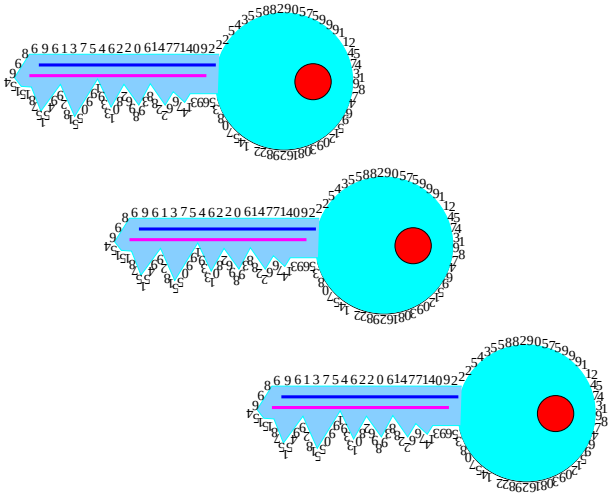
Ljubljana - sreda 6. decembra, 2007

PAMETNE KARTICE V ZASEBNEM ŽIVLJENJU JAVNIH KLJUČEV

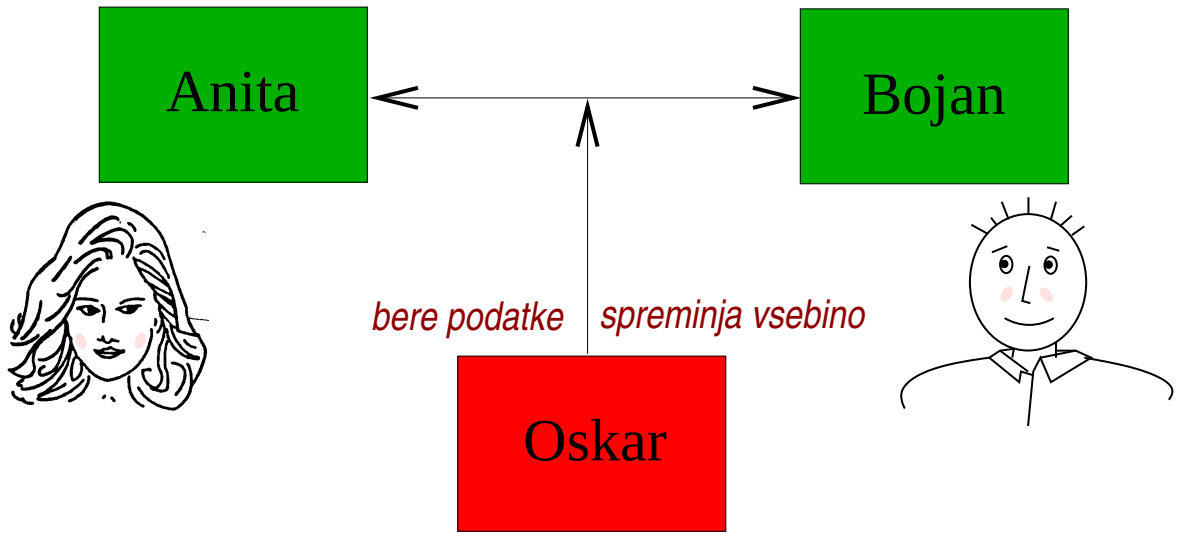
Aleksandar Jurišić
Laboratorij za kriptografijo in računalniško varnost
FRI

http://lkrv.fri.uni-lj.si/~ajurisic



Kaj je kriptografija?

Kriptografija je veda o komunikaciji v prisotnosti aktivnega napadalca.

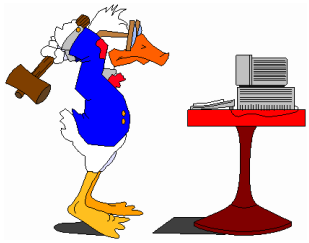


diffie10 (o kriptografiji - 44s), diffie20 (šifre in Enigma - 67s)

Osnovni cilji kriptografije

1. **Zaupnost**: ohranjevanje tajnosti
   pred vsemi razen pooblaščenimi.
2. **Celovitost**: zagotovilo, da informacija ni bila
   spremenjena (z nepooblaščenimi sredstvi).
3. **Overjanje podatkov**:
   potrditev izvora informacij.
4. **Pristnost**: potrditev identitete.
5. **Preprečevanje tajenja**:
   preprečiti neizpolnitev sprejetih obvez ali akcij.

Odšifriranje (razbijanje) klasičnih tajnopisov



Kriptografske sisteme kontroliramo s pomočjo ključev, ki določijo transformacijo podatkov.
Seveda imajo tudi ključi elektronsko obliko (binarno zaporedje: 01001101010101...).

Držimo se **Kerckhoffovega principa**, ki pravi, da "nasprotnik"

pozna kriptosistem oziroma algoritme,
ki jih uporabljamo, ne pa tudi ključe,
ki nam zagotavljajo varnost.

swordfish50 (o razbijanju po pritiskom - 2min)

Vohunova dilema

Bilo je temno kot v rogu, ko se je vohun vračal v grad po opravljeni diverziji v sovražnem taboru.

Ko se je približal vratom, je zaslišal šepetajoč glas:

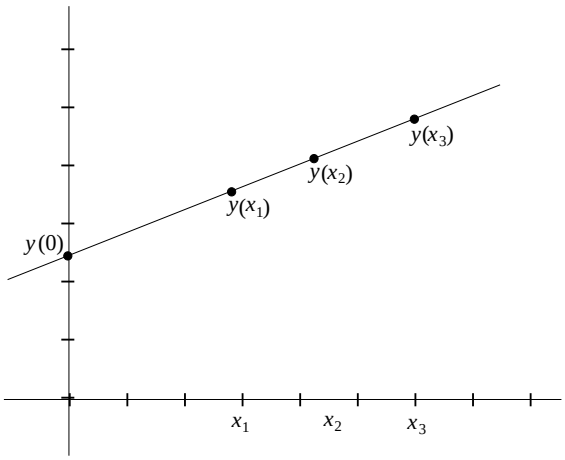
Kako vohun prepriča "stražarja", da pozna geslo, ne da bi ga izdal morebitnemu vsiljivcu/prisluškovalcu?

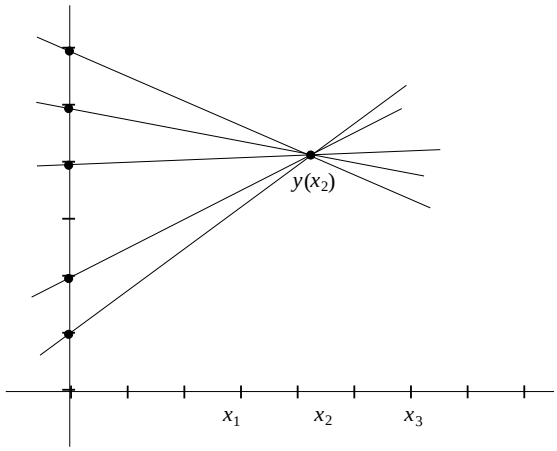
Deljenje skrivnosti

Problem: *V banki morajo trije direktorji odpreti trezor vsak dan, vendar pa ne želijo zaupati kombinacijo nobenemu posamezniku. Zato bi radi imeli sistem, po katerem lahko odpreta trezor poljubna dva med njimi.*

Ta problem lahko rešimo z $(2, 3)$-stopenjsko shemo.

Stopenjske sheme za deljenje skrivnosti sta leta 1979 neodvisno odkrila **Blakey in Shamir**.



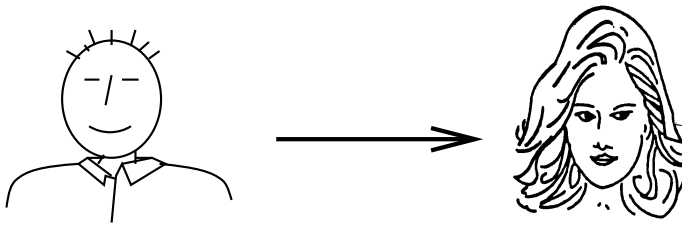


Vsak dobi le y-koordinato svoje točke.
Program v trezorju ima še ustrezne od 0 različne x- koordinate, zato lahko izračuna ključ $y(0)$.
Vsaki točki natanko določata premico in s tem ključ.

Če imamo eno samo točko, ne moremo ugotoviti, kateri ključ je pravi, saj so vsi videti enako dobri.

Koncept javne kriptografije

Bojan pošlje Aniti pismo, pri tem pa si želi, da bi pismo lahko prebrala le ona (in prav nihče drug) **[zaščita]**.

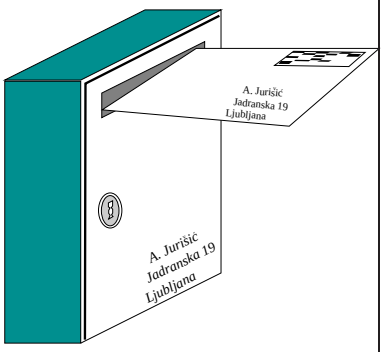


Anita pa si poleg tega želi biti prepričana, da je pismo, ki ga je poslal Bojan prišlo prav od njega **[podpis]**.

Leta 1976 sta Whit **Diffie** in Martin **Hellman** predstavila koncept kriptografije z javnimi ključi.

Tu ima za razliko od sim. sistema vsak uporabnik **dva** ključa, podatke *zaklepa*, drugi pa jih *odklepa*.

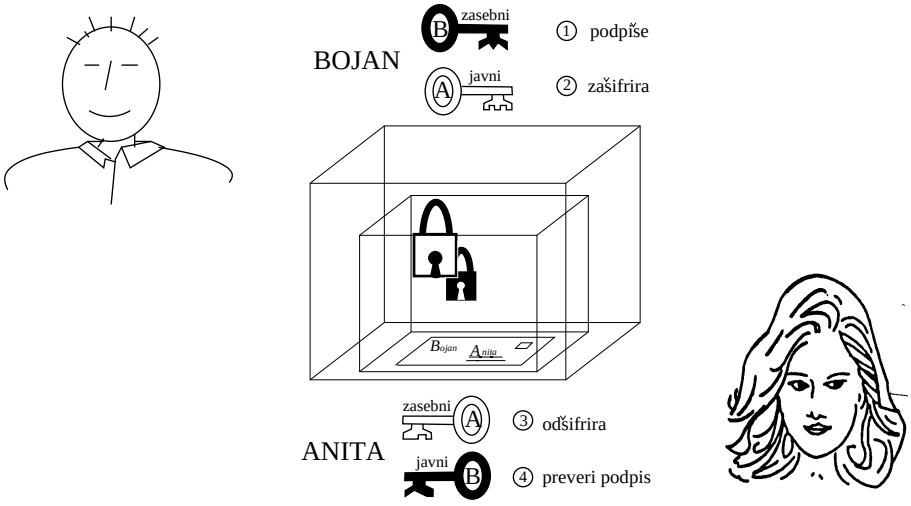
Pomembna lastnost tega sistema:
ključ, ki zaklepa, ne more odklepati
in obratno,
ključ, ki odklepa, ne more zaklepati.



To omogoči lastniku, da en ključ objavi, drugega pa hrani v tajnosti (npr. na pametni kartici). Zato imenujemo ta ključa zaporedoma **javni** in **zasebni**.

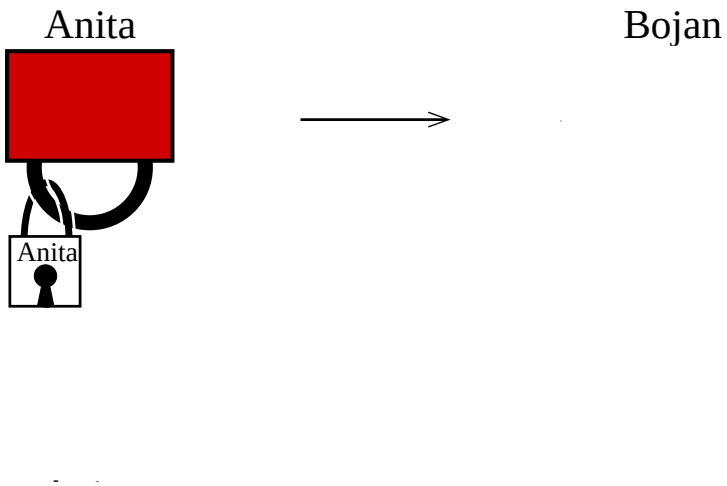
Bojan pošlje Aniti podpisano zasebno pismo:

(1) podpiše ga s svojim zasebnim ključem Z_B in ga
(2) zašifrira z Anitinim javnim ključem J_A.

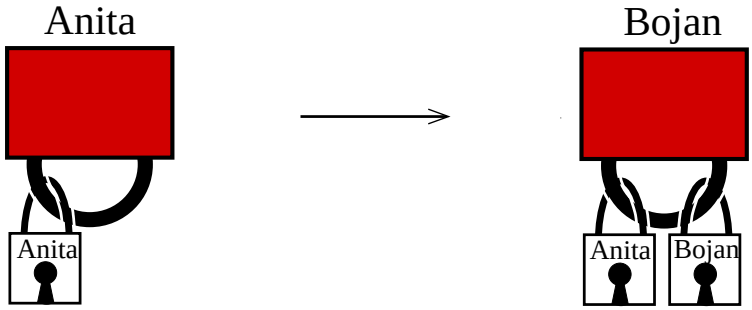


(3) Anita ga s svojim zasebnim ključem Z_A odšifrira,
(4) z Bojanovim javnim ključem J_B preveri podpis.

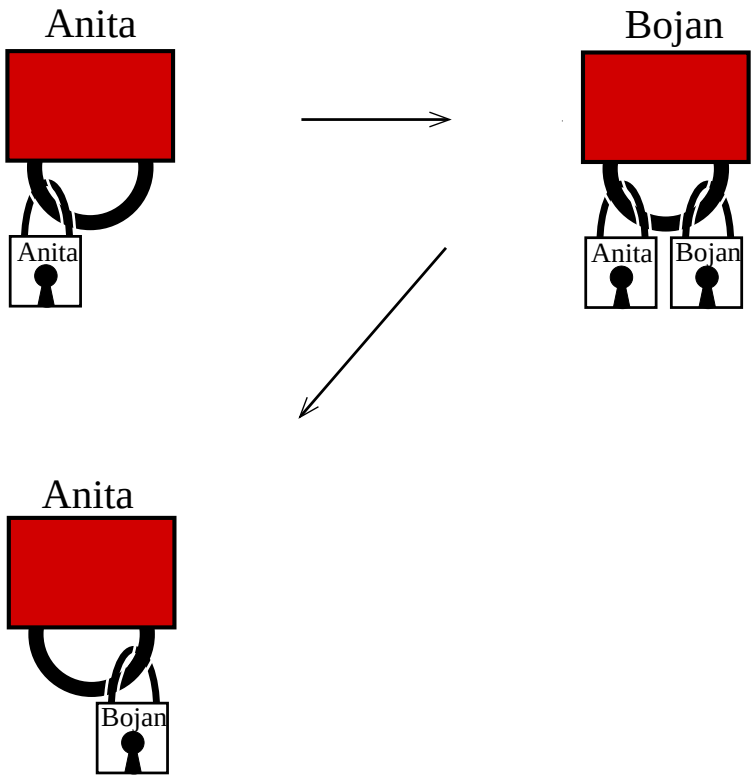
Protokol Massey-Omura



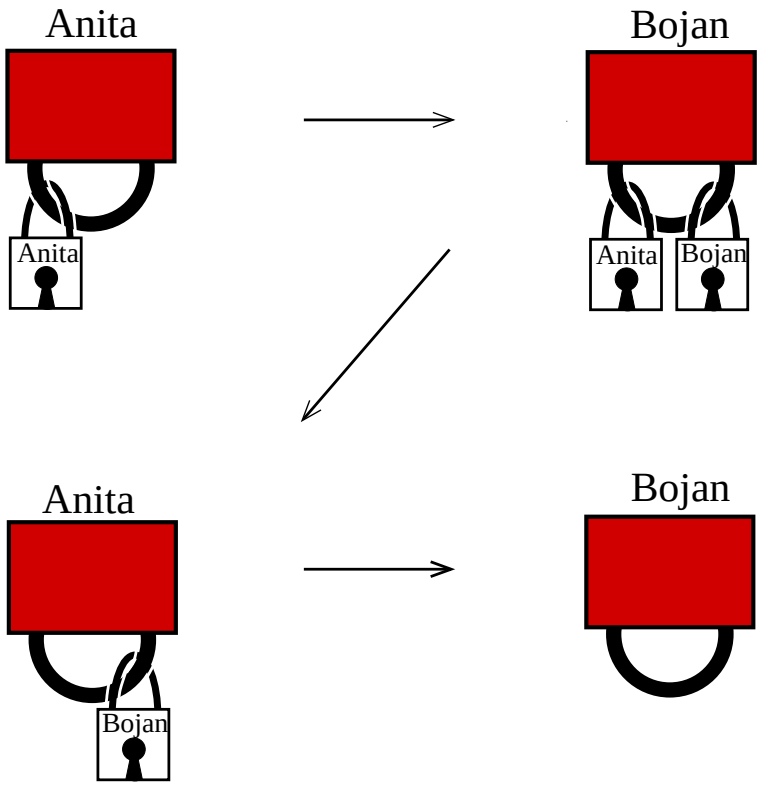
Protokol Massey-Omura (1. korak)



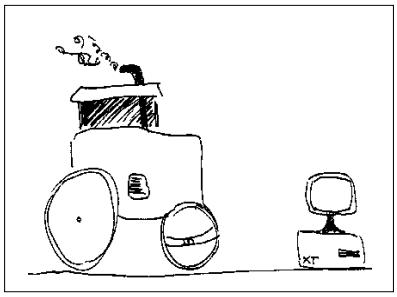
Protokol Massey-Omura (2. korak)

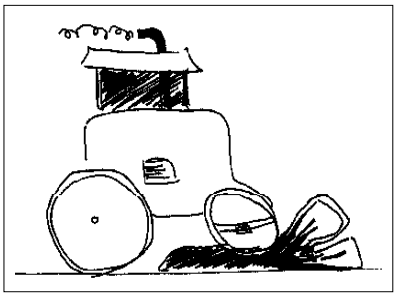
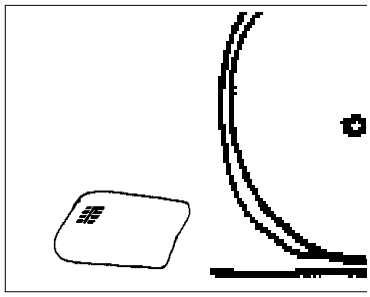


Protokol Massey-Omura (3. korak)



Pametne kartice



Po računski moči so pametne kartice primerljive z originalnim IBM-XT računalnikom,
kartice s **kripto koprocesorjem** pa v nekaterih opravilih prekašajo celo 50 Mhz 486 računalnik.

Zakaj pametna kartica

Gotovo je najbolj pomembna razlika med pametno kartico in magnetno kartico

varnost.

Pametna kartica ima svoj **procesor**, ki kontrolira vse interakcije med od zunaj nedostopnim spominom in različnimi zunanjimi enotami.

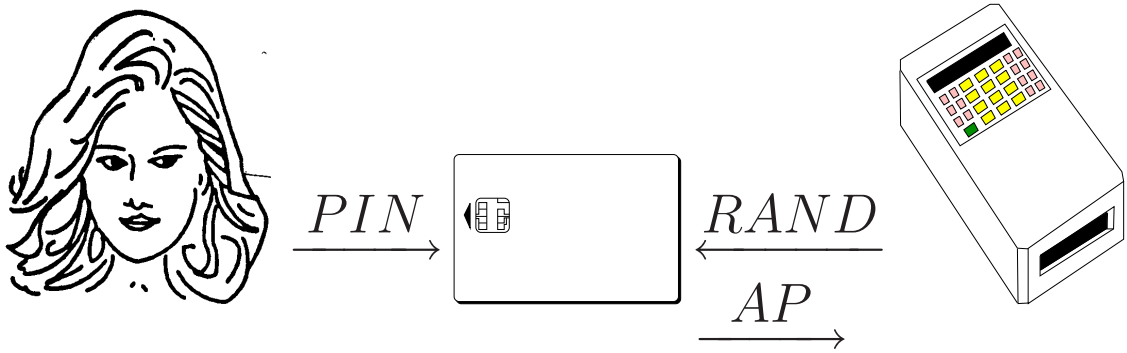
Dodaten, pomemben, del pametne kartice je **non-volatile spomin (ROM)**, t.j. spomin, ki se ga ne da spremeniti in ostane prisoten tudi po prekinitvi napajanja.

Zagotovitev varnosti

Identifikacija se opravi v dveh delih:

(a) kartica mora biti zares prepričana,
da jo uporablja njen lastnik (lokalno overjanje),

(b) kartica komunicira (varno) z računalnikom
(dinamično overjanje).



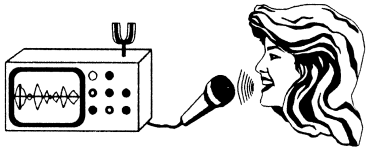
Biometrični testi

prstni odtisi

geometrija roke

odtis noge

vzorec ven
(otroci)



prepoznavanje glasu

vzorec zenice

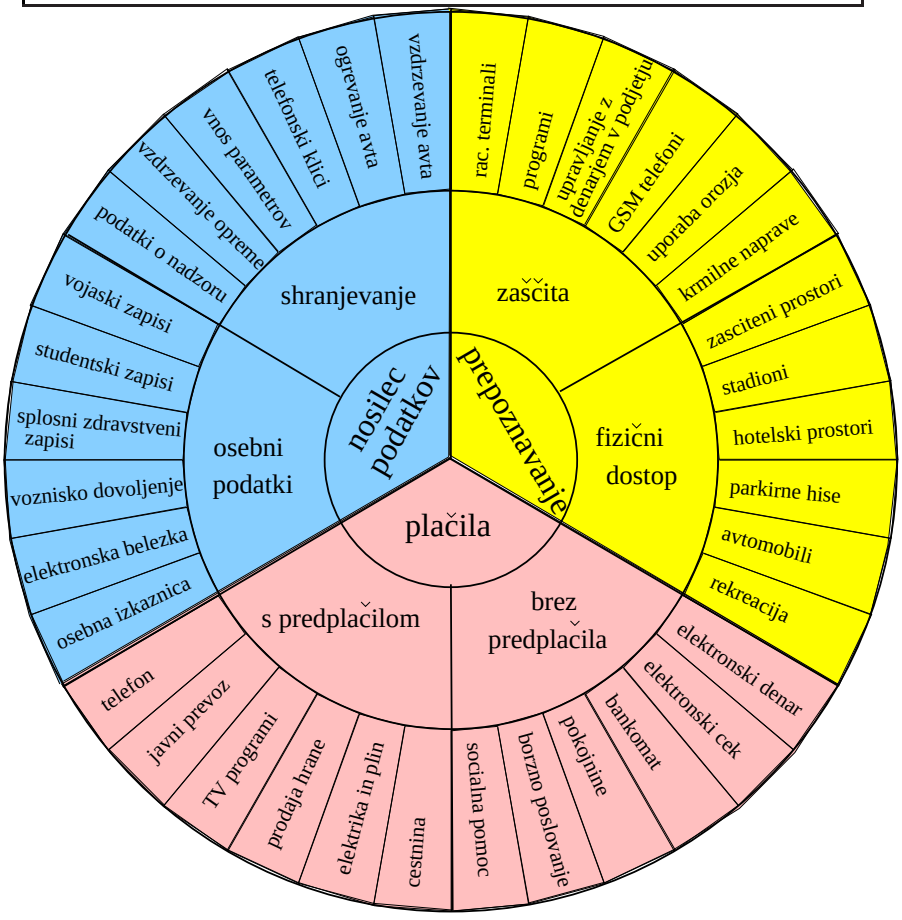
prepoznavanje obraza

zapis zob

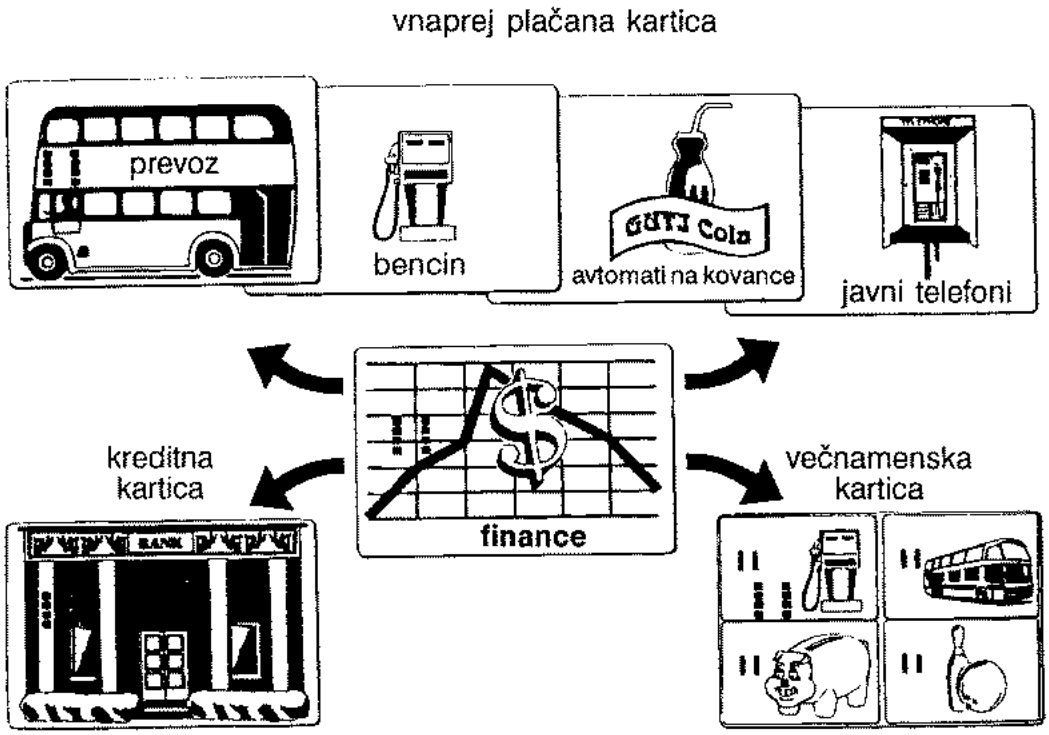
RNK (DNA)

podpis

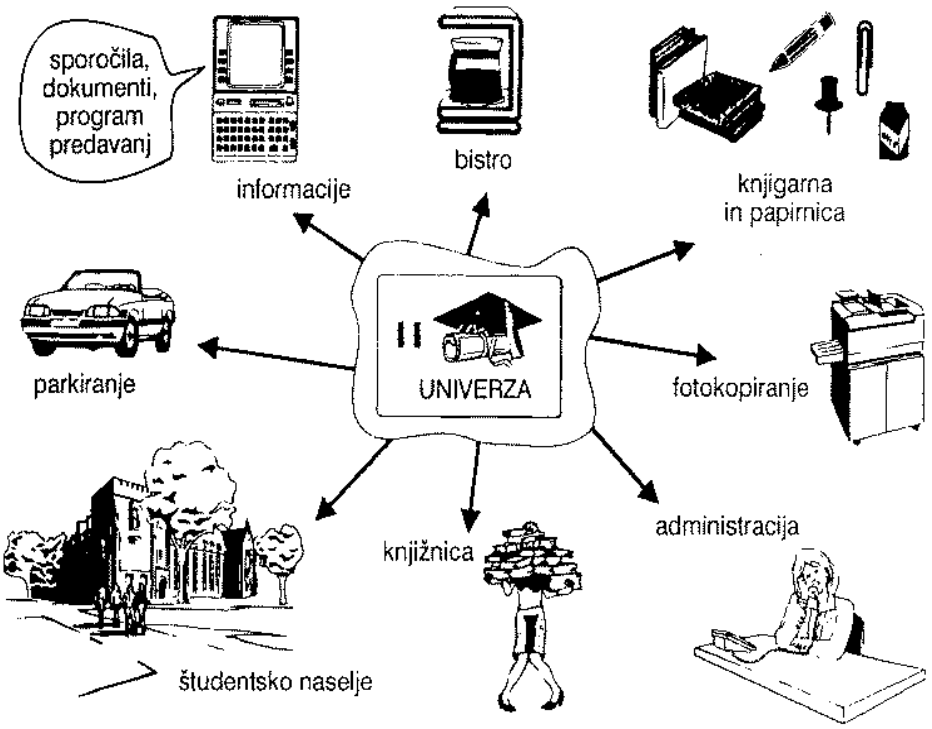
Uporaba pametnih kartic



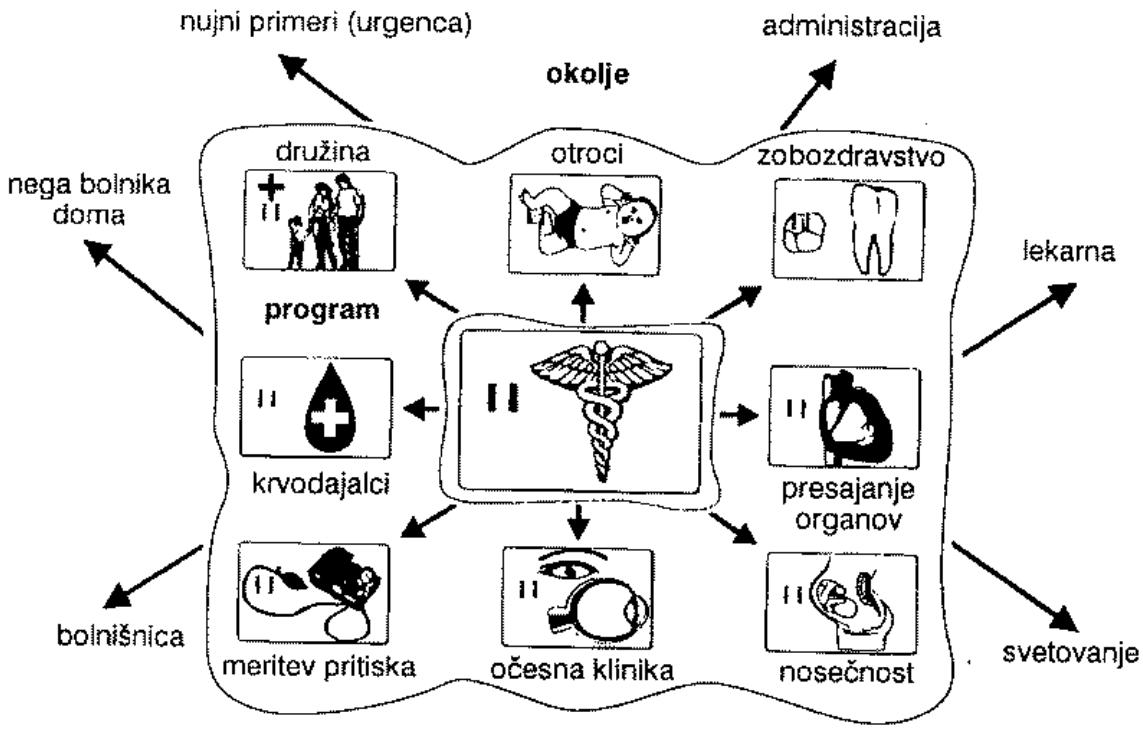
Plačilne, kreditne in večnamenske kartice, ki se uporabljajo na področju *financ*.



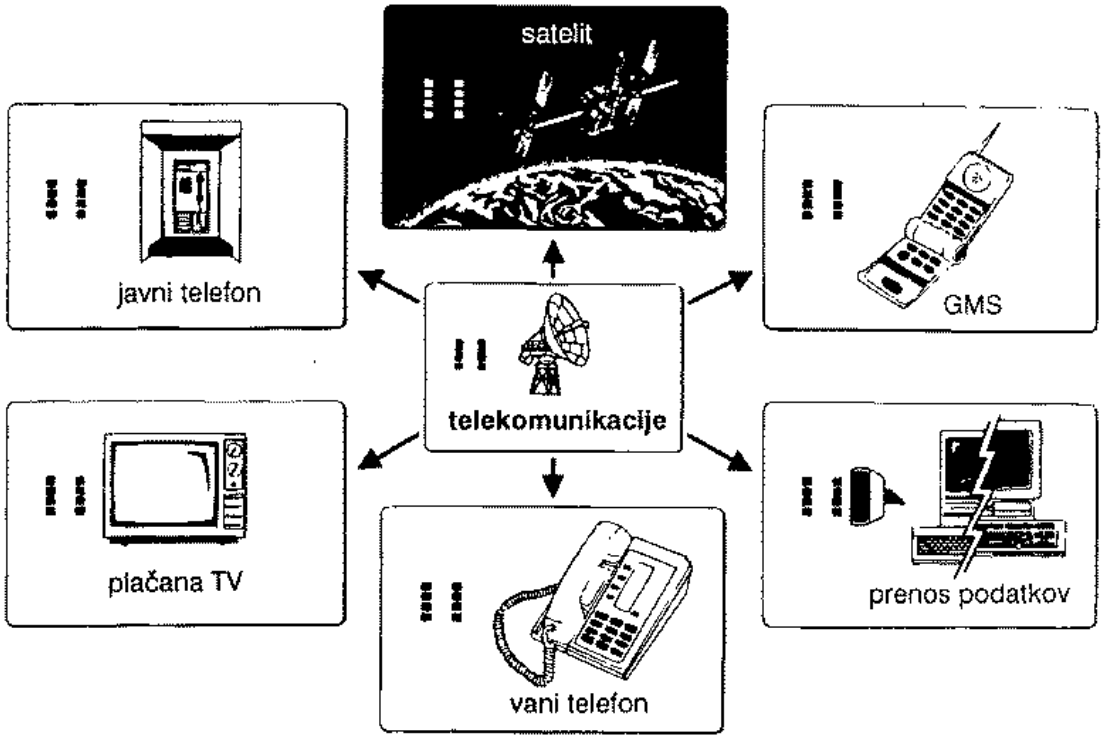
Uporaba pametnih kartic na *univerzi/fakulteti*, ki je ponekod mesto v malem.



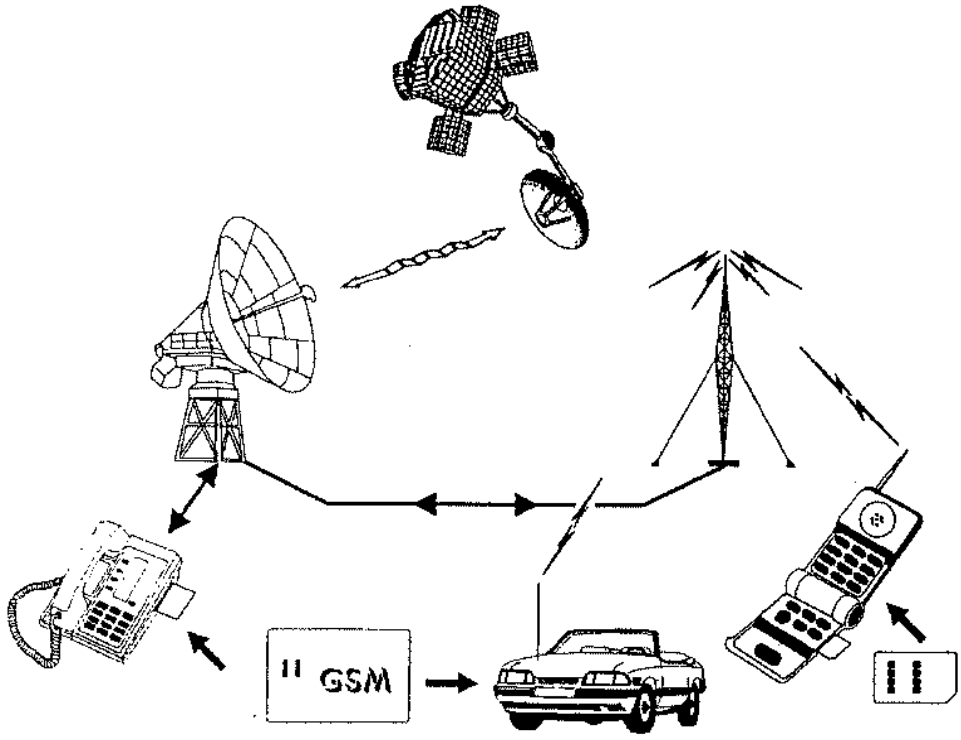
Področja v *zdravstvu*, kjer se uporabljajo pametne kartice.



Uporaba pametne kartice v *telekomunikacijah* in uporabniški elektrotehniki.



GSM (globalni sistem za prenosno komuniciranje)



code50 (o kodah in CD-jih - 2min)