovim šumom s podatki:
  - pasovna širina kanala je 4000 Hz
  - razmerje signal/šum na kanalu je konstantno 30dB, kar ustreza razmerju moči Ps/Pn=1000
- Odgovor: Največja hitrost prenosa po takšnem kanalu je približno 40.000 bitov v sekundi:
  - $r_{max}=4000 \log_2(1001)=39869$ bit/s

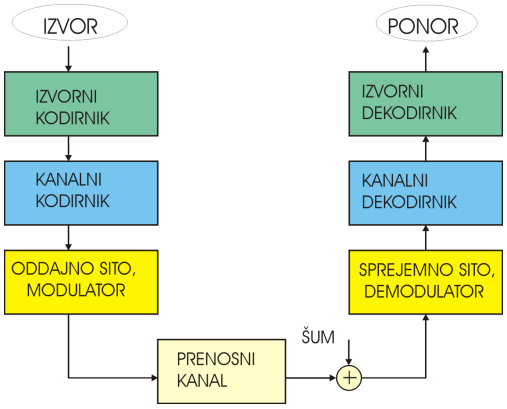
$$r_{\max} = B \cdot \log_2(1+\frac{P_s}{P_n})$$



## Kodiranje signalov

V modelu prenosnega sistema nastopata dve vrsti kodiranja:

- kodiranje izvora ali **izvorno kodiranje**
- kodiranje za prenos ali **kanalno kodiranje**



## Namen kanalnega kodiranja

- **Kanalni kodirnik dodaja redundanco informacijskemu signalu.**
- **Učinek kodiranja se stopnjuje glede na delež redundance:**
  - **Če dodamo malo redundance, lahko detektiramo napake pri prenosu,**
  - **Če v kanalnem kodirniku dodamo več redundance, lahko v sprejemniku na kanalnem dekodirniku detektiramo in tudi popravljamo napake.**


- **Učinkoviti postopki kanalnega kodiranja in dekodiranja uporabljajo dekodiranje na osnovi prepoznavanja najbolj verjetnih dolgih znakovnih zaporedij.**



## Odkrivanje in popravljanje napak

- Napake odkrivamo običajno z dodajanjem redundance v obliki paritete ali v obliki ciklične redundance (CRC).
  - Paritetni bit v 7B-8B kodi pove ali je v predhodnih 7 bitih sodo ali liho število enic:
    - 00110111 ni napake
    - 00010111 prišlo je do napake
  - Namesto paritetnega bita lahko dodamo CRC. CRC je lahko dolg več bitov in ga izračunamo na osnovi vseh bitov v bloku s pomočjo polinoma. CRC omogoča odkrivanje več napak v bloku.

- **Da bi lahko napako popravili, moramo dodati več redundance.**

**Primer popravljanja je bločno kodiranje z dvakratno pariteto:**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | |

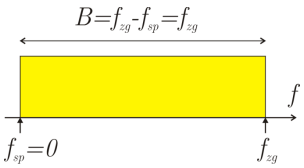
## 7. DIGITALNE MODULACIJA

- Povezava z analognimi postopki
- Model digiatlnega modulatorja
- Osnovni binarni modulacijski postopki: ASK, PSK in FSK
- Mešani postopek, kvadraturna modulacija QAM
- Prenos z več nosilci
- Primerjava postopkov na primerih iz prakse



## Delitev frekvenčnih pasov

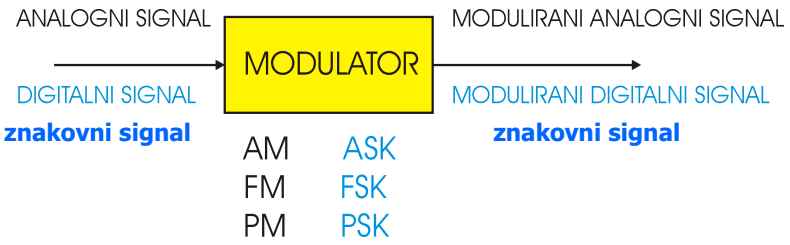
- **Osnovni frekvenčni pas** (baseband) je frekvenčno območje v katerem se nahaja večji del moči signala izvora. V znakovnih komunikacijah z bipolarno ali večnivojsko kodo uporabljamo frekvenčno področje od 0Hz naprej:




- **Znakovna komunikacija v osnovnem frekvenčnem pasu mogoča le po žičnih kablih.**
- **Radijske znakovne komunikacije ne potekajo v osnovnem pasu, pač v višjih frekvenčnih pasovih (passband).**

## Digitalne modulacije

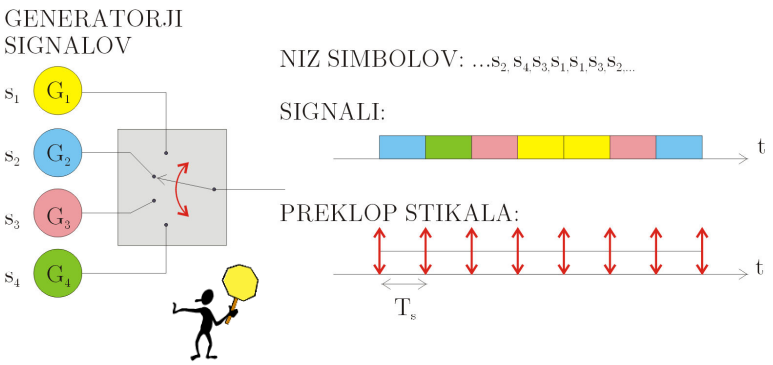
- Osnovni digitalni modulacijski postopki so podobni analognim modulacijskim postopkom, razlika je v signalu na vhodu modulatorja:





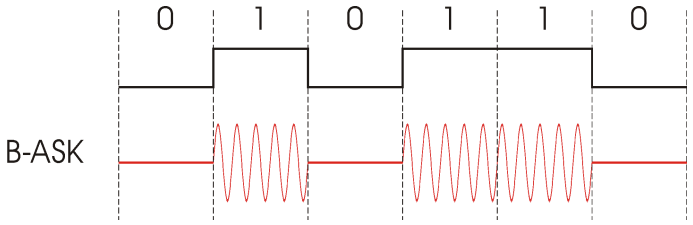

## Digitalni modulator

- Vsak znak predstavlja električni signal.
- Izberemo M harmoničnih signalov, ki se razlikujejo po amplitudi, fazi ali frekvenci !



## Amplitudna modulacija ASK

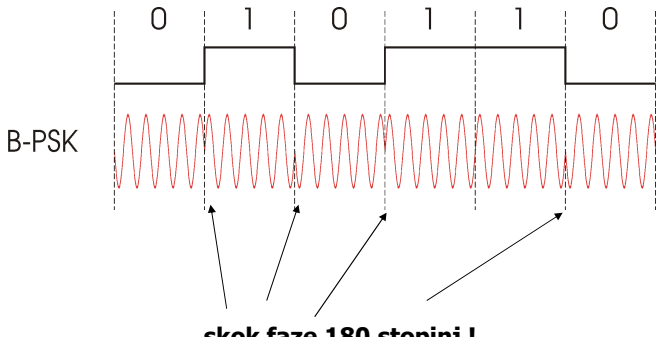
- **ASK** (Amplitude-Shift Keying) , "amplitudni skok" . Znaki se razlikujejo po amplitudi nosilca.
- Najbolj preprost je binarni ASK (BASK):





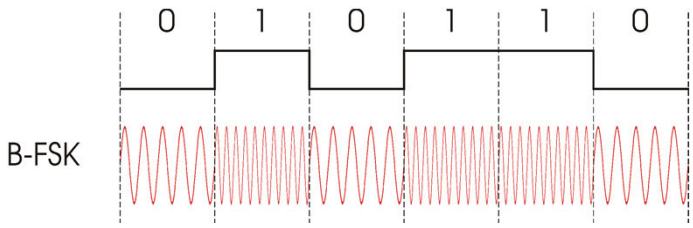

## Fazna modulacija **PSK**

- PSK (Phase Shift Keying) , "fazni skok". Znaki se razlikujejo po fazi nosilca.
- Najbolj enostaven PSK je binarni PSK (BPSK):



## Frekvenčna modulacija **FSK**

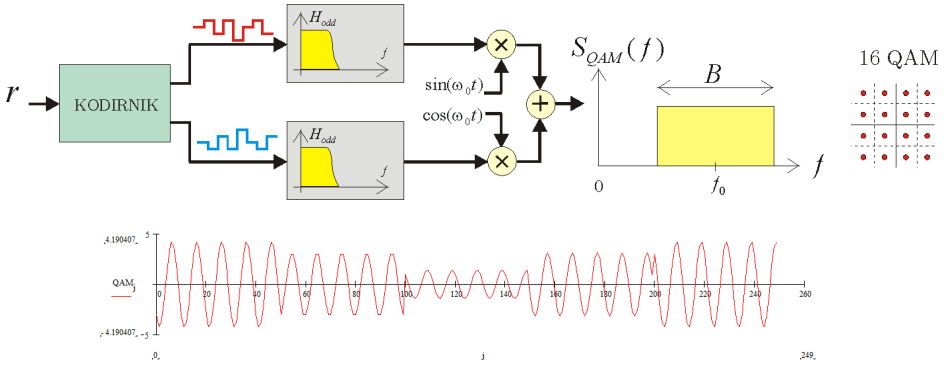
- FSK (Frequency Shift Keying) , "frekvenčni skok". Znaki se razlikujejo po frekvenci nosilca.
- Najbolj enostaven FSK je binarni FSK (BFSK):





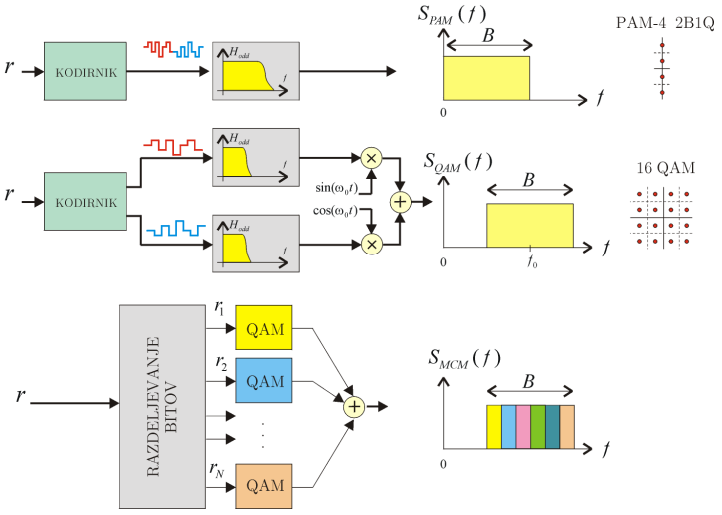

## Kvadraturna amplitudna modulacija QAM

- QAM (Quadrature Amplitude Modulation) signal je vsota dveh amplitudno muduliranih signalov. Ločitev obeh komponent v sprejemniku je mogoča zaradi različne faze nosilcev:



# Več kanalni QAM (MCM)

- PAM
- QAM
- **MCM**
  **DMT**
  **OFDM**






# Katera modulacija je najboljša ?

- Izbira modulacijskega postopka je odvisna od razmer na prenosnem kanalu.

žični prenosni kanal:

- če je na razpolago osnovni pas od 0Hz dalje, modulacija ni potrebna.
- sodobni telefonskih modemi uporabljajo kodirani QAM = TCM,
- nekatere xDSL tehnologije uporabljajo CAP (QAM) in DMT (večkanalni QAM),

radijski prenosni kanal:

- na mobilnem kanalu se uporablja FSK, PSK, (QAM)
- digitalni radio in TV (DAB in DVB) uporabljata OFDM (večkanalni DQPSK in QAM)
- zmogljive fiksne radijske povezave uporabljajo QAM

katera modulacija je najboljša ? .....

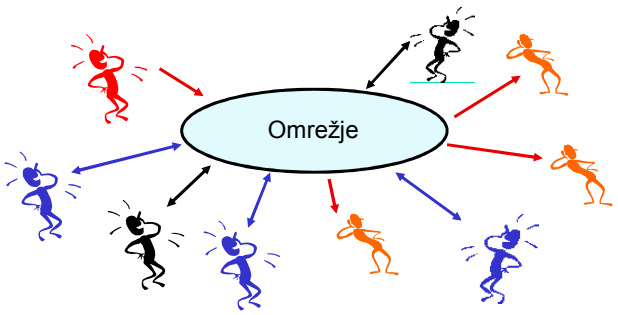
# 8. KOMUNIKACIJSKA OMREŽJA in PROTOKOLI

- Povezovanje v omrežja in topologije omrežij
- Preklapljanje v omrežjih
- Medmrežja in Internet
- Komunikacijski protokoli: vrste in pomen standardi
- Pomen omrežnih protokolov
- Hierarhični model razslojitve po plasteh, protokolni sklad
- OSI referenčni model
- IP protokolni sklad
- Razvrstitev najpogostejših IP protokolov
- Primerjava OSI in IP modela na zgledu

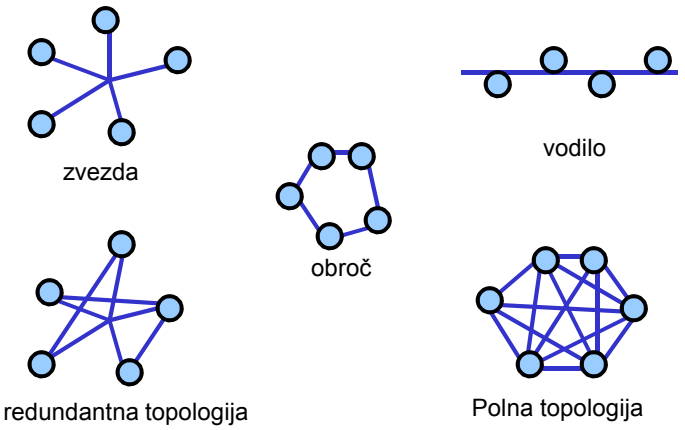


# Omrežja

- Omrežja omogoča poljubno povezovanje med uporabniki.
- Uporabljajo lahko delitev ali zaseganje kapacitet.
- Obstajajo različni načini povezav skozi omrežje:
  - **točka – točka** (point to point),
  - **točka – več točk** (broadcasting, multicasting),
  - **konferenčna zveza**.



# Topologije omrežja

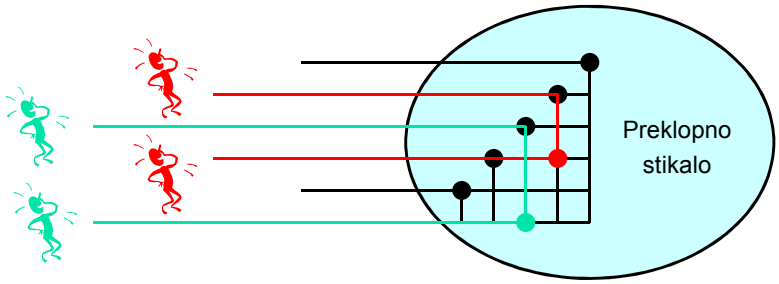





# Preklapljanje v omrežju

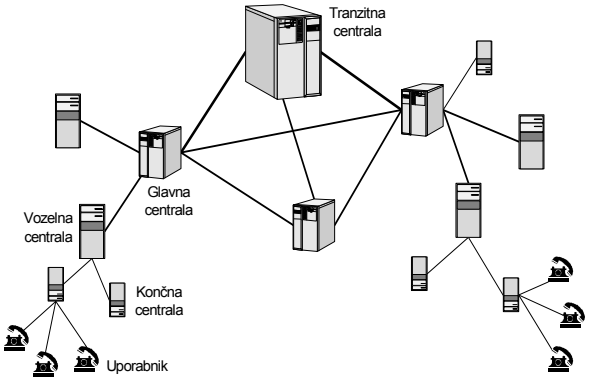
## Tokokrogovno preklapljanje povezav

- V preklopnem omrežju se vzpostavi povezava med uporabniki.
- Povezava med dvema uporabnikoma je lahko vzpostavljena po fizično ločeni liniji ali pa zasedeta fiksen del zmogljivosti medija (kanal).
- Pred začetkom komunikacije je potrebno vzpostaviti zvezo in jo p koncu porušiti.
- Ta način zagotavlja določeno kapaciteto posameznim uporabnikom (QoS) in je zato primeren za prenos v realnem času (telefonsko omrežje).



# Hierarhična struktura preklopnega omrežja

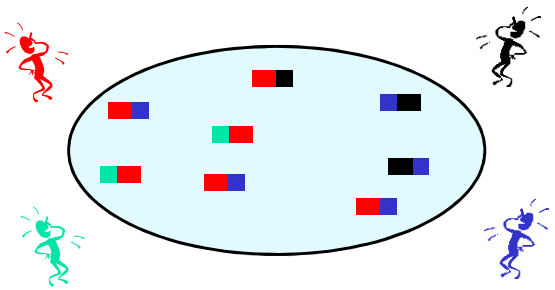
## Telefonsko omrežje:





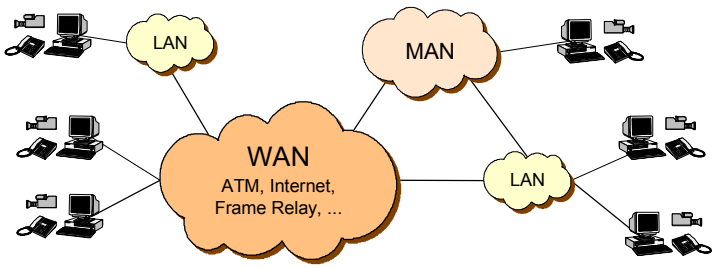

# Paketno omrežje

- V paketnem omrežju se ne vzpostavlja zveze.
- Paketna omrežja lahko delujejo na osnovi zaseganja medija ali delitve prenosne zmogljivosti.
- Med uporabniki potujejo podatki v paketih. Ker ni vzpostavljene zveze, mora biti vsak paket opremljen z naslovom prejemnika, običajno pa tudi z naslovom pošiljatelja.
- Ta način običajno ne zagotavlja določene kapacitete porabnikom, temveč deluje po najboljših možnostih.



# Medmrežje

- Medmrežje (internet) predstavlja povezavo več omrežij.
- Posamezna omrežja lahko slone na enaki ali pa tudi različni tehnologiji.
- Kadar pišemo besedo internet z veliko začetnico mislimo na svetovno omrežje Internet, ki temelji na IP oziroma TCP/IP protokolu.






# citat iz SSKJ

**protokol** -a m (o)

1. uradna in družabna pravila za medsebojne stike uradnih predstavnikov držav: držati se protokola; sprejem predsednika republike, veleposlanika je potekal po protokolu / diplomatski protokol // urad, oddelek ustreznega organa, ki skrbi za izvajanje teh pravil: sprejem je organiziral protokol; delati v protokolu / šef protokola
2. polit. mednarodni dogovor, navadno o določenem vprašanju: delegaciji sta podpisali protokol o gospodarskem sodelovanju; finančni protokol
3. polit. zapisnik o poteku, rezultatih mednarodne konference, sestanka: ker diplomati niso dosegli sporazuma, so objavili samo protokol
4. star. (uradni) zapisnik: protokol zasliševanja / sestaviti protokol; dati na protokol / sodnijski protokol

## KOMUNIKACIJSKI PROTOKOLI

**PROTOKOL** je nabor pravil in postopkov, ki določajo in uravnavajo obliko ter prenos podatkov med dvema uporabnikoma (računalnikoma, aplikacijama).

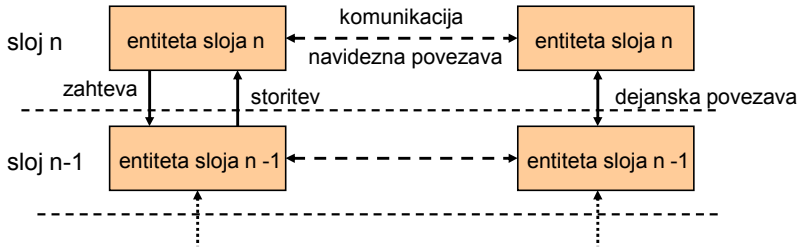


## Protokoli v omrežju

- Za zagotovitev delovanja omrežja so potrebni protokoli.
- Protokole potrebujemo tako pri preklopnih kot pri paketnih omrežjih.
- Pri preklopnih omrežjih so potrebni predvsem v zvezi z vzpostavljanjem in rušenjem zveze (handshaking) med tem, ko so pri paketnih omrežjih nujni pri usmerjanju paketov.
- Protokoli morajo biti standardizirani. Poznamo tako imenovane de iure in de facto standarde.
- De iure (pravni) standardi so standardi, ki jih izdelajo za to pooblaščene standardizacijske organizacije na mednarodnem in nacionalnem nivoju. Za področje telekomunikacij so to predvsem ITU (International Telecommunications Union) , ETSI (European Telecommunications Standards Institute), ki delujejo v okviru mednarodne organizacije ISO (International Standardization Organisation)
- De facto standardi nastajajo izven teh organizacij. V glavnem so akterji pri nastajanju teh standardov proizvajalci opreme in druge neodvisne organizacije.

## Protokolni sklad

- Zaradi boljše interoperabilnosti med različnimi sistemi so omrežni protokoli načrtovani hierarhično in razdeljeni v sloje.
- Nižji sloj nudi višjemu sloju storitev, ki je za višji sloj transparentna.
- V protokolnem skladu ločimo horizontalne protokole med entitetami istoležnih slojev na nasprotnih straneh in vertikalne protokole med entitetami na sosednjih slojih iste strani.
- Le horizontalni protokoli so nujno stvar standardov.

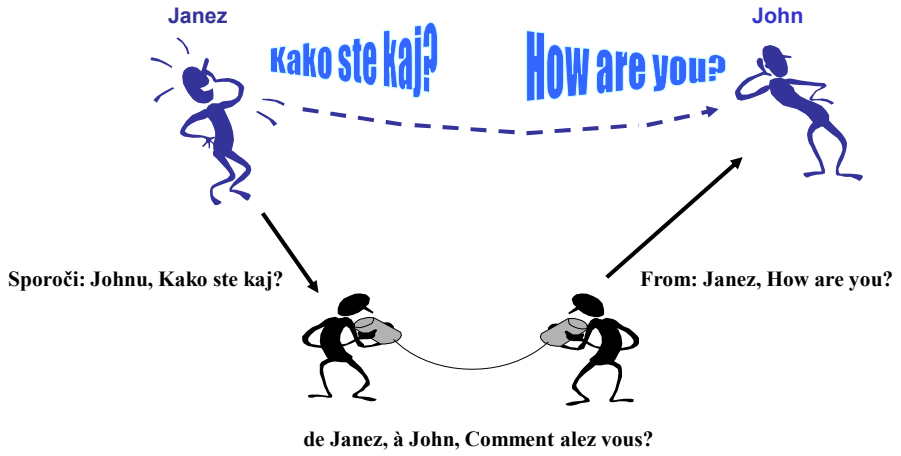





## Komunikacija med protokolnimi plastmi

- Istoležne protokolne plasti med seboj komunicirajo preko navideznih povezav in horizontalnih protokolov.
- Dejanski prenos podatkov poteka vertikalno med plastmi protokolnega sklada preko vertikalnih protokolov.

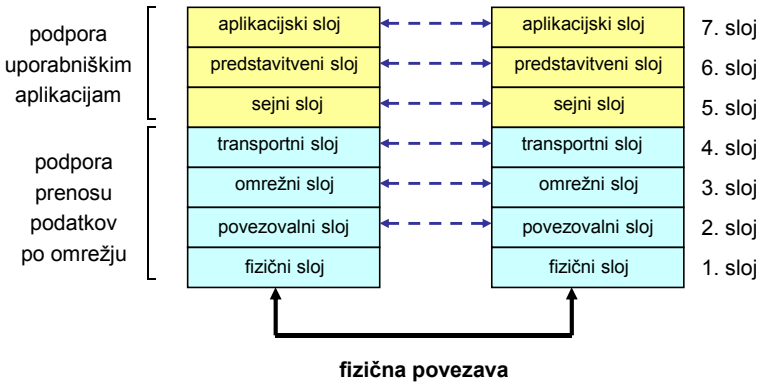
## Primer komunikacije po plasteh



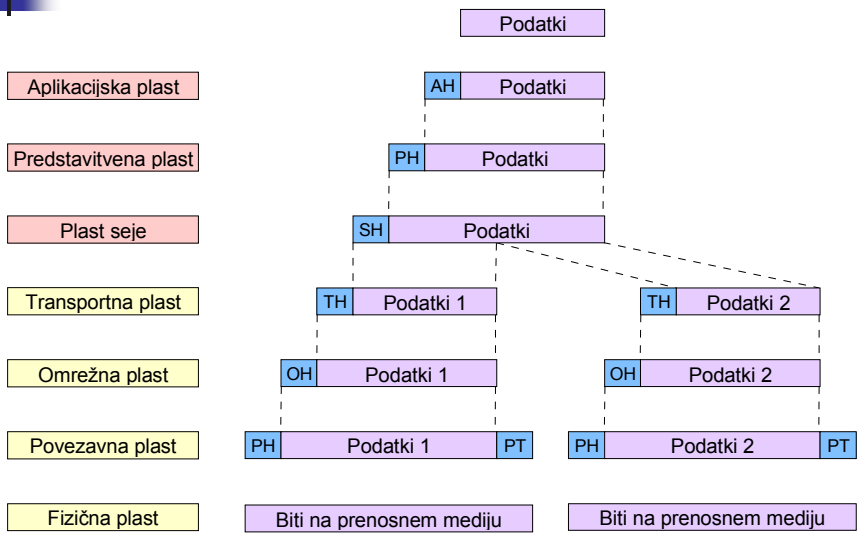



## OSI referenčni model

OSI referenčni model sam po sebi ne predstavlja standarda temveč okvir, v katerem se sprejemajo standardi.



## Dodajanje informacij v protokolnem skladu





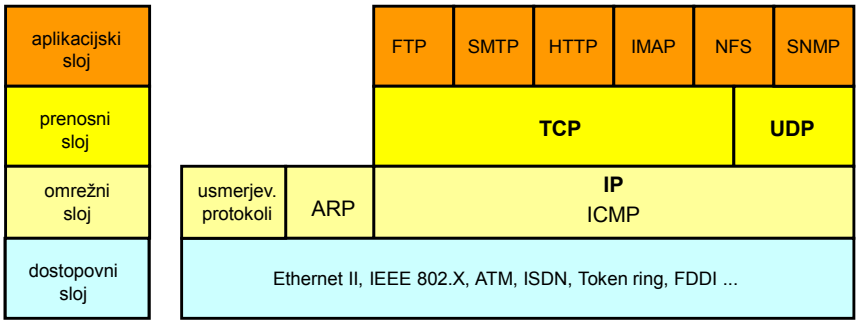

## Primerjava OSI in IP protokolnega sklada

- IP sklad je preprostejši in ima manj plasti.
- OSI sklad je bolj sistematičen in konceptualen.
- OSI sklad je zgolj referenčni model in nikoli ni v celoti zaživel.

| OSI | IP |
|---|---|
| Aplikacijska plast | Aplikacijska plast |
| Predstavitvena plast | Nedefinirano |
| Plast seje | |
| Transportna plast | Transportna plast |
| Omrežna plast | Internetna plast |
| Povezavna plast | Računalnik/omrežje |
| Fizična plast | |

## Protokoli IP sklada

Prikazanih je nekaj najbolj znanih protokolov, jedro celotnega delovanja Interneta pa predstavlja internet protokol IP.

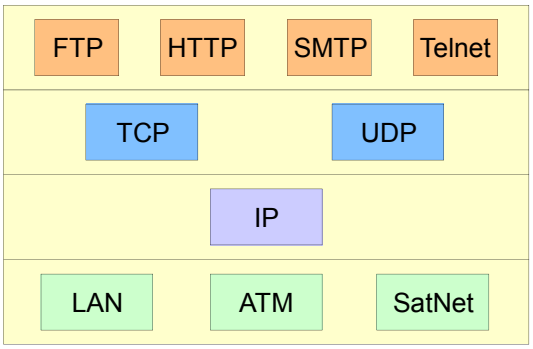





## IP protokolni sklad


- Aplikacijska plast gosti protokole, ki uporabnikom in/ali aplikacijam zagotavljajo neposredne storitve.
- Transportna plast je namenjena transportnim protokolom, ki skrbijo za prenos podatkov med uporabniki. Ti protokoli so lahko povezavni ali nepovezavni.
- Internetna plast ustreza 3. omrežni plasti OSI modela. V njej je realiziran nepovezavno naravnan protokol.
- Plast za povezavo z omrežjem ni definirana ali predpisana. Uporabljajo se različne tehnologije kot so: Ethernet, ATM, Frame Relay in druge. Po OSI modelu zajema 1. in 2. plast.

## Uvrstitev nekaterih najpogostejših IP protokolov




Aplikacijska plast

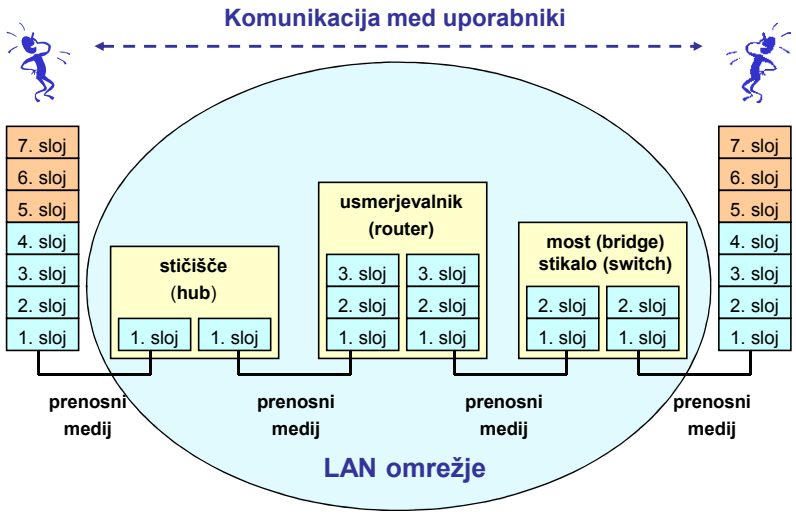
Transportna plast

Internetna plast

Računalnik/omrežje



## Primer delovanja omrežnih naprav po slojih



## TCP

- TCP (Transmission Control Protocol) skrbi za pakiranje podatkov, ki jih dobi od višje ležečega aplikacijskega sloja, v datagrame, ki jih posredujeta IP sloju.
- Transportni sloj skrije omrežno strukturo pred aplikacijo, tako, da aplikaciji ni potrebno skrbeti za razkosanje sporočila v datagrame, oštevilčevanje datagramov, odkrivanje napak in podobno.
- TCP na transportnem sloju zaščiti IP sloj pred potrebo po razdeljevanju datagramov med različne aplikacije. Vsaka aplikacija ima namreč svojo številko vrat, kamor je potrebno dostaviti datagram, ki ji je namenjen.
- TCP tudi za detekcijo napak in ponovno pošiljanje datagramov. Ravno tako skrbi za kontrolo povezave in kontrolo dostave datagramov.



## IP

- IP (Internet protokol) skrbi za dostavo podatkov (datagramov) do določenega IP naslova. IP ne daje nobene garancije o dostavi in je glede tega popolnoma nezanesljiv.
- IP ne daje nobene garancije, da bodo vsi datagrami dostavljeni v celoti po isti poti. Zato lahko prispejo prej oddani datagrami kasneje od tistih, ki so bili oddani za njimi.
- IP mora razumeti delovanje spodnjih slojev omrežja, da lahko pripravi podatke v obliki (dolžina paketov), ki so primerni za uporabljeni fizični sloj.
- Ravno tako mora omogočiti dostavo v skladu z načinom naslavljanja v lokalnih omrežjih, ki ne uporabljajo IP naslova (MAC naslov v Ethernetu, DLCI naslov v Frame Relayu, itd.)

## TCP/IP in OSI

Uvrstitev TCP/IP protokolnega sklada v OSI model ni enoumna in jo različni avtorji uvrščajo različno. V resnici ni natančne preslikave med OSI sloji in sloji TCP/IP protokolnega sklada.

<table>
<tr><th>OSI model</th><th>TCP/IP</th></tr>
<tr><td>aplikacijski sloj</td><td rowspan="2">aplikacijski sloj</td></tr>
<tr><td>predstavitveni sloj</td></tr>
<tr><td>sejni sloj</td><td rowspan="2">prenosni sloj</td></tr>
<tr><td>prenosni sloj</td></tr>
<tr><td>omrežni sloj</td><td>omrežni sloj</td></tr>
<tr><td>povezovalni sloj</td><td rowspan="2">dostopovni sloj</td></tr>
<tr><td>fizični sloj</td></tr>
</table>



## Razvrstitev protokolov po plasteh (2)

1. fizični nivo povezav: po optiki, žicah, brezžično
2. povezava (data link)
   1. Ethernet protokol določa pravila za korekcijo napak pri prenosu in dostop v LAN.
   2. Tudi blokovno posredovanje FR je protokol drugega sloja.
3. omrežje (network)
   1. IP protokol omogoča usmerjanje paketov skozi omrežje spomočjo internetnih naslovov.
4. transport (transport)
   1. protokoli za usmerjanje prometa glede na vsebino.
   2. diferenciacija po vsebini omogoča boljšo kakovost storitve.
   3. TCP protokol je protokol 4. plasti.
5. seja (session)
   1. šifriranje z namenom varovanja tajnosti komunikacije poteka na 5. plasti
   2. H323 paketiranje govora poteka na 5. plasti,
6. predstavitev (presentation)
   1. kontrolira izgled strani na uporabnikovem ekranu. Jezik HTML je standard šestega sloja.
7. aplikacija (application)
   1. na aplikacijskem nivoju delujejo uporabniške aplikacije. Protokol za prenos hiperteksta HTTP je protokol 7. plasti.

## 9. VARNOST KOMUNIKACIJ

- Elektronski in tiskani zapisi in dokumenti
- Tajnost , verodostojnost, avtentičnost in neovrgljivost
- Šifriranje sporočil
  - Zgodovina šifriranja
  - Simetrično in asimetrično šifriranje
- Digitalni podpis
  - Pomen zgoščevalne funkcije
  - Uporaba asimetričnega šifriranja
- Digitalna potrdila



## Elektronski in tiskani dokumenti

- Skoraj vsi dokumenti nastajajo s pomočjo računalnika.
- Elektronski dokument ima veliko prednosti:
  - kadarkoli ga lahko ponovno natisnemo
  - lahko ga tudi spreminjamo: spremenimo naslovnika, datum...
- Zakaj se potem velik del dokumentov še vedno tiska na papir ?
- Vprašljiva je originalnost elektronskega dokumenta
- Tiskani dokument vsebuje lastnoročne podpise in časovne žige
- Elektronski dokument brez varnostnih mehanizmov ni pravno veljaven:
  - ne more služiti za arhiv ali kot pogodba

## Razvoj izmenjave elektronskih dokumentov

- dokument natisnemo na papir in po pošti pošljemo naslovniku
- dokument pošljemo iz računalnika direktno na telefaks naslovnika
- dokument pošljemo v elektronski obliki na fizičnem mediju (kurir, pošta, DHL..)
- dokument posredujemo v elektronski obliki na primer preko elektronske pošte

- zadnji način je od vseh naštetih najbolj učinkovit vendar hkrati tudi najbolj ranljiv !



## Zaupni dokumenti in zasebnost komunikacije

- Zaupni dokument je namenjem samo naslovniku, zato želimo preprečiti vpogled tretje osebe.
- Govorimo o zasebnosti ali tajnosti komunikacije.
- Če zaupni dokument pride v napačne roke je zasebnost komunikacije izgubljena.
- Verjetnost takšnega dogodka je omejena s stopnjo varovanja zasebnosti. Zelo zaupne dokumente varujemo z najvišjo možno stopnjo varovanja zasebnosti (tajnosti).
- Pri pismu je zasebnost udeležencev v komunikaciji slabo varovana z vlaganjem tiskanega dokumenta v ovojnico. Zaupnost tiskanega dokumenta je lahko posebej označena, kar pa lahko še dodatno pritegne pozornost.

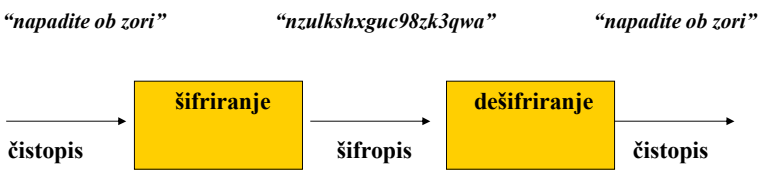
## Zagotavljanje celovitosti sporočil

- zasebnost ali tajnost:
  - Ali je vsebina sporočila res dostopna samo naslovniku ?
- verodostojnost :
  - Ali je sprejeto sporočilo res enako oddanemu sporočilu ?
- avtentičnost zagotavlja izjavljeno identiteto pošiljatelja:
  - Ali nam sporočilo res pošilja predstavljeni pošiljatelj ?
- neovrgljivost:
  - Ali lahko pošiljatelj zanika avtorstvo sporočila ?



## Šifriranje dokumentov

- Varovanje zasebnosti zagotovimo s šifriranjem dokumentov tako, da velja:
  - iz šifriranega dokumenta ni mogoče razbrati vsebine in
  - samo naslovnik zna dešifrirati dokument.
- Primer šifriranja teksta:



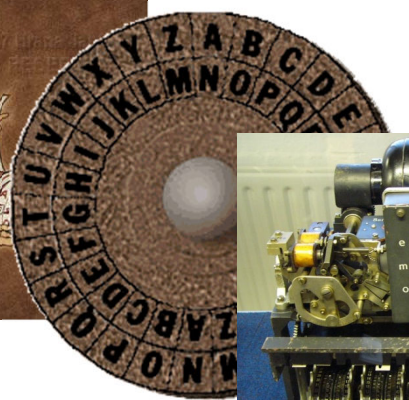
## Zgodovina šifriranja sporočil

- Veda o šifriranju (kriptologija) je bila zelo dolgo na seznamu najstrožje varovanih skrivnosti
  - Grki: kryptos "skrite" , logos "besede", angl: cryptology
  - Cezarjev postopek šifriranja : CESARUS->FHVDUAV
  - Nemški šifrirni stroj iz II. svetovne vojne: Enigma
- Javno uporabo kriptografije je omogočila iznajdba asimetričnega postopka šifriranja pred približno 30. leti
  - junija 1991 je Philip Zimerman objavil programski paket za varno izmenjavo sporočil PGP (Prety Good Privacy)
  - Danes uporabljamo vrsto standardnih postopkov šifriranja sporočil v privatnih in poslovnih komunikacijah.

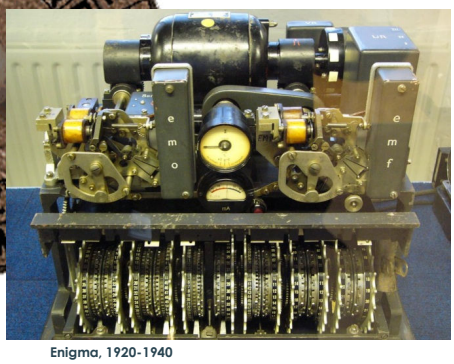


## Varnost je včasih temeljila na tajnosti postopka:

Sparta, 500 p.n.š.



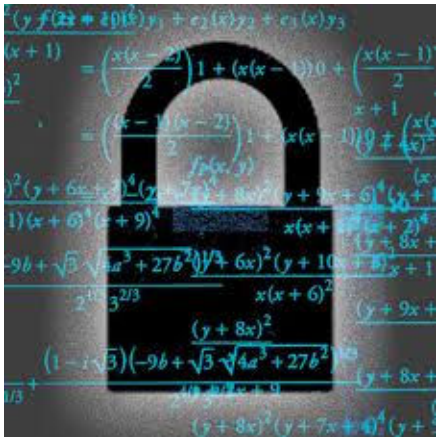

Julij Cezar, 100 p.n.š.



Enigma, 1920-1940

## Moderno šifriranje je bolj varno:

- šifrirni **algoritem je javen**, varnost pa temelji na tajnosti ključev.
- **namen** šifriranja, varnostni vidiki:
  - tajnost
  - verodostojnost
  - avtentičnost
  - neovrgljivost
- šifrirni **algoritmi**:
  - DES, IDEA, **AES**
  - **RSA**, DH
  - MD5, **SHA**-1,..SHA-3



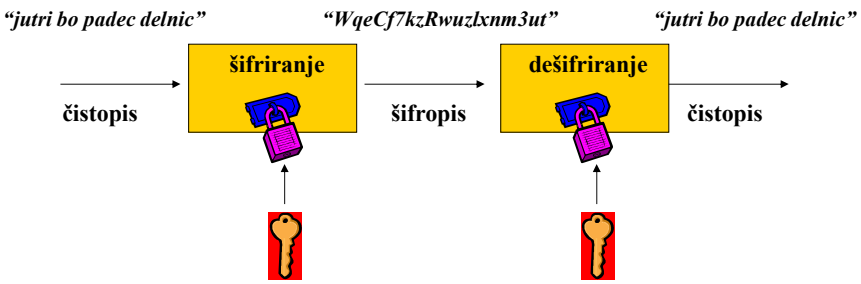


## Šifrirni postopek

- Lastnosti dobrega šifrirnega postopka:
  - Zasebnost ne sloni na tajnosti postopka pač pa na tajnosti ključa za dešifriranje.
  - Postopek šifriranja mora biti izvedljiv na računalniku v realnem času.
  - Postopek dešifriranja mora izvedljiv na računalniku v realnem času za tistega, ki pozna dešifrirni ključ.
  - Postopek dešifriranja ne sme biti izvedljiv v realnem času za napadalca, ki ne pozna ključa, čeprav razpolaga z zelo zmogljivim računalnikom.
- Glede na smernost šifrirnega postopka ločimo:
  - Simetrično šifriranje (dvosmerno šifriranje)
  - Asimetrično šifriranje (enosmerno šifriranje)

## Simetrično šifriranje

- Za šifriranje in dešifriranje uporabimo enak tajni ključ:

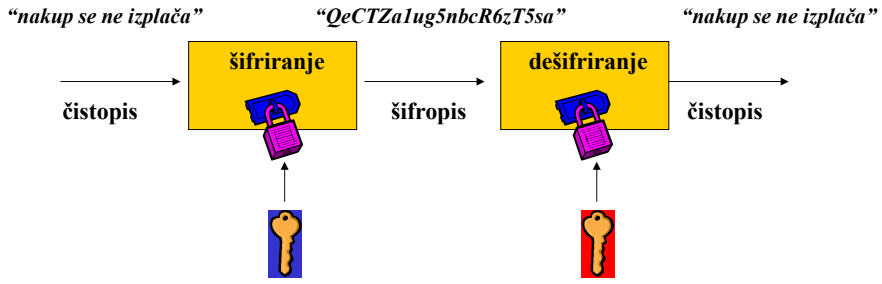



- **Primer simetričnih šifrirnih algoritmov: DES, AES**



## Asimetrično šifriranje

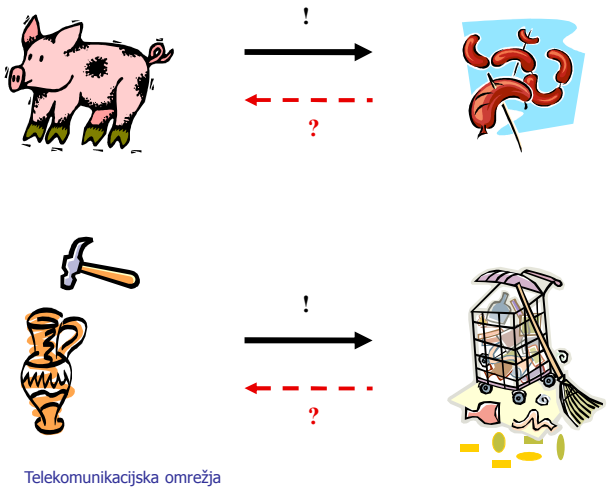
- Ključa za šifriranje in dešifriranje nista enaka:




- **Pošiljatelj šifrira sporočilo z javnim ključem prejemnika.**
- **Prejemnik dešifrira sporočilo z zasebnim tajnim ključem.**
- **Primer asimetričnih šifrirnih algoritmov: RSA, ElGamal...**

## "Enosmerne funkcije" ☺☺

- Preslikava v nasprotni smeri je zelo težavna ali pa praktično ni mogoča:






## Mešani postopek šifriranja

- Asimetrični šifrirni postopek zahteva mnogo več računanja kot simetrični šifrirni postopek. V praktičnih sistemih se zato uporablja mešani postopek šifriranja:
  - Asimetrični postopek uporabimo za izmenjavo začasnega sejnega ključa.
  - Po simetričnem postopku s sejnim ključem šifriramo in dešifriramo sporočilo.
- Pošiljatelj pošlje simetrično šifrirano sporočilo in zraven še asimetrično šifriran ključ, s katerim je bilo sporočilo šifrirano:
  - Pošiljatelj naključno generira sejni ključ in z njim šifrira sporočilo.
  - Ključ s katerim je sporočilo šifrirano se šifrira z javnim ključem naslovnika.
- Prejemnik prejme šifrirano sporočilo in šifriran sejni ključ.
  - Prejemnik dešifrira sejni ključ s svojim privatnim tajnim ključem.
  - Prejemnik na osnovi sejnega ključa dešifrira sporočilo.

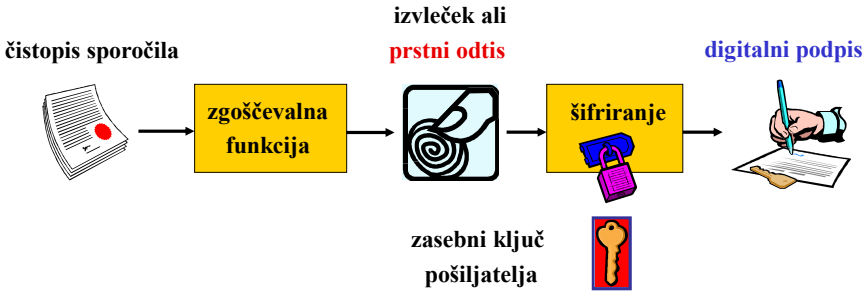
## Verodostojnost, avtentičnost in neovrgljivost

- Elektronski prstni odtis dokumenta
- Digitalni podpis
- Upravljanje s ključi
- Digitalno potrdilo



## Digitalni podpis

- Digitalni podpis je s tajnim ključem šifrirani prstni odtis sporočila:




- **Zgoščevalna funkcija je enosmerna funkcija in vsaka sprememba čistopisa spremeni tudi prstni odtis sporočila.**
- **Napadalec bi lahko spremenil sporočilo in dodal nov prstni odtis !**
- **Pošiljatelj zaščiti prstni odtis s šifriranjem!**

## Zgoščevalna funkcija

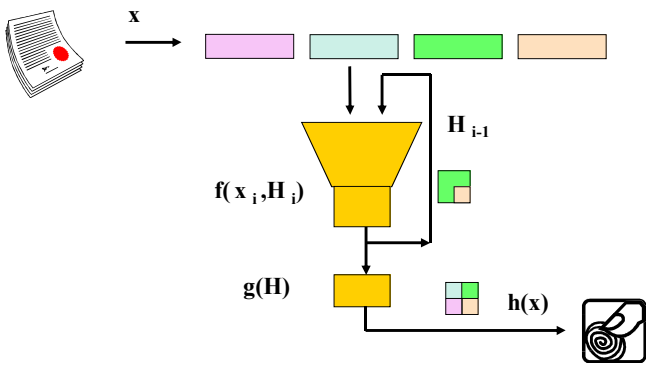
- Zgoščevalna funkcija (hash function) preslika poljubno dolgo sporočilo v blok podatkov končne dolžine. Izvleček (digest) imenujemo tudi prstni odtis (digital fingerprint) sporočila.
- Zgoščevalna funkcija je enosmerna funkcija.
- Verjetnost, da najdemo sporočilo z enakim prstnim odtisom mora biti zelo majhna **Pr(** $h(x_1)=h(x_2)$ **) --> 0** .


**čistopis** **izvleček ali prstni odtis**

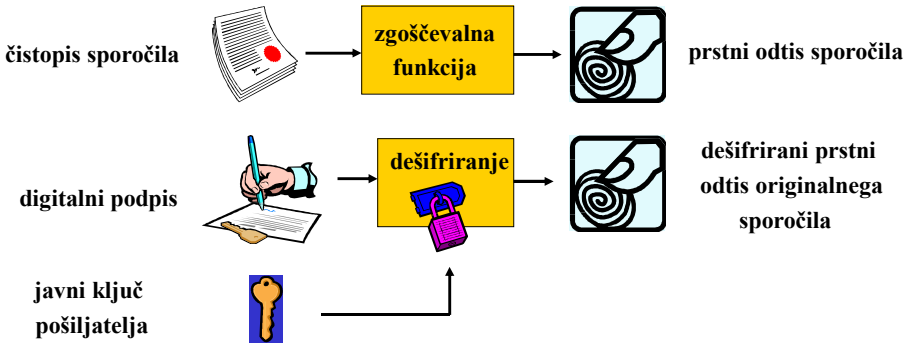


## Model iteracijske zgoščevalne funkcije

- Sporočilo razdelimo na bloke dogovorjene dolžine.
- Postopek zgoščevanja ponavljamo in vsakič uporabimo izvleček predhodnih blokov.



## Preverjanje digitalnega podpisa




- Prejemnik preveri ujemanje prstnih odtisov in če sta enaka
  - je sporočilo verodostojno,
  - potrjena je identiteta pošiljatelja in
  - pošiljatelj ne more zanikati sporočila.



## Namen digitalnega podpisa

- Digitalni podpis dodajamo nešifriranemu sporočilu in zato ne zagotavlja tajnosti komunikacije.
- Pošiljatelj z digitalnim podpisom zagotovi:
  - verodostojnost sporočila,
  - potrjuje svojo identiteto in s tem
  - sprejme tudi odgovornost za sporočilo.
- Prejemnik lahko hkrati preveri verodostojnost in avtentičnost:
  - Ali je sprejeto sporočilo res enako oddanemu sporočilu ?
  - Ali nam sporočilo res pošilja predstavljeni pošiljatelj ?
- Če prejemnik potrdi verodostojnost sporočila in avtentičnost pošiljatelja, potem tudi pošiljatelj ne more sporočila zanikati:
  - Če se prstna odtisa ujemata, potem sporočilo ni bilo spremenjeno in podpisal ga je lahko le pošiljatelj, ki ima edini pravi zasebni ključ.
- Digitalni podpis omogoča zagotavljanje verodostojnosti, avtentičnosti in neovrgljivosti sporočil.

## Uporaba zasebnih in javnih ključev

- Digitalni podpis temelji na asimetričnem šifrirnem postopku, ki uporablja parov imetnikovih ključev: javni ključ + zasebni ključ

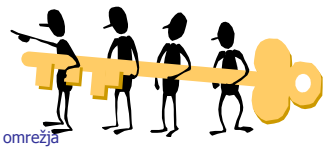
- Vsak uporabnik nosi odgovornost za uporabo in varovanje zasebnega ključa. Dostop do tajnega ključa varujemo z dolgim geslom, ki ga imenujemo fraza. Uporabnik ne sme zaupati nikomur svojega zasebnega ključa. Če to stori, potem nosi tudi vso odgovornost za zlorabe.

- Javni ključ mora biti vsakomur dostopen z jamstvom, da pripada navedenemu uporabniku. V nasprotnem primeru lahko pride do problemov:
  - Problem lažne identitete: napadalec podtakne lažni javni ključ in dešifrira vsa prestrežena sporočila.
  - Problem zanikanja identitete: pošiljatelj zanika lastno sporočilo.



## Upravljanje s ključi

- Javni ključ mora nositi garancijo, da res pripada navedenemu uporabniku. Overjanje javnih ključov opravlja posebna služba (podobno notarju), ki skrbi tudi za upravljanje s ključi.
- Urad za overjanje (**CA**=Certification Authority) potrjuje verodostojnost javnih ključev z digitalnim podpisom odgovorne osebe. Imetnik javnega ključa se mora ob registraciji identificirati in s tem prevzema odgovornost za uporabo zasebnega ključa. Identifikacijo izvrši uradna oseba (RA=Registration Authority).
- Na zahteve imetnikov opravlja CA tudi razveljavitve javnih ključev. Potreba po preklicu javnega ključa nastopi v primeru izgube tajnosti zasebnega ključa.



## Digitalno potrdilo

- Digitalno potrdilo (digital certificate) je kopija javnega ključa, ki je overjena od tretje osebe ali institucije.
- Imetnik javnega ključa se mora ob registraciji identificirati in s tem prevzema tudi odgovornost za uporabo zasebnega ključa. Identifikacijo izvrši uradna oseba RA (Registration Authority).
- Urad za overjanje potrdil CA (Certification Authority) je nevtralna organizacija, ki ji uporabniki zaupajo.
- Upravljanje z javnimi ključi ne zajema samo shranjevanje digitalnih potrdil na strežniku, pač pa celoten postopek posrednih overjanj izdajateljev potrdil, razveljavitve javnih ključev itn.
- Infrastruktura javnih ključev PKI (Public Key Infrastructure) določa protokole in storitve pri upravljanju z javnimi ključi.

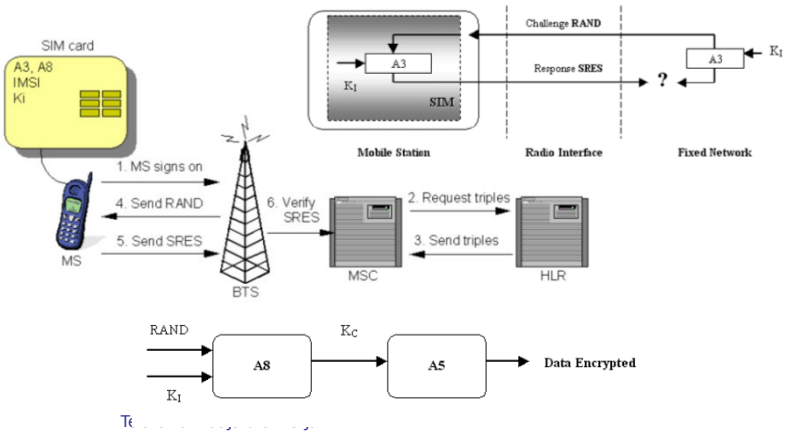


## Format digitalnega potrdila

- Digitalno potrdilo vsebuje poleg javnega ključa tudi množico identifikacijskih podatkov uporabnika in izdajatelja potrdila.
- Najbolj znana formata sta X-509 in PGP:
  - ITU-T mednarodni standard predpisuje X-509 format digitalnih potrdil. V opisu je določeno katere informacije so vsebovane v poljih potrdila in kakšen je njihov format zapisa.
    - X-509 v1 1988, osem polj
    - X-509 v2 1993, + dodani dve identifikacijski polji - 10 polj
    - X-509 v3 1996, + dodano polje za razširitve
  - PGP format digitalnega potrdila se uporablja v programskem paketu za varno izmenjavo podatkov PGP (Pretty Good Privacy). PGP je v začetku devetdesetih let ustvaril Phil Zimmerm

# Varnost mobilnih komunikacij – primer GSM

- tajni ključ *Ki* je shranjen na SIM kartici in varovan z dostopovnimi kodami (PIN, PUK) in se ne prenaša po radijskem kanalu
- identiteta uporabnika je v komunikaciji prikrita: TMSI - IMSI
- avtentikacija mobilne postaje s strani omrežja
- komunikacija na radijskem delu zveze je šifrirana

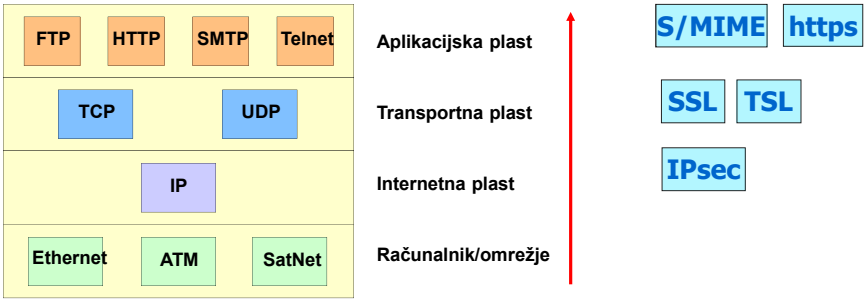





# Varnostni protokoli na Internetu

**osnovni internetni protokoli:**

**dodani so varnostni protokoli delujejo na različnih plasteh:**

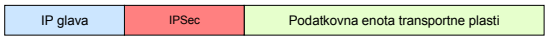


## IPsec

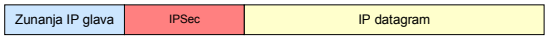
IP Security (IPsec) omogoča varovanje na omrežni plasti.

IPsec deluje na dva možna načina:

- IPsec transportni način ohranja glave IP paketov nespremenjene, šifrira se samo vsebina paketa
- IPsec tunelski način dodaja novo glavo IP paketom, stara glava in vsebino paketa pa se prenašata v šifrirani obliki. Varovana komunikacija poteka med parom prehodov (gateway to gateway), ki jih naslavljajo dodane glave IP paketov.




**Transportni način**



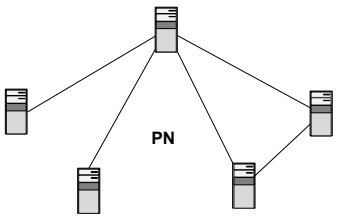

**Tunelski način**

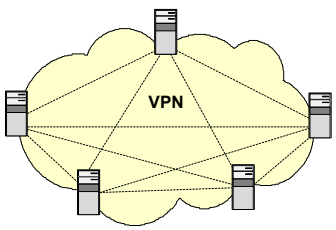


## VPN

VPN je navidezno zasebno omrežje (Virtual Private Network)

- Povezave v navideznih zasebnih omrežjih so dinamične in navidezne. Potekajo kot tuneli po javni TK infrastrukturi.
- Varno komunikacijo zagotavlja tunelski protokol, na primer IPsec.



## Varna komunikacija na spletu

- https ni poseben protokol, pač pa pomeni da HTTP poteka preko varne transportne plasti: **SSL**.
- SSL (Secure Socket Layer) je razvil Netscape za varno komunikacijo med spletnim klientom in strežnikom. SSL podpira preverjanje identitete strežnika. V komunikaciji se za vsako sejo ustvari varni kanal. SSL zagotavlja varno komunikacijo na transportni plasti. TLS (Transport Layer Security) je standardizirana (IETF) zamenjava za SSL. TLS_v1 in SSL_v3 sta zelo podobna, vendar nista interoperabilna.
- S/MIME (Secure/Multipurpose Internet Mail Extentions) je varna izboljšava standarda za format elektronske pošte MIME.
  - MIME je protokol za izmenjavo podatkov, ki niso v ASCII formatu. MIME določa nabor funkcij za pretvorbo priponk v ASCII in obratno.
  - S/MIME uporablja X-509 infrastrukturo javnih ključev

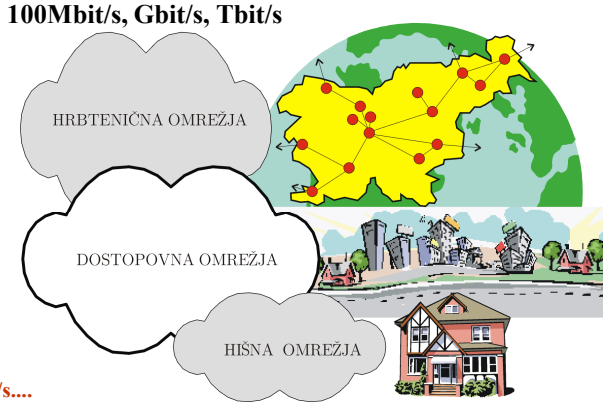


## 10. VRVIČNA DOSTOPOVNA OMREŽJA

- Uporaba razpoložljivega žična omrežja:
  - telefonsko omrežje
  - omrežje kabelske televizije
  - nizkonapetostno energetsko omrežje
- Posodobitve žičnih omrežij z dodajanjem optičnih vodov:
  - hibridno omrežje - HFC, HFT
  - optično vlakno do vozlišča - FTTN
  - gradnja novega v celoti optičnega omrežja do doma - FTTH
- Vizije razvoja

# Problem prenosnih kapacitet

**>> 100Mbit/s, Gbit/s, Tbit/s**




**POTS, V.92: 56kbit/s**
**ISDN: 128kbit/s**

---

**ADSL: 4(0,8) Mbit/s**
**CATV: 5(0,5) Mbit/s**

---

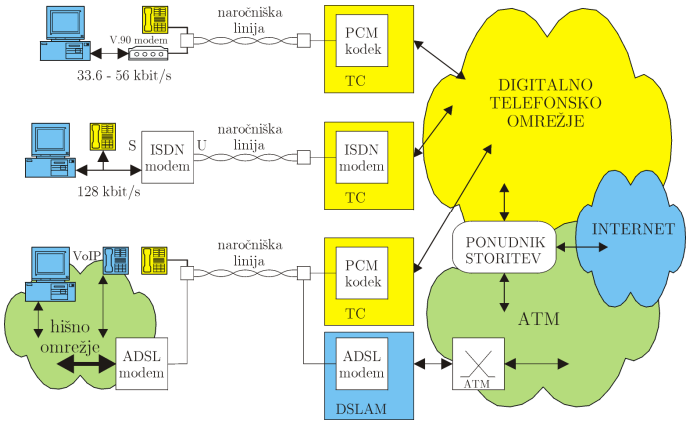
**VDSL: do 100Mbit/s**
**FTTH: 100Mbit/s , 1Gbit/s....**

**100Mbit/s ..**



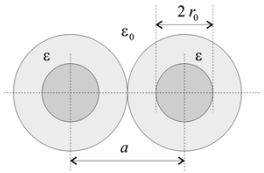
# Telefonsko omrežje

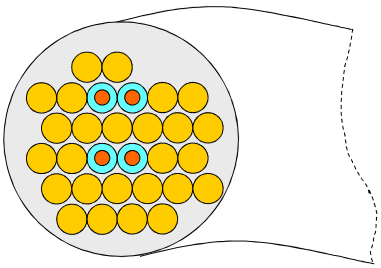
**Začetki digitalizacije naročniškega omrežja – DSL (Digital Subscriber Loop):**



## Značilnosti prenosnega medija

- Telefonsko omrežje je bilo načrtovano za prenos analognega govornega signala v frekvenčnem območju od 300 do 3400Hz. Za hitri znakovni prenos potrebujemo bistveno širši frekvenčni pas!
- Največja motnja pri komunikaciji je presluh med vodi znotraj istega kabla.



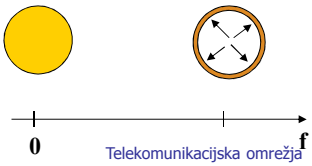



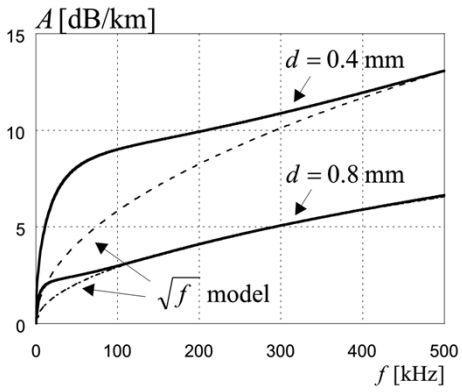


## Slabljenje

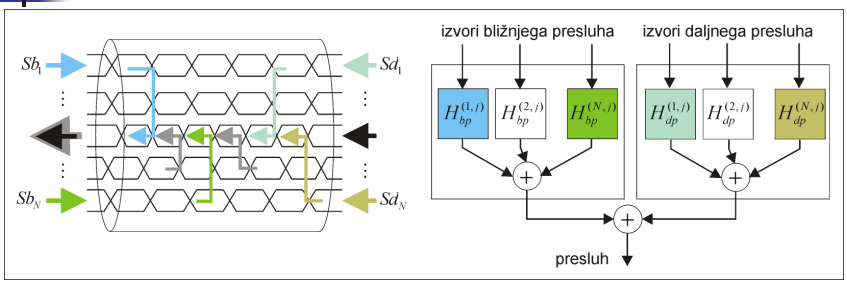
- Kožni pojav ima prevladujoč vpliv na potek slabljenja: pri visokih frekvencah teče električni tok samo še po površini vodnika.
- Slabljenje signalav kablu narašča približno s kvadratnim korenom frekvence:

**učinek kožnega pojava:**



## Presluh



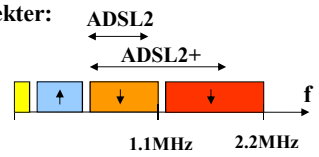

- Zanima nas moč vsote preslušnih signalov iz množice sosednih izvorov na bližnjem in daljnem kraju.
  - bližnji presluh NEXT (Near End Crosstalk)
  - daljni presluh FEXT (Far End Crosstalk)



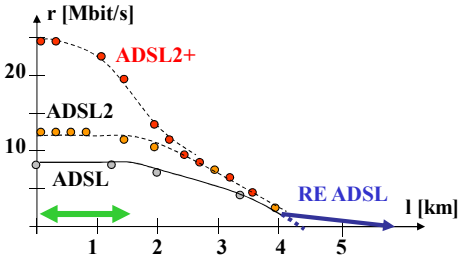
## ADSL standardi

- ADSL (1999)
  - G.992.1 G.dmt 32kbit/s -> 8Mbit/s
  - G.992.2 G.lite
- ADSL2 (2002)
  - G.992.3 G.dmt.bis
  - G.992.4 G.lite.bis
- ADSL2+ (2003)
  - G.992.5 do 24Mbit/s
- Annex
  - A: ADSL+POTS
  - B, J: ADSL+ISDN
  - L: (G.992.3) RE ADSL (Reach Extended ADSL)

spekter:

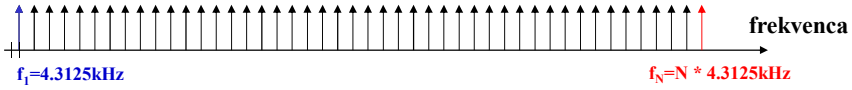



informacijski pretok:

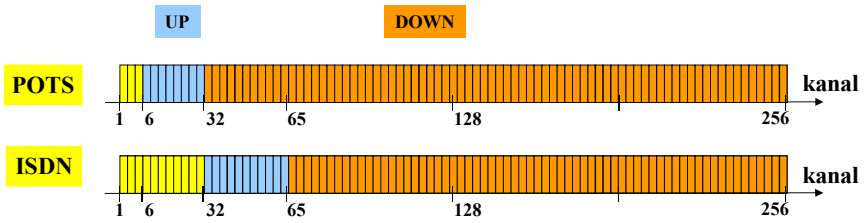


## ADSL DMT kanali

- DMT modem generira N različnih frekvenc v razmiku 4.3125kHz:




- **uporaba in razdelitev kanalov za ADSL, ADSL2 (annex A in B):**

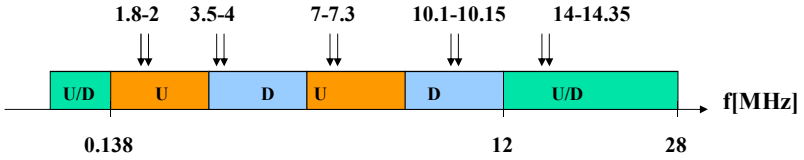





## VDSL

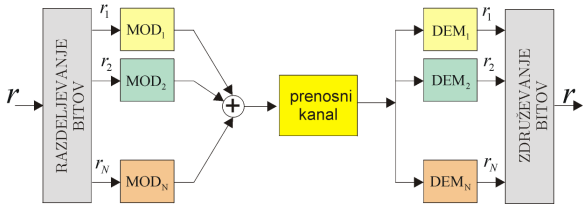
Zelo hitri prenos po bakreni parici na kratkih razdaljah:

- VDSL G.993.1 (2004), frekvenčno območje do 12MHz
- VDSL2 (ITU 2005), frekvenčno območje do 30Mhz
- VDSL DMT modem ima enak razmik med toni kot ADSL
- obstajajo različni načrti uporabe frekvenčnega pasu:
  - plan 997, plan 998,..

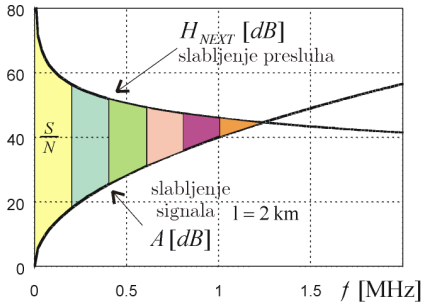


## Prilagajanje razmeram na kanalu

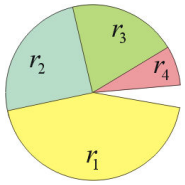
**MCM modem: (DMT, OFDM)**




**razmere za primer naročniškega voda v okolju NEXT:**

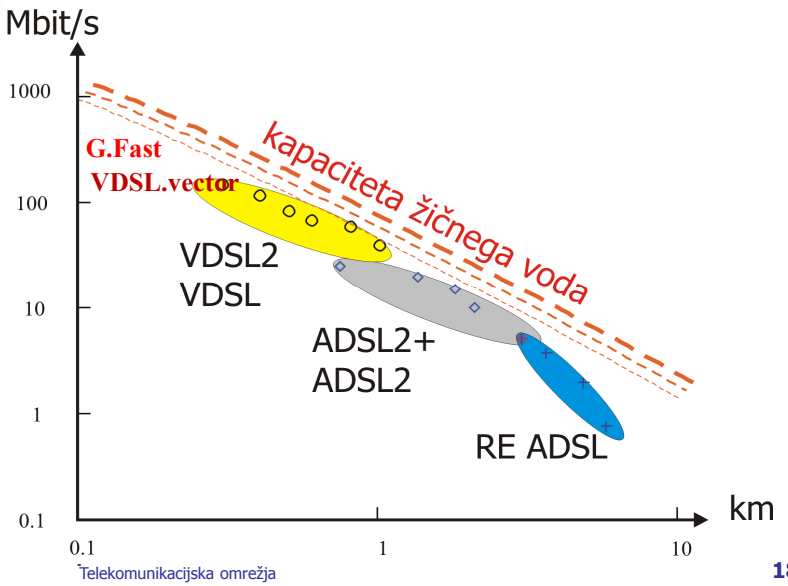



**razdelitev prenosne hitrosti po kanalih:**

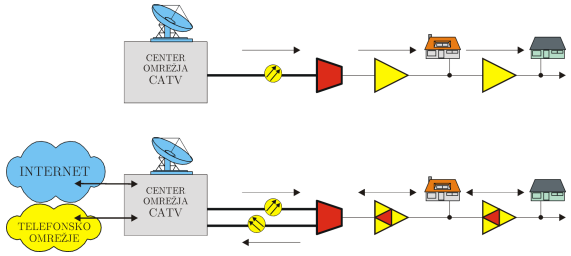





## Pretok in doseg xDSL



## Omrežje kabelske televizije




| smer | pretok | frekvenca | B | modulacija |
|---|---|---|---|---|
| od uporabika (UPLINK) | 0,32-5 Mbit/s<br>0,64-10 Mbit/s | 5-42 MHz | 200kHz-3200kHz | QPSK, 16 QAM |
| proti uporabniku (DOWNLINK) | 30 Mbit/s<br>43 Mbit/s | 88-860 MHz | 8 MHz | 64 QAM<br>256 QAM |

| DOCSIS | Downstream | Upstream |
|---|---|---|
| 1.x | 42.88 (38) Mbit/s | 10.24 (9) Mbit/s |
| Euro | 57.20 (51) Mbit/s | 10.24 (9) Mbit/s |
| 2.0 | 42.88 (38) Mbit/s | 30.72 (27) Mbit/s |
| 3.0 | +480 Mbit/s | +120 Mbit/s |

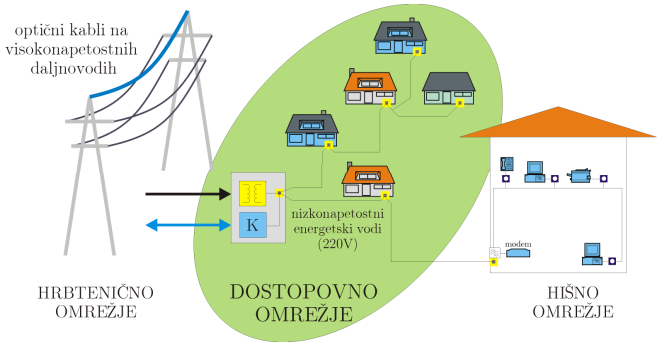
**Uporabniki si delijo prenosne kapacitete kanalov !**



## Sodobno kabelsko omrežje

- kabelsko omrežje je hibridno
  - uporablja dva prenosna medija – HFC
  - prenaša analogne in digitalne kanale
- kabelskih modemi delujejo po specifikacijah EuroDOCSIS (Data Over Cable Service Interface Specification) verzije DOCSIS1.0, 1.1, 2.0,3.0
- definirana je arhitektura in nabor specifikacij vmesnikov za multimedijske storitve preko HFC paketnega omrežja – EuroPacketCable

## Elektroenergetsko omrežje ?

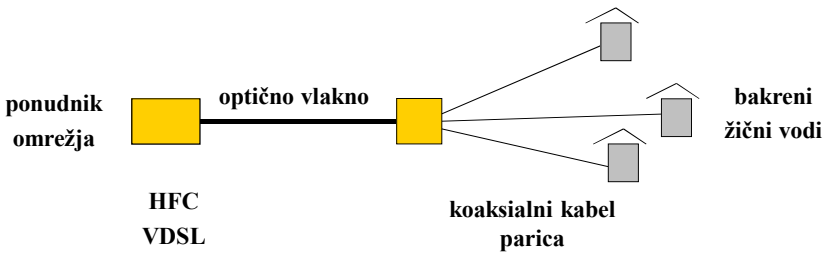



- **frekvenčni pas za PLC širokopasovne komunikacije: 1Mhz-30Mhz**
- **EU IST OPERA (Open PLC European Research Alliance), jan. 2004-> 2008**
- **PLC Forum napovedi: 2-20Mbit/s, doseg do 500 metrov**
- **Ascom Powerline: pretok do 4,5 Mbit/s , doseg ~ 300 metrov**



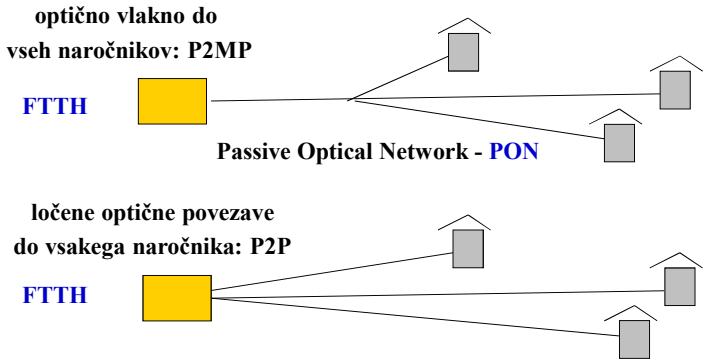
## Hibridno omrežje

- razdalje bakrenih vodov zmanjšamo z dodajanjem optičnih vodov:
  - kabelsko omrežje HFC (200-500/vlakno)
  - naročniško omrežje HFT-VDSL (30-100/vlakno)



## Optika do doma, zgradbe

- Bakrene vode v celoti nadomestimo z optičnimi vlakni. Ločimo dve osnovni topologiji FTTH:



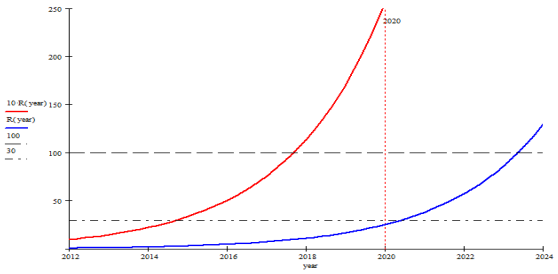



## Digitalna Agenda v EU (DAE)

- osnovni širokopasovni dostop za vse prebivalce v EU do 2013:
  - *basic* broadband= (>144kbit/s ali 2Mbit/s ali 4/1 Mbit/s ..)?
- hitri širokopasovni dostop v omrežjih naslednje generacije (NGA) ima bolj jasno definiran cilj:
  - najmanj 30Mbit/s , 100% razpoložljivost,
  - 100Mbit/s ali več , 50% razpoložljivost.
- napovedi članic EU:
  - Nemčija: 50Mbit/s, 75%, do 2014,
  - Finska: 100Mbit/s, 100% do 2015,
  - U.K.: 25Mbit/s, 90% do 2015,
  - Avstrija, Danska: 100Mbit/s, 100%, do leta 2020,
  - Švedska:100Mbit/s, 90% do 2020,
  - Francija: 100Mbit/s, 100% do 2025,

## Eksponentna rast prenosnih kapacitet ?

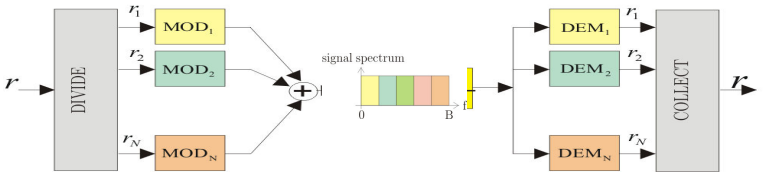
- Nielsen: 50% letna rast potreb po kapaciteti najbolj zahtevnih uporabnikov.
- ekstrapolacija za naslednjih 10 let za različni izhodišči v letu 2012:
  - 1Mbit/s
  - 10Mbit/s




- Rešitev so optična omrežja FTTH . Še vedno nizek povprečni delež FTTH v EU. Razloga sta visoka cena in počasna izgradnja. Japonska je potrebovala 10 let za doseganje 50% pokritosti.
- Za dosego ciljev DAE potrebujemo tudi alternativne vendar začasne tehnologije:
  - VDSL.vector , G.Fast

## Od ADSL, VDSL do VDSL.vector in G.Fast

- Osnova DSL sistemov je učinkovit in spektralno prilagodljiv prenosni sistem, ki uporablja modulacijo z več nosilci
  - DMT, (US,DS), N * 4.3125kHz,
  - omogoča dinamično upravljanje spektra DSM,

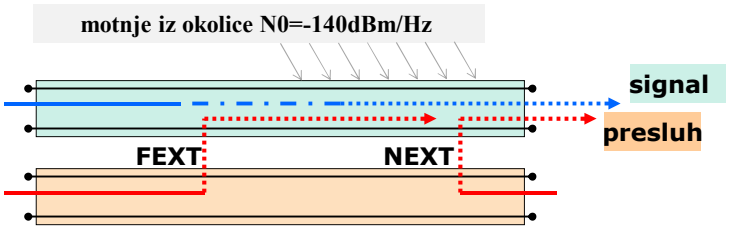



- **G.Fast** , Ω-DSL , ITU standard v letu 2014
  - DMT: 2048 * 51.75kHz, $b_{max}$=12, DS/US=(90/10, 50/50, 10/90)
  - $f_{sp}$=(2.2MHz, 8.5MHz, 17,7MHz), B>100MHz

  Prenosne kapacitete in doseg:
  - 500Mbit/s , l<100m
  - 250Mbit/s, l<200m

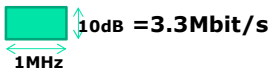
# Motnje v ADSL in VDSL sistemih

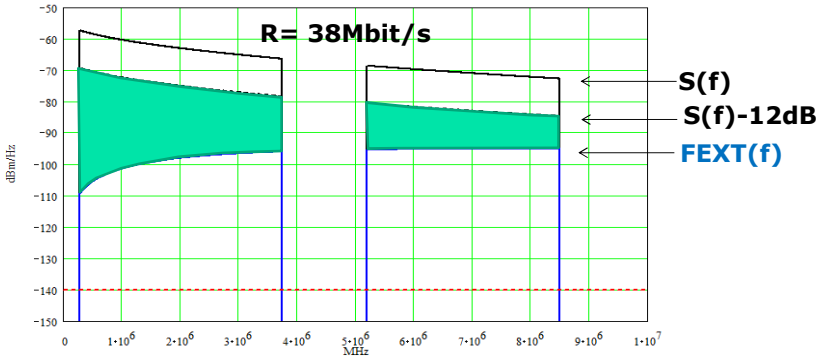
- Bližnji presluh NEXT nima vpliva v FDD načinu, zato je FEXT glavni omejevalni dejavnik prenosne kapacitete ADSL in VDSL sistemov.
- Na osnovi poznavanja signalov sosednih paric je mogoče izločiti tudi FEXT in mnogo šibkejši šum iz okolice postane edini omejevalni dejavnik.
- **VDSL.vector** ima dodatno vgrajen adaptivni sistem za izločanje daljnega presluha FEXT, ki upošteva množico vseh izvorov iz sosednih paric v kablu, kar v obdelavi tvori večdimenzionalni signal (mat. imenovanje =vektor).




# Prenosna kapaciteta, vpliv FEXT

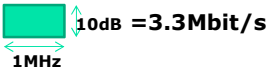
- **VDSL2 Annex B**, DS : B=6.78MHz, P=14.5dBm
- dolžina kabla=500m, d=0.6mm
- prenosna kapaciteti je sorazmerna zeleno obarvani površini:

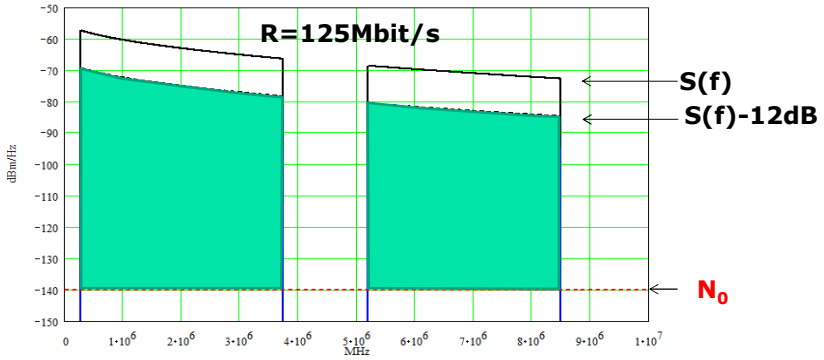


## Prenosna kapaciteta, vpliv $N_0$

- **VDSL.vector: motnja zaradi presluha FEXT je izločena, moti le še šum ozadja N0**
- dolžina kabla=500m, d=0.6mm
- prenosna kapaciteti je sorazmerna zeleno obarvani površini:




## Napovedi ?

- Ob nespremenjenem trendu rasti potreb naprednih uporabnikov lahko v bližnji prihodnosti edino optična omrežja zagotovijo zadostne prenosne kapacitete.
- Izgradnja v celoti optičnih omrežij FTTH je še vedno draga in zamudna, več kot 50% pokritost zato ni verjetno pred letom 2020.
- Pričakujemo lahko, da bo VDSL.vector prevzel pomembno vlogo pri doseganju ciljev DAE v prehodnem obdobju do leta 2020.
- Obstaja velika verjetnost, da bodo VDSL sistemi za najbolj zahtevne uporabnike kmalu po ciljnem datumu DAE 2020 postali zastareli.

- Prihodnost dostopovnih omrežij ?
  - mobilne naprave zahtevajo povezovanja brez žic, torej radijsko komunikacijo,
  - visoke prenosne kapacitete za vse uporabnike lahko zagotovimo le majhnih celicah,
  - omrežje bo razdrobljeno na veliko število radijskih dostopovnih točk, ki bodo povezana preko optičnih povezav.

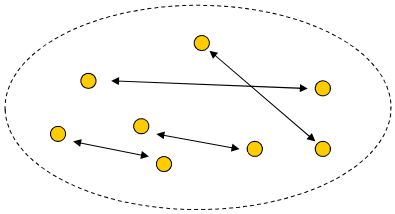
## 11. SODOSTOP

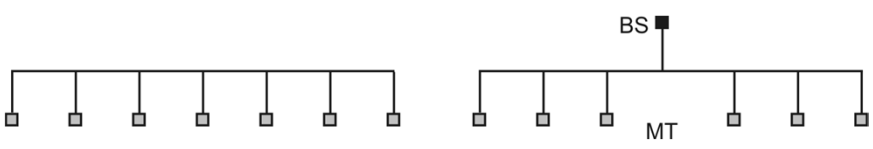
- Delitev prenosnega medija z signali
- Dodeljevanje kanalov po različnih protokolih
  - statično
  - dinamično: naključno ali na zahtevo
- Tehnike sodostopa:
  - SDMA
  - FDMA
  - TDMA
  - CDMA



## Uporaba skupnega medija

- po istem prenosnem mediju želi dvosmerno komunicirati množica uporabnikov:





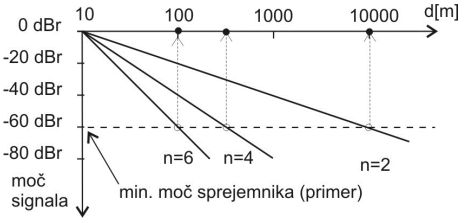
## Razdelitev in dodeljevanje prenosnih kapacitet

- primarna razdelitev frekvenčnih pasov velikim uporabnikom (FDM)
- delitev prenosne kapacitete na množico kanalov
  - prostorska delitev - SDMA
  - delitev s signali: FDMA, TDMA, CDMA,
- dodeljevanje kanalov uporabnikom (protokoli)
  - statično dodeljevanje kanala za ves čas zveze
  - dinamično dodeljevanje kapacitet:
    - naključno zaseganje kanala z različno stopnjo "uglajenosti" do souporabnikov (Aloha, CSMA, CSMA-CD, CSMA-CA ...), QoS ???
    - usklajena uporaba kanala z rezervacijami po dogovoru glede na potrebe uporabnikov. Uporabijo se lahko različni rezervacijski protokoli z algoritmi razporejanja kapacitet.



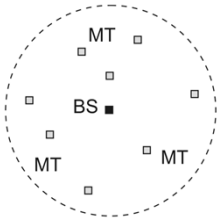
## Območje "skupnega medija"

- Moč signala v sprejemniku strmo upada z razdaljo. Doseg radijske zveze je zato omejen na določeno geografsko območje.

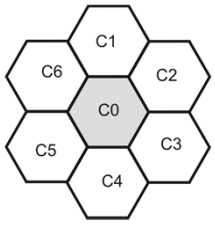



$$P_R(d) = P_T \cdot K \cdot d^{-n}$$

**celica:**

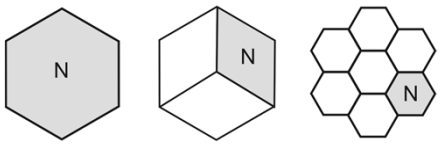



**celično radijsko omrežje:**

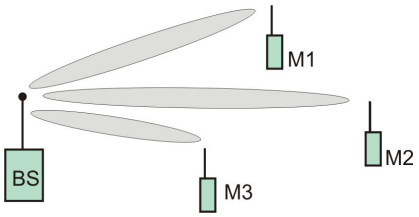


## Povečanje prostorske ločljivosti

- sektorizacija in drobitev celic



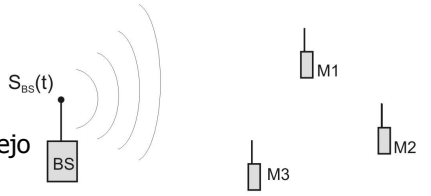

- prilagodljive usmerjene antene ( SA"pametne" antene) omogočajo usmerjene povezave in s tem omejeno prostorsko ločevanje kanalov - SDMA



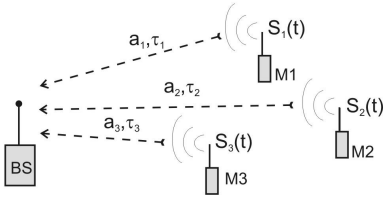



## Multipleksiranje signalov in sodostop

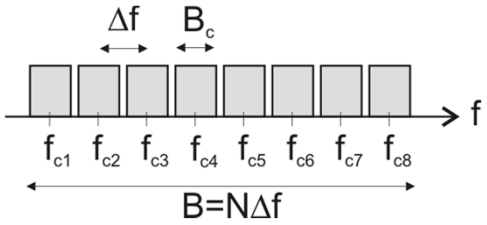
- Bazna postaja oddaja multipleksirani signal




- Mobilni terminali sodostopajo do skupnega medija. Signali se razlikujejo po moči in zakasnitvah !



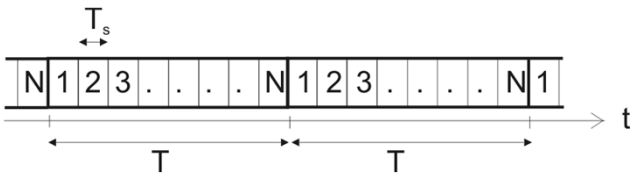
## Frekvenčni sodostop - FDMA




- enakomerna delitev frekvenčnega pasu na N kanalov,
- (+) nizka zahtevnost naprav (ozkopasovni FDMA),
- mobilni sistemi 1G: NMT, AMPS,..

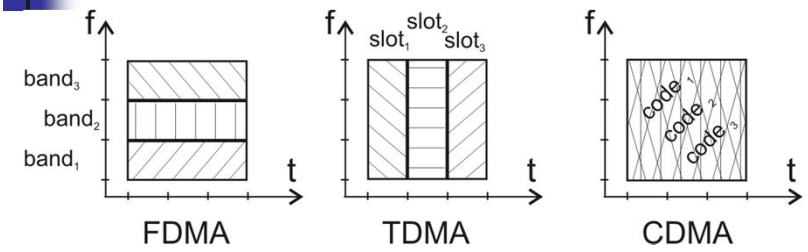


## Časovni sodostop - TDMA




- enakomerna delitev časovnega okvira na N časovnih rezin,
- (+) preprosto dodajanje kapacitet,
- (-) ISI, sinhronizacija naprav !!
- mobilni sistemi 2G: GSM, DECT, DC3,..

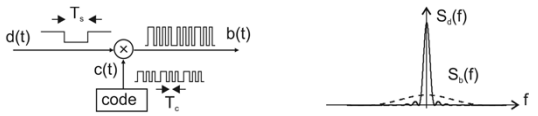
## Kodni sodostop - CDMA



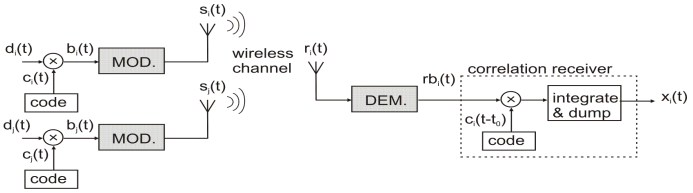

- Signali različnih niso ločeni po frekvenci ali času.
- Signali so generirani z različnimi kodami in se med seboj ne motijo, če so kode ortogonalne – OCDMA (primer: Walsh-Hadamard)
- Signali so lahko generirani tudi z neortogonalnimi kodami (primer: Gold, Kasami), ki nudijo **večje število kanalov**. V tem primeru nastopa tudi omejena motnja (interferenca) med signali različnih uporabnikov.



## Princip razširjanja spektra: DS-CDMA




- CDMA uporablja komunikacijo z razširjenim spektrom.
- Faktor razširjanja spektra *Gs* določa dolžina PN kode: *Ts= Gs Tc*
- detekcija "pravega signala" temelji na poznavanju kodnega niza oddajnika:



## Sklepne ugotovitve

- Radijski spekter je omejen in zato dragocen naravni vir. Uporaba spektra mora biti učinkovita. Največji učinek na povečanje prenosnih kapacitet ima drobljenje celic na geografsko majhna območja. Samo uporaba prostorskega sodostopa SDMA ne zadošča, potrebujemo tudi ločitev različnih signalov: TDMA, FDMA ali CDMA.
- Pri FDMA in TDMA se kapaciteta danega frekvenčnega pasu enakomerno deli med (N) kanalov.
- V CDMA je število kanalov lahko mnogo večje, zasedanje skupne prenosne kapacitete pa je dinamično. Interferenca med kanali je sorazmerna številu hkrati aktivnih oddajnikov.
- Razvoj sistemov 1G, 2G, 3G -> 4G pomeni tudi evolucijo tehnik sodostopa:
  - FDMA, TDMA, CDMA --> OFDM

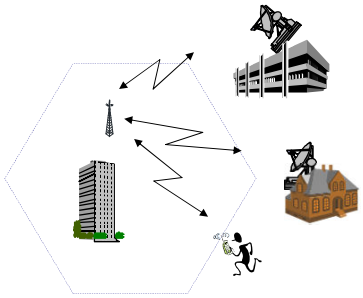


## 12. RADIJSKA DOSTOPOVNA OMREŽJA

- Prednosti uporabe radijskih povezav
- Slabosti prenosnega medija
- Tehnologije radijskih dostopovnih omrežij
  - Lokalno brezžično omrežje WLAN, WiFi
  - WMAN omrežje: WiMAX
  - Mobilna celična omrežja: GSM, UMTS, LTE
  - Satelitska omrežja in aeronavtične ploščadi

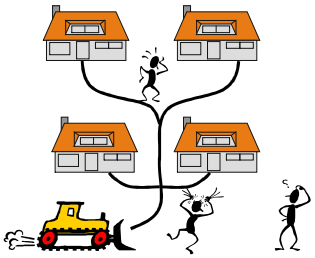
## Prednosti brezžičnih zvez

- Hitrejše in cenejše pokrivanje področja.
- Lažje vzdrževanje in dograjevanje omrežja.
- Postopnost investicije.



**stroški gradnje : stroški opreme**
**20 : 80**

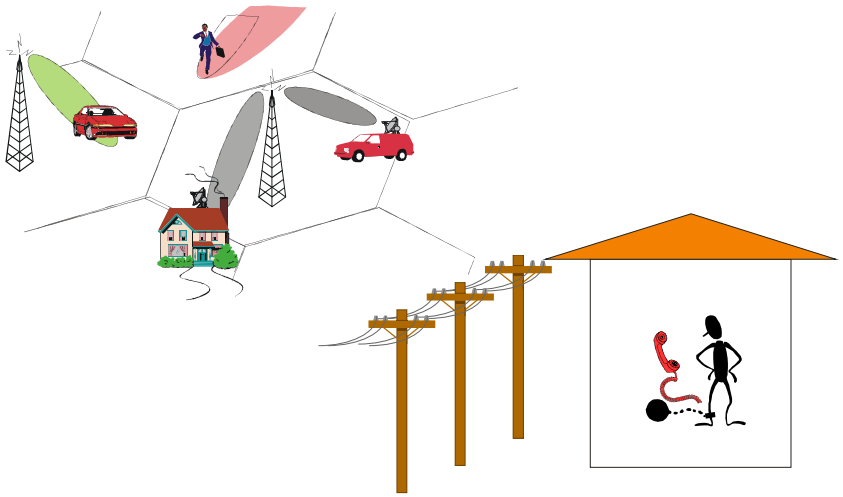
**stroški gradnje : stroški opreme**
**90 : 10**





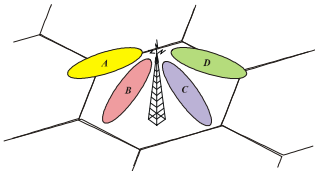
## Glavna prednosti radijskih komunikacij

- Mobilnost uporabnikov !

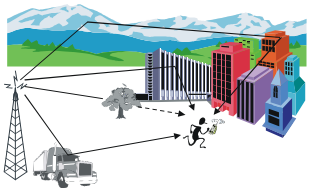


## Slabosti brezžičnih zvez

- Omejitve prenosnih kapacitet zaradi zaradi skupnega medija, potrebujemo sodostop (FDMA, TDMA, CDMA, SDMA).




- Radijski signali so podvrženi različnim motnjam:
  - slabljenje signala, odboji in širjenje po več poteh,
  - motnje in šum,
  - uporabniki so mobilni , zato se razmere za prenos hitro spreminjajo!

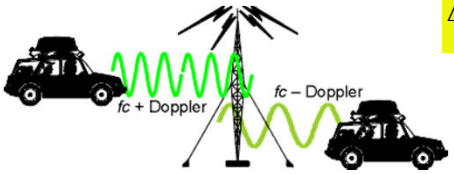


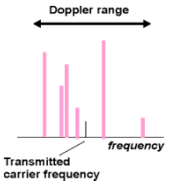


## Dopplerjev pojav

- Če se razdalja med sprejemnikom in oddajnikom spreminja nastopi premik frekvenc:

$$\Delta f = \frac{f_0}{c} \cdot v \cdot \cos(\alpha)$$

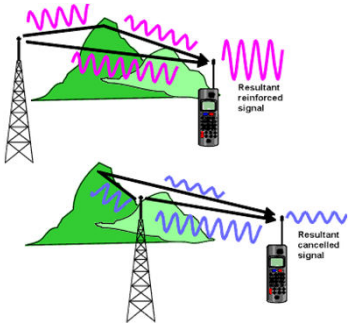



- **<u>Primer:</u> Pri frekvenci nosilca $f_0$=1GHz in relativni hitrosti premikanja 100km/h je odmik 92.6Hz**

## Razširjanje signala po več poteh

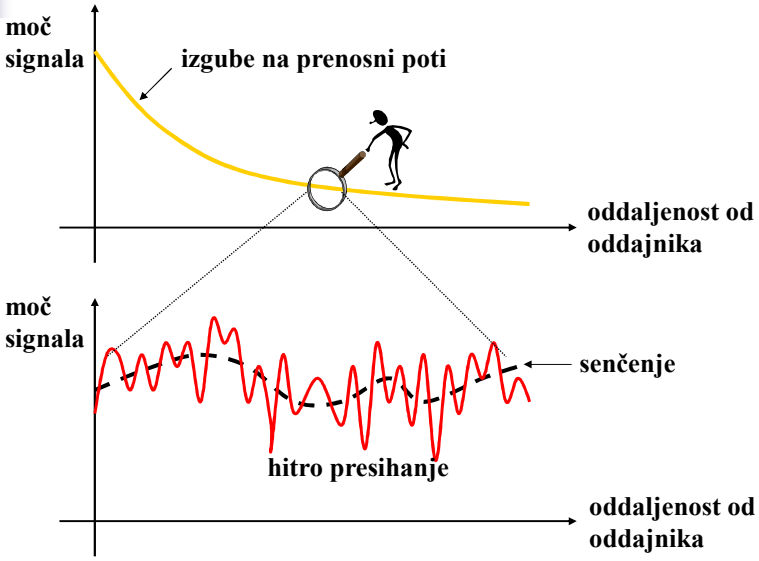
- Signal v sprejemniku je vsota različno zakasnjenih komponent:




- **Signala se lahko seštejeta z enako ali različno polariteto !**

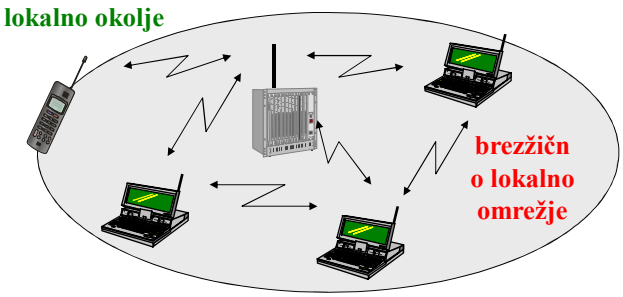


## Upadanje in nihanje moči sprejetega signala



## Lokalna brezžična omrežja - WLAN

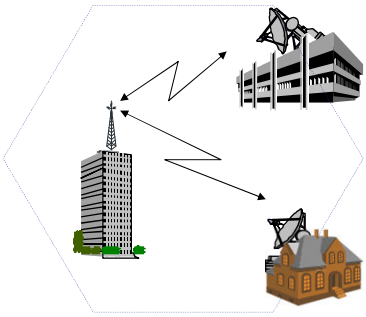
- WLAN: IEEE 802.11, WiFi





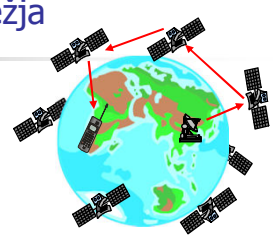

## WMAN

- IEEE 802.16 , WiMAX
- 802.16e , mobilni WiMAX



# Satelitska omrežja

- Edina rešitev za zagotavljanje globalnega pokrivanja.
- Podatkovne hitrosti do 64 Mb/s.
- Za interaktivne storitve so potrebne nižje krožnice, kar podraži sistem.

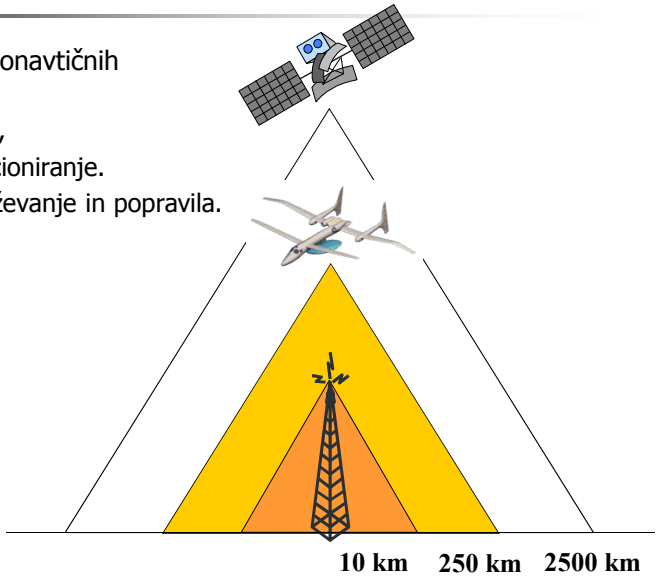


| | višina [km] | okvirni čas obhoda zemlje | čas vidljivosti satelita iz iste točke na zemlji | čas potovanja signala zemlja - satelit - zemlja | primer sistema |
|---|---|---|---|---|---|
| **LEO** | 200 - 1500 | 90 min | 15 min | do 10 ms | Globalstar, Teledisc, SkyBridge |
| **MEO** | 5000 - 13000 | 5 -12 h | 2 - 4 h | 40 do 100 ms | ICO, Spaceway |
| **GEO** | 35786 | 24 h | ves čas | 250 ms | Inmarsat |



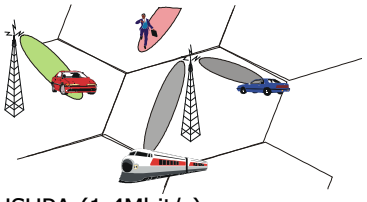
# Sateliti in aeronavtiče ploščadi

- Prednosti aeronavtičnih ploščadi:
  - nižja cena,
  - lažje pozicioniranje.
  - lažje vzdrževanje in popravila.



## Razvoj mobilnih celičnih omrežij

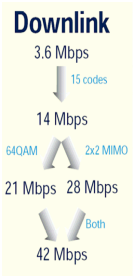
- NMT, GSM, GPRS, EDGE, UMTS , HSPA, LTE
- Omejitve hitrosti prenosa podatkov:
  - do 82,4 kb/s (GPRS),
  - do 236,8 kb/s (EDGE),
  - do 384 kb/s (UMTS)
  - do 3,6 Mb/s (HSDPA)
  - nadgradnja HSPA: HSDPA(7.2Mbit/s), HSUPA (1.4Mbit/s)
- zadnja tehnologija 3G : LTE (Long Term Evolution)
- naslednja generacija, 4G: LTE advanced





## HSPA + , LTE in LTE Advanced

- Že z običajnim HSPA je mogoče doseči hitrosti do 14,4 Mbit/s v smeri iz omrežja
- HSPA+ omogoča hitrosti prenosa podatkov od 21 Mbit/s naprej; realna hitrost do uporabnika je 8 Mbit/s, v smeri omrežja je 5,76 Mbit/s
- HSPA+ omogoča hitrosti do 42 Mbit/s v smeri iz omrežja;
- LTE (Long Term Evolution) je še vedno 3 G (3,9 G)
- Teoretično največja hitrost prenosa podatkov iz smeri omrežja je do 326.4 Mbit/s. Realistično lahko pričakujemo 100 Mbit/s
- Teoretično največja hitrost prenosa podatkov v smeri proti omrežju je 86.4 Mbit/s
- Kasnejša nadgradnja na LTE-Advanced je programska in bo lahko omogočala hitrosti do 1 Gbit/s



# LTE v Sloveniji (december 2013)

- MOBITEL: *Poglavitna prednost mobilnega omrežja LTE/4G Telekoma Slovenije je v doseganju visokih hitrosti, ki teoretično znašajo* ***do 100 Mb/s*** *v smeri proti uporabniku in* ***do 50 Mb/s v smeri od uporabnika k omrežju****.* Visoka hitrost in odzivnost omogočata prenos videoposnetkov visoke ločljivosti in 3D-vsebin ter izjemno zmogljivo mobilno širokopasovno povezljivost, ki je ključna za storitve v oblaku, M2M (Machine to Machine), »On Line Gaming« in »Internet of Things«.

- SIMOBIL : *Gradimo omrežje LTE (Long Term Evolution - dolgoročna evolucija), najsodobnejše omrežje četrte generacije, ki omogoča najhitrejši prenos podatkov doslej ter zmogljivost omrežja za veliko število uporabnikov hkrati.*