INTERNET

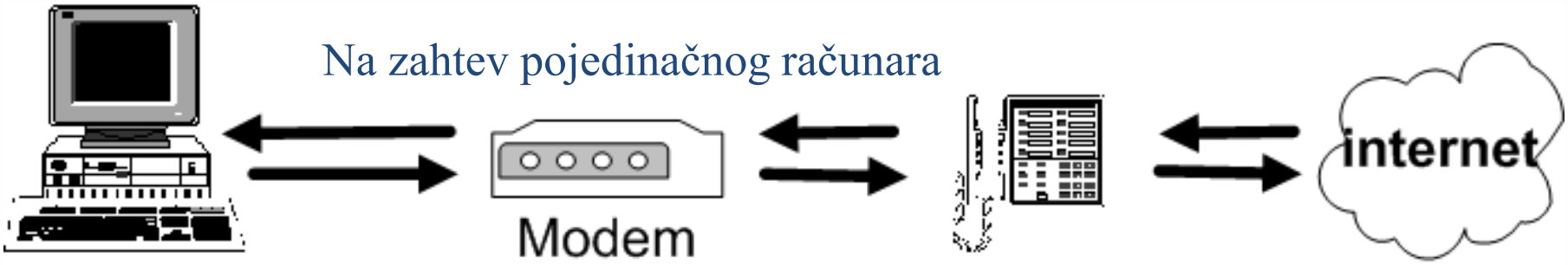
Povezivanje

Zaštita na internetu

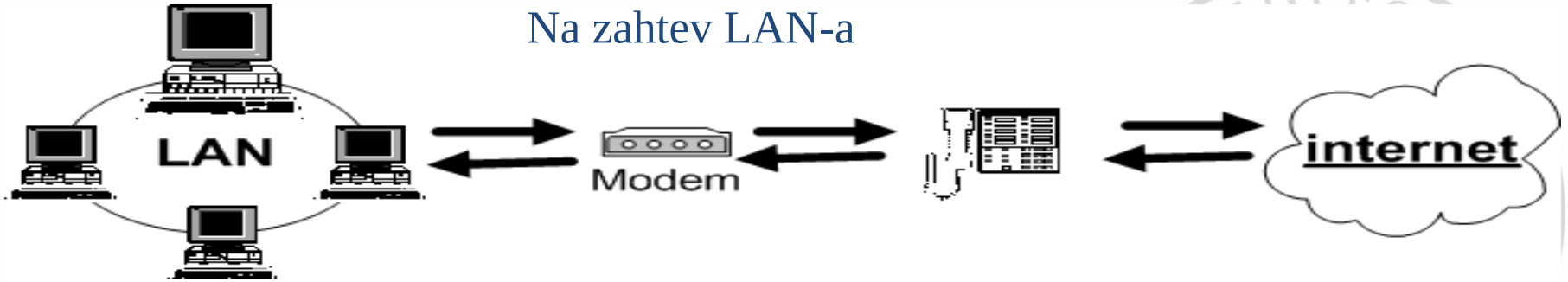
Miomir Todorović

Povezivanje na internet

Na zahtev pojedinačnog računara



Na zahtev LAN-a



Povezivanje na internet

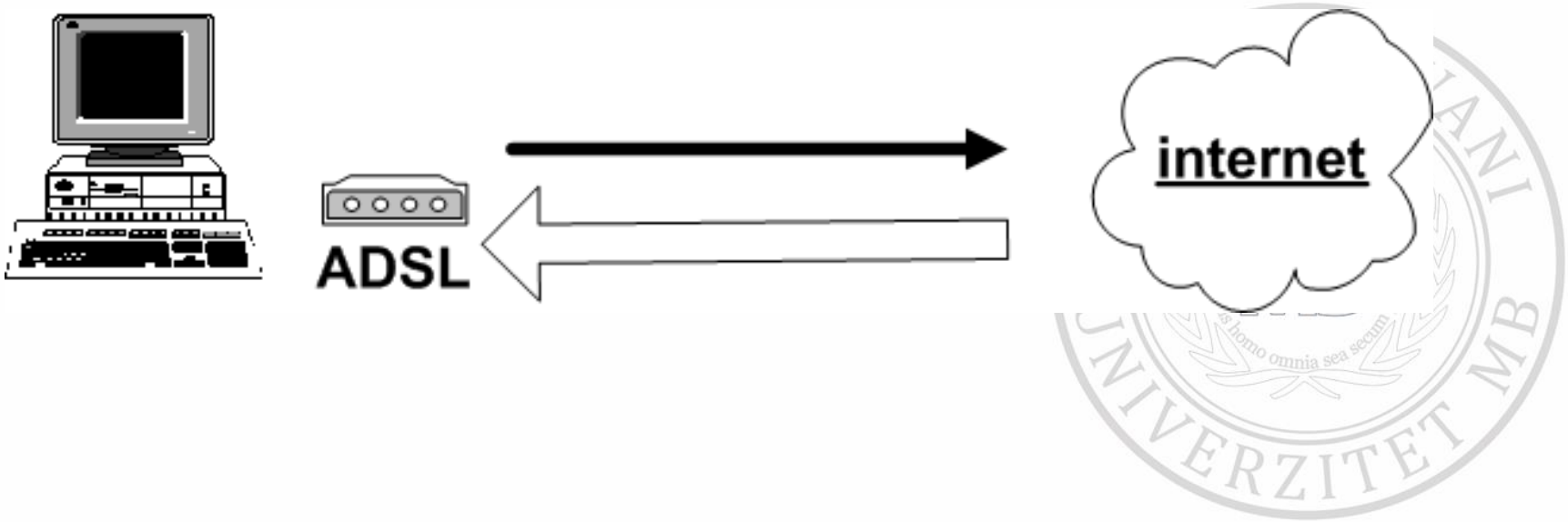
- Prema tehnologiji
  - analogna veza
  - digitalna veza
    - HDSL (*High-speed Digital Subscriber Line*) uređaji.
    - U Zapadnoj Evropi pojedinačni korisnici uglavnomkoriste posebno razvijen sistem digitalnih veza ISDN - integrisani servisi digitalne mreže (*Integrated Services Digital Network*).

Povezivanje na Internet ISDN

- Za ISDN servis postoje dve vrste priključaka:
  - PRI - primarni, sa ukupnim kapacitetom 2048 Kbit/s;
  - BRI - bazni, sa ukupnim kapacitetom 128 Kbit/s (dva B kanala za kombinovani prenos podataka, zvuka, mirne ili pokretne slike i jedan D kanal za prenos signalizacije).
  - BRI se može koristiti i za stalni i za povremeni pristup, a PRI uglavnom za stalni pristup Internetu.

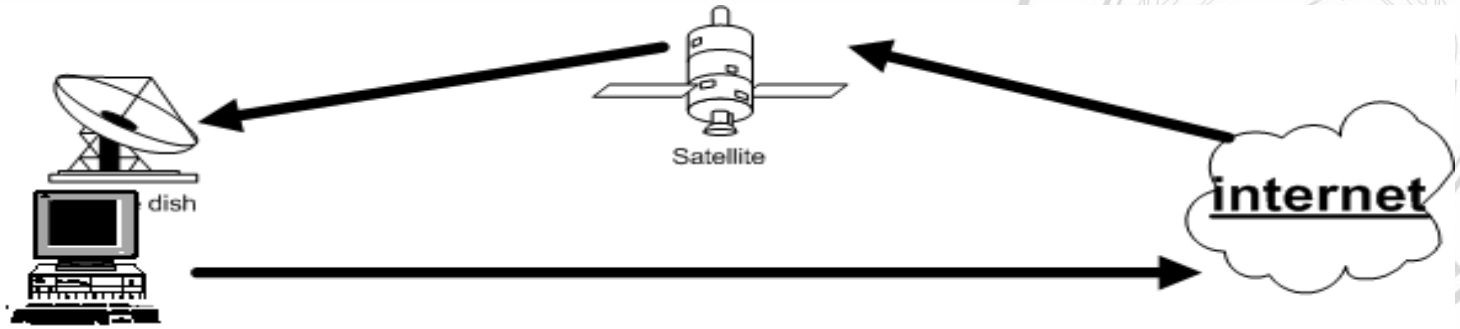
Povezivanje na Internet ADSL

ADSL - asimetrična digitalna pretplatnička petlja
(*Asymetric Digital Subscriber Line*)



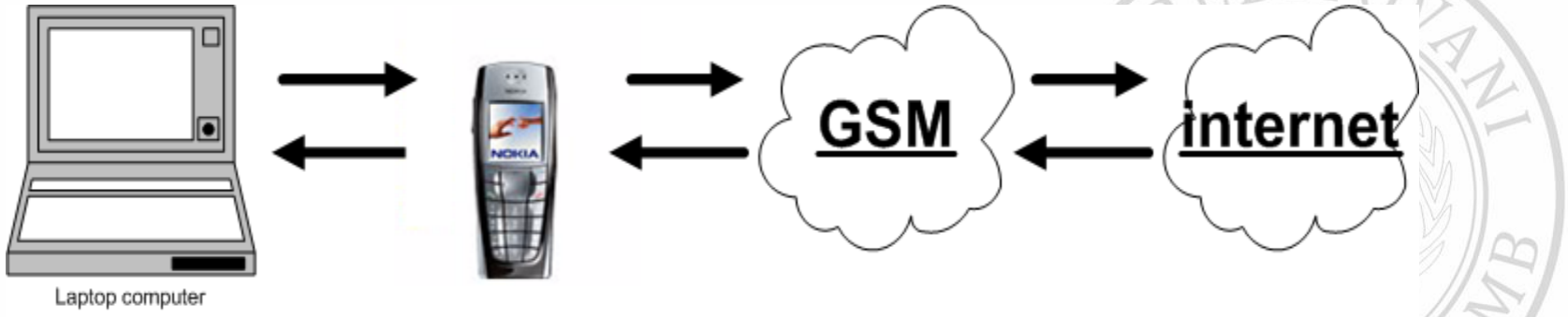
Povezivanje na Internet

- Mikrotalasna veza
- Satelitska veza
- DirecPC
    - DirecPC je specijalizovani servis za asimetrični pristup tipičnog korisnika Internetu. Za saobraćaj od računara ka Internetu koristi se neki od klasičnih načina (npr. modem, ISDN ili stalna veza), a za dolazni saobraćaj (koji je uglavnom mnogo veći nego odlazni) koristi se VSAT (Very Small Aperature Terminal) satelitska antena malog prečnika i prijemnik



Povezivanje mobilnim telefonom

- Pristup *Note-book, Palm-top, PDA-Personal Digital Assistant*).
- Protokol kao što je WAP (*Wireless Application Protocol*), omogućeno je da i sam mobilni telefon postane uređaj, terminal, koji služi za direktan pristup Internetu - ovaj koncept je poznat i pod imenom “mobilni *Web*”.



Zaštita podataka na Internetu

- Promena sadržaja poruka;
- Ubacivanje novih poruka;
- Prekidanje postojećeg toka poruka.

Sigurnosni servisi

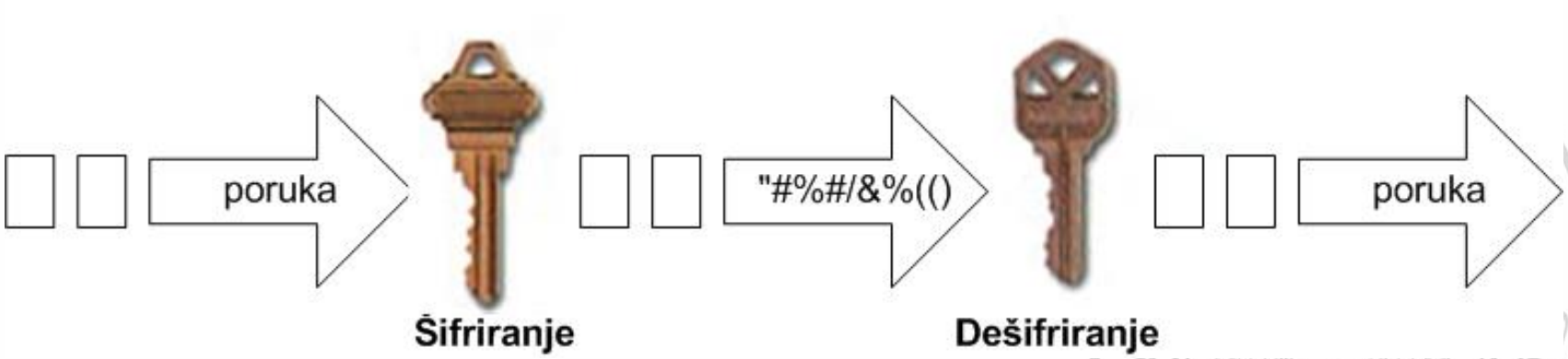
- Tajnost podatka, koja se ostvaruje šifriranjem, odnosno upotrebom tzv. kriptografskih algoritama.
- Autentifikacija poruka, koja omogućava pimaocu da pouzdano utvrdi identitet pošiljaoca.
- Integritet poruka, servis koji garantuje primaocu da poruku nisu menjale neautorizovane osobe.
- Neporicanje poruka, servis koji pošiljaoca treba da spreči da porekne slanje i sadržaj poruke. Digitalni potpis je najčešći mehanizam kojim se rešavaju ovi problemi.
- Kontrola pristupa, servis koji obezbeđuje kontrolisan pristup resursima Interneta. Najčešće se ostvaruje sistemom korisničkih imena sa tajnim lozinkama (*password*), a u novije vreme primenom inteligentnih kartica i tzv. mrežnih barijera (*firewall*).

Šifriranje - Simetrično

- *Simetrično* - šifriranje i dešifriranje vrši se istim ključem. Ako želimo da sačuvamo tajnost poruke, ključ naravno mora biti poznat samo pošiljaocu i primaocu, zato se i zove tajni ključ. Ovde se javlja problem distribucije tajnog ključa udaljenom učesniku komuniciranja.

Asimetrično - šifriranje

- *Asimetrično* - šifriranje i dešifriranje vrši se pomoću dva ključa.
- Korisnik generiše javni i tajni ključ
- Javni ključ razmenjuje sa primaocem



Digitalni potpis

Digitalni potpis realizuje se na sledeći način:

- Kreirate neki dokument.
- Na osnovu vašeg privatnog ključa, softverski mehanizam zaštite generiše zapis kao digitalni potpis koji se dodaje kreiranom dokumentu.

  Ako bi neko izmenio samo jedno slovo u tom dokumentu, digitalni potpis više ne bi odovarao, što znači da se digitalni potpis ne može ukrasti i iskoristiti za lažnu overu nekog drugog dokumenta.
- Krajnji korisnik, koji je dobio dokument uz pomoć vašeg javnog ključa, dobija potvrdu da ste ga zaista vi napisali.

Digitalni vodeni žigovi

- Digitalni vodeni žigovi su elektronski ekvivalent klasičnog vodenog žiga na dokumentima kao što su novčanice, čime se ostvaruje zaštita od neovlašćenog kopiranja i istovremeno dokazuje vlasništvo ili autorstvo.
- vidljivi i nevidljiv

Inteligentne kartice

- Na kartici se mogu nalaziti različiti podaci, kao što su: naziv izdavača, ime vlasnika, fotografija, rok važnosti. Jezgro inteligentne kartice čine programabilni mikroprocesor i odgovarajuće memorije tipa RAM, ROM i EPROM. Intelgentne kartice komuniciraju sa spoljnim svetom preko specijalizovanih ulazno-izlaznih uređaja računara.
- Tajni ključ može biti zapisan na inteligentnoj kartici, i može biti aktiviran samo uz pomoć vlasnika kartice, kako bi se izvršio odgovarajući kriptografski algoritam.

Biometrijski sigurnosni mehanizmi

- biološke karakteristike ljudi, kao što su otisak palca, boja glas ali i izgled zenice
- pomoću kamere slika palca se zapisuje u šifrovanom digitalnom obliku i po potrebi upoređuje sa slikom palca korisnika koji se predstavlja sistemu

Sigurnosne barijere