Uvod

Odkar so ljudje pričeli komunicirati,
pa naj si bo to preko govora, pisave, radija,
telefona, televizije ali računalnikov,
so želeli tudi *skrivati* vsebino svojih sporočil.

Ta nuja, oziroma že kar obsedenost
po *tajnosti*, je imela dramatičen vpliv
na vojne, monarhije in seveda tudi
na individualna življenja.

Vladarji in generali so odvisni od uspešne
in učinkovite komunikacije že tisočletja,
hkrati pa se zavedajo posledic, v primeru,
če njihova sporočila pridejo v napačne roke,
izdajo dragocene skrivnosti rivalom ali
odkrijejo vitalne informacije nasprotnikom.

Danes vse to velja tudi za moderna vodstva
uspešnih podjetij in tako postaja

“informacijska/računalniška varnost”

eno izmed najbolj pomembnih gesel
informacijske dobe.

Vlade, industrija ter posamezniki,
vsi hranijo informacije v *digitalni obliki*.

Ta medij nam omogoča številne prednosti
pred fizičnimi oblikami:

- je zelo kompakten,

- prenos je takorekoč trenuten,

hkrati pa je omogočen tudi

- organiziran dostop do raznovrstnih podatkovnih baz.

Z razvojem

- telekomunikacij,
- računalniških omrežij in
- obdelovanja informacij

pa je precej lažje prestreči in spremeniti *digitalno (elektronsko) informacijo* kot pa njenega *papirnega predhodnika*.

Zato so se povečale zahteve po **varnosti**.

Informacijska in računalniška varnost

opisuje vse preventivne postopke in sredstva
s katerimi preprečimo nepooblaščeno uporabo
digitalnih podatkov ali sistemov,
ne glede na to ali gre pri ustreznih podatkih kot sta

digitalni denar (nosilec vrednosti) in
digitalni podpis (za prepoznavanje)

za

- razkritje,
- spreminjanje,
- zamenjavo,
- uničenje,
- preverjanje verodostojnosti.

Predlagani so bili številni ukrepi,
a niti eden med njimi ne zagotavlja
popolne varnosti.

Med preventivnimi ukrepi, ki so na voljo danes, nudi

kriptografija

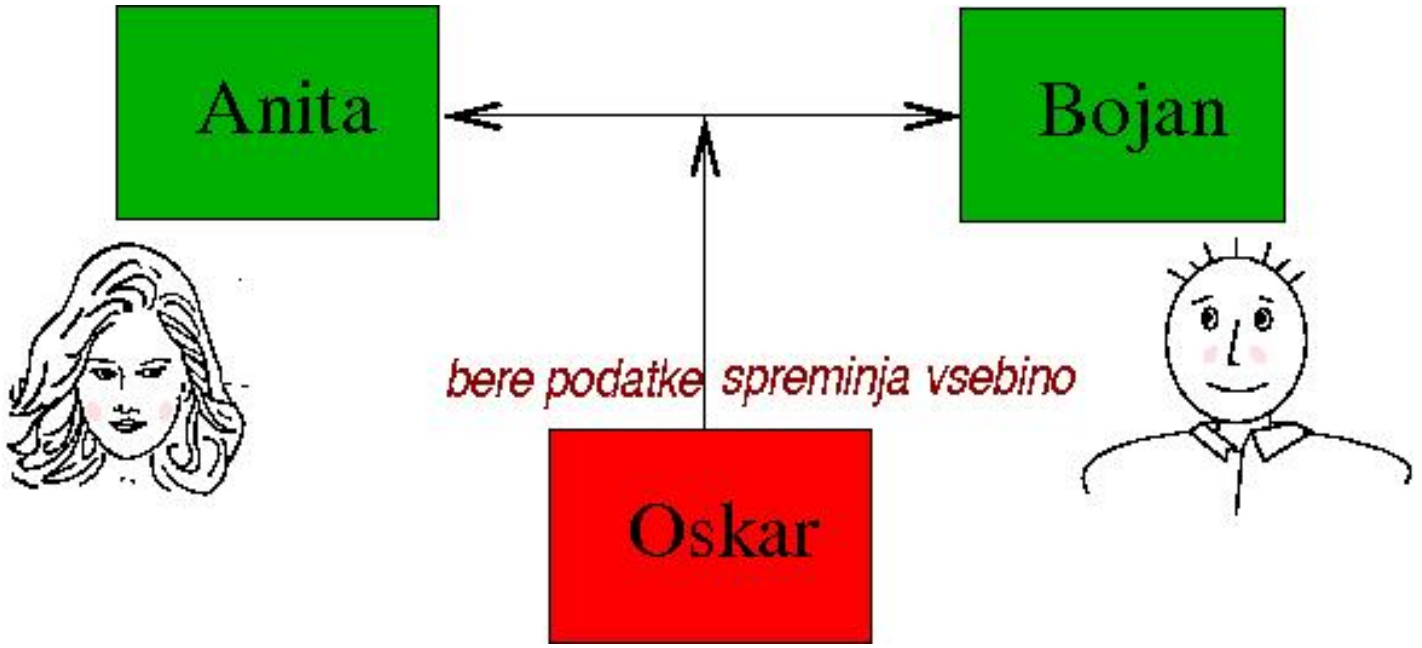
(če je seveda pravilno implementirana ter uporabljana)

največjo stopnjo varnosti

glede na svojo prilagodljivost digitalnim medijem.

Kaj je kriptografija?

Kriptografija je veda o komunikaciji v prisotnosti aktivnega napadalca.



Primer:

pošiljanje papirnih dokumentov po pošti

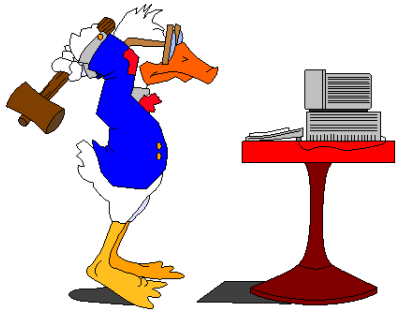
Kakšna zagotovila varnosti so na voljo? In kako?

- **Fizična varnost:** zapečatene kuverte.
- **Zakonska infrastruktura:**
  ročni podpis je zakonsko sprejeto sredstvo,
  zakoni proti odpiranju/oviranju pošte, itd.
- **Poštna infrastruktura:**
  varni in sprejeti mehanizmi za
  dostavljanje pošte širom po svetu.

Primer: digitalni podatki

- **ZA**: hranjenje je enostavno in poceni, hiter in enostaven transport.
- **PROTI**: enostavno kopiranje; transportni mediji niso varni (npr. pogovor po mobilnem telefonu, internetna seja, ftp seja, komunikacija s pomočjo elektronske pošte).
- **Vprašanje**: Kako lahko omogočimo/ponudimo enake možnosti za papirni kakor tudi digitalni svet?

Odšifriranje (razbijanje) klasičnih šifer



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

Držali se bomo **Kerckhoffovega principa**, ki pravi, da "nasprotnik"

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

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:

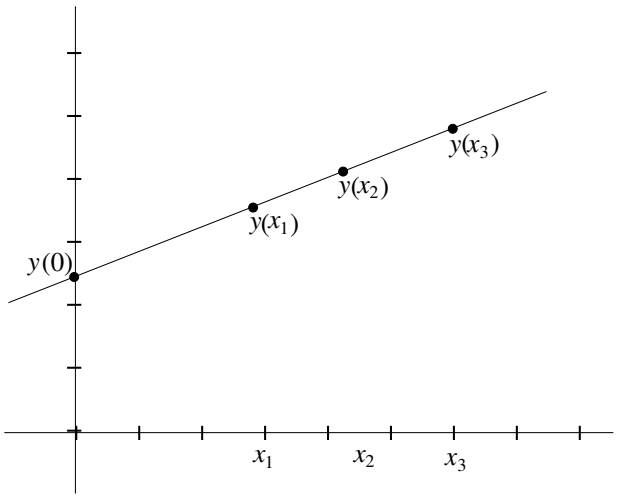
Kako vohun prepriča “stražarja”, da pozna geslo,
ne da bi ga izdal morebitnemu vsiljivcu/prisluškovalcu?

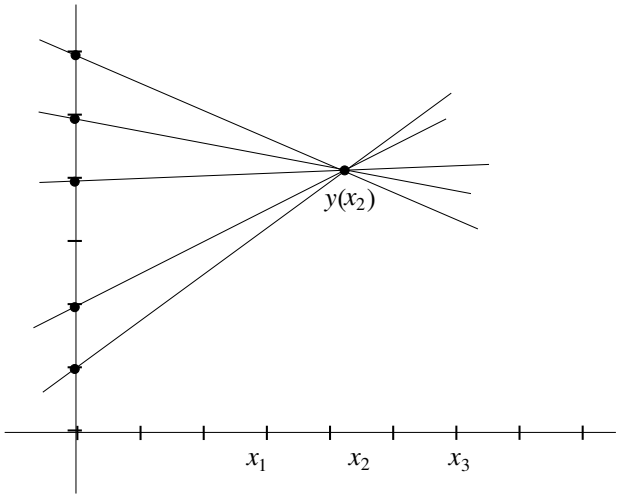
Deljenje skrivnosti

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**.

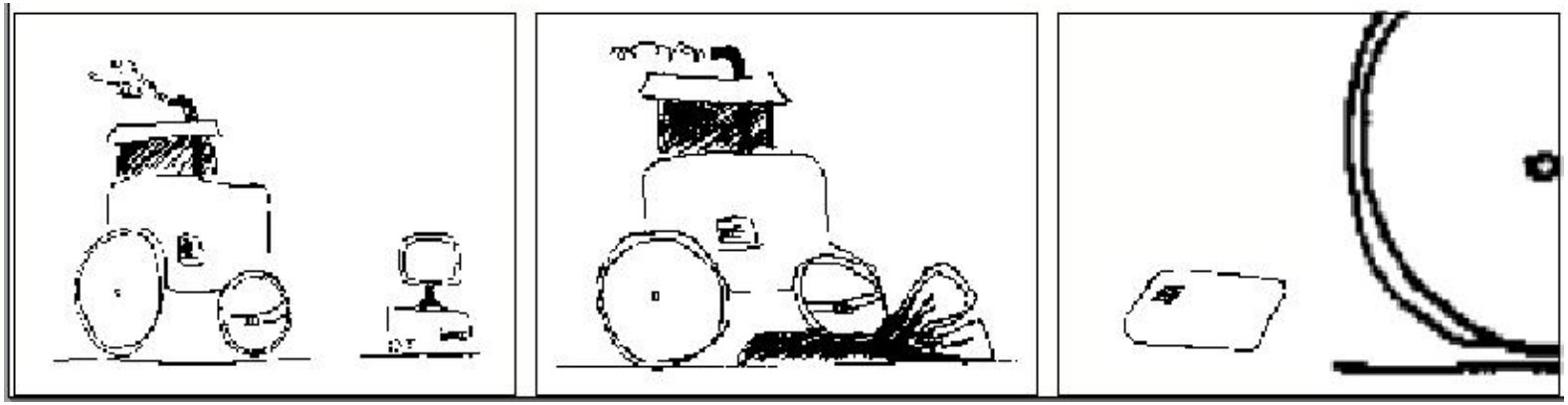




Vsak dobi le y-koordinato svoje točke.
Program v trezorju ima še ustrezne od 0 različne
x- koordinate, zato lahko izračuna ključ $y(0)$.
Vsaki točki natanko določata premico in s tem ključ.

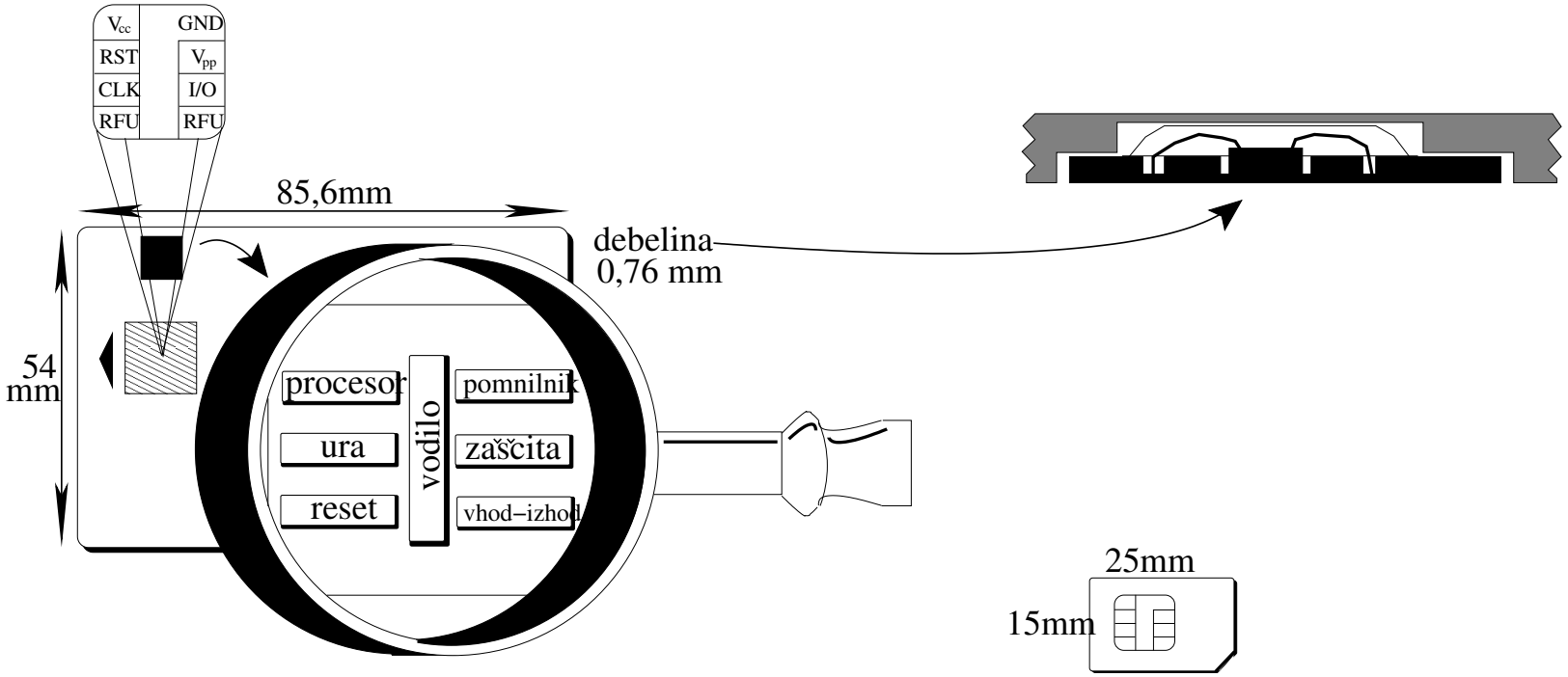
Če imamo eno samo točko, ne moremo ugotoviti,
kateri ključ je pravi, saj so vsi videti enako dobri.

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.



Velikost pametne kartice ustreza ISO 7810 standardu, sestavljajo pa jo mikroprocesor, pomnilnik (ROM, RAM, EEPROM), vhodno/izhodna enota (I/O).

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),
tj. spomin, ki se ga ne da spremeniti in
ostane prisoten tudi po prekinitvi napajanja.

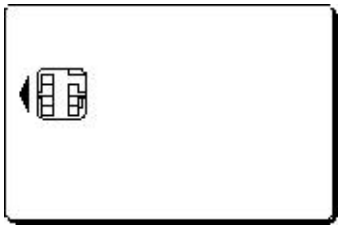
Zagotovitev varnosti

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).

$PIN \rightarrow$



$\leftarrow RAND$

$AP \rightarrow$

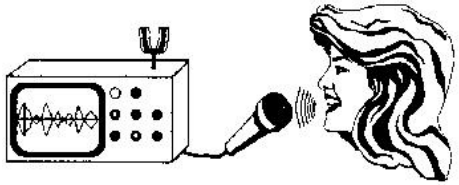
Biometrični testi

prstni odtisi

geometrija roke

odtis noge
(otroci)

vzorec ven

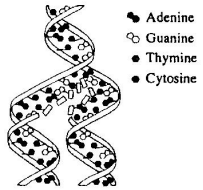


prepoznavanje glasu

vzorec zenice

prepoznavanje obraza

zapis zob



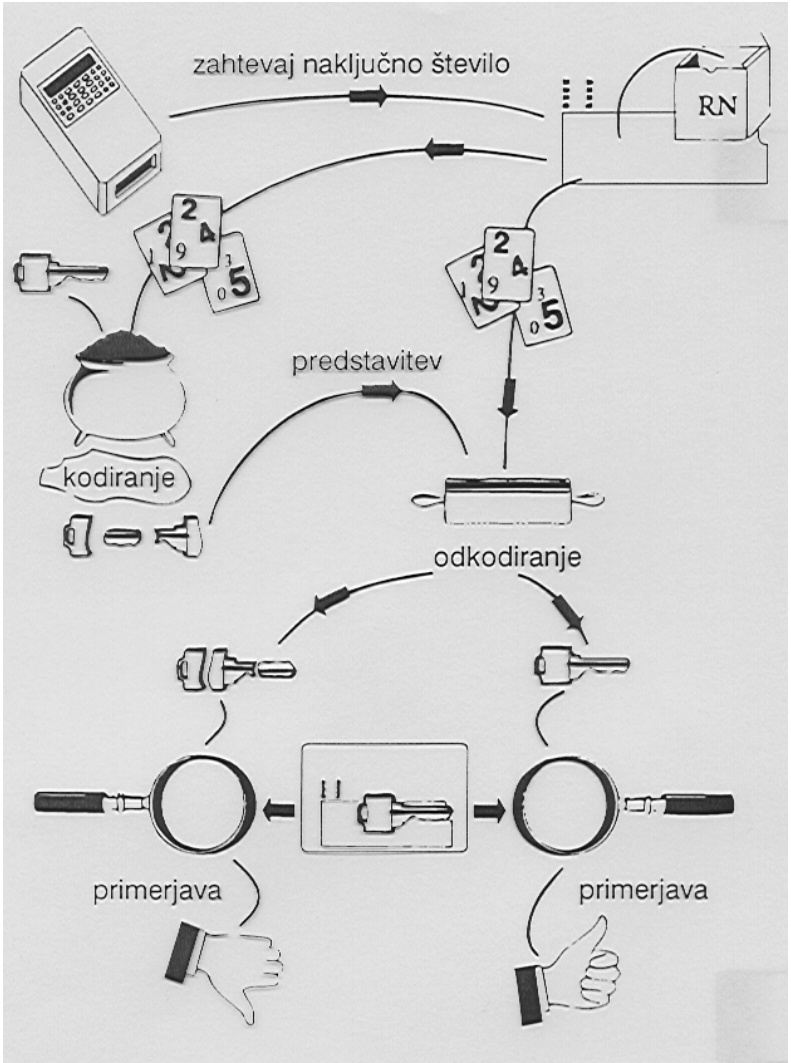
RNK (DNA)

podpis

Pametna kartica zgenerira naključno število, ter ga pošlje čitalniku.

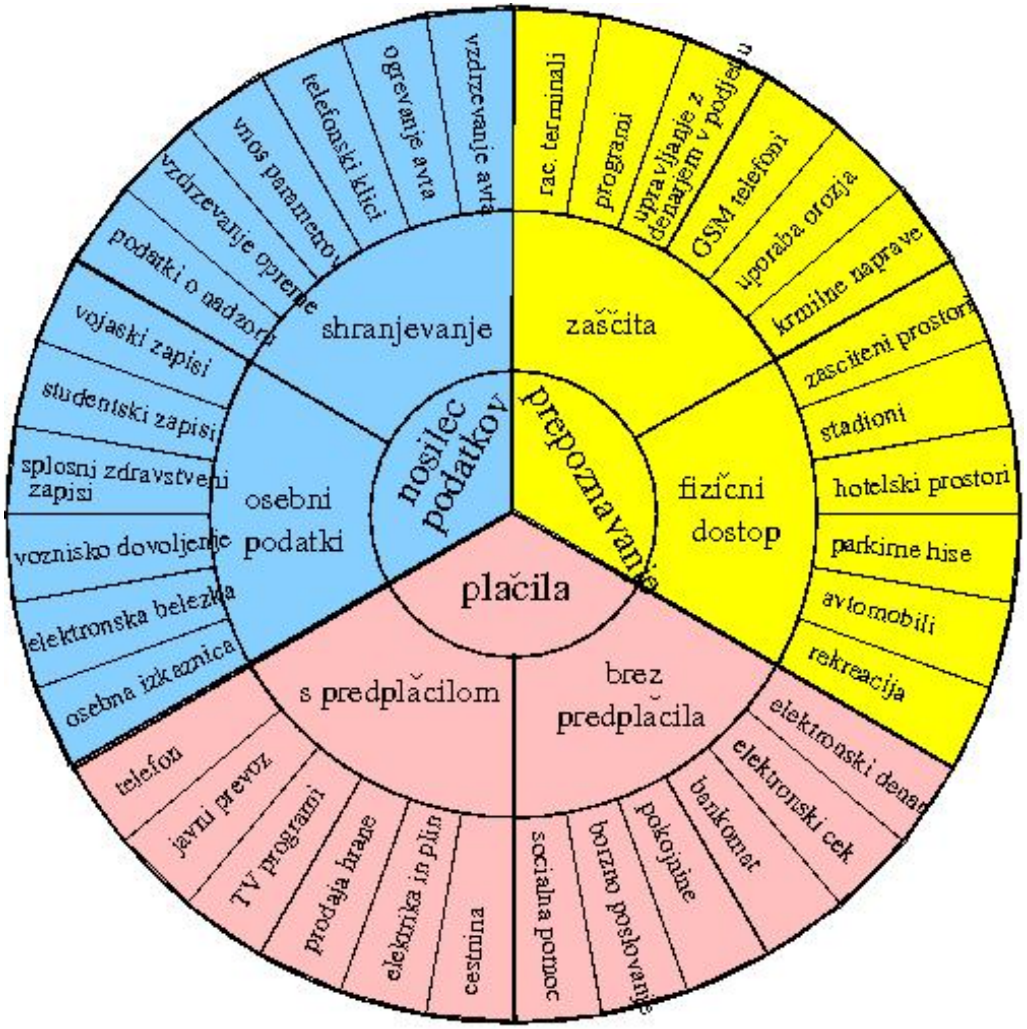
Ta ga zašifrira z zasebnim ključem in rezultat pošlje pametni kartici.

Če pametna kartica uspešno odšifrira naključno število z javnim ključem, potem je prepričana o pristnosti čitalnika.

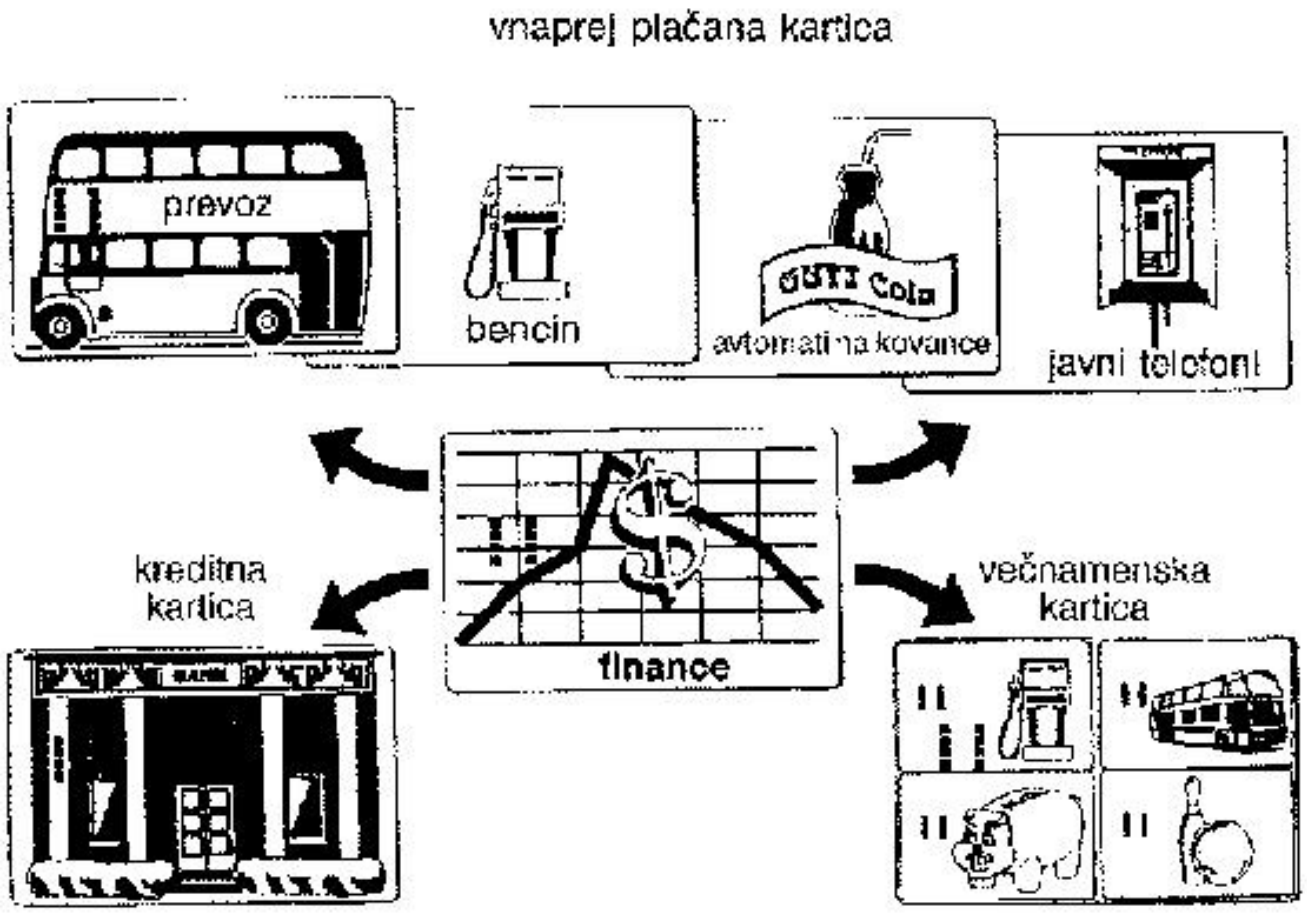


Enak proces poteka v nasprotni smeri.

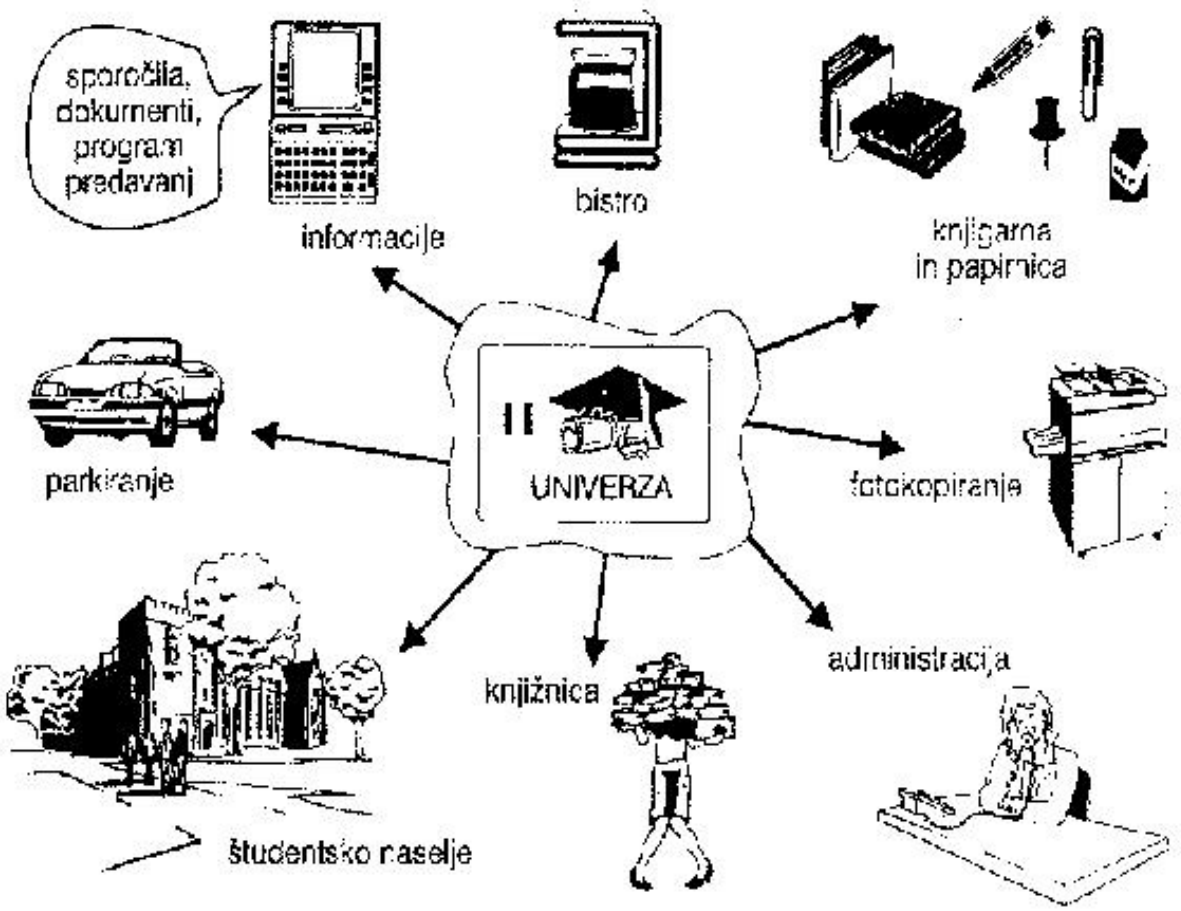
Uporaba pametnih kartic



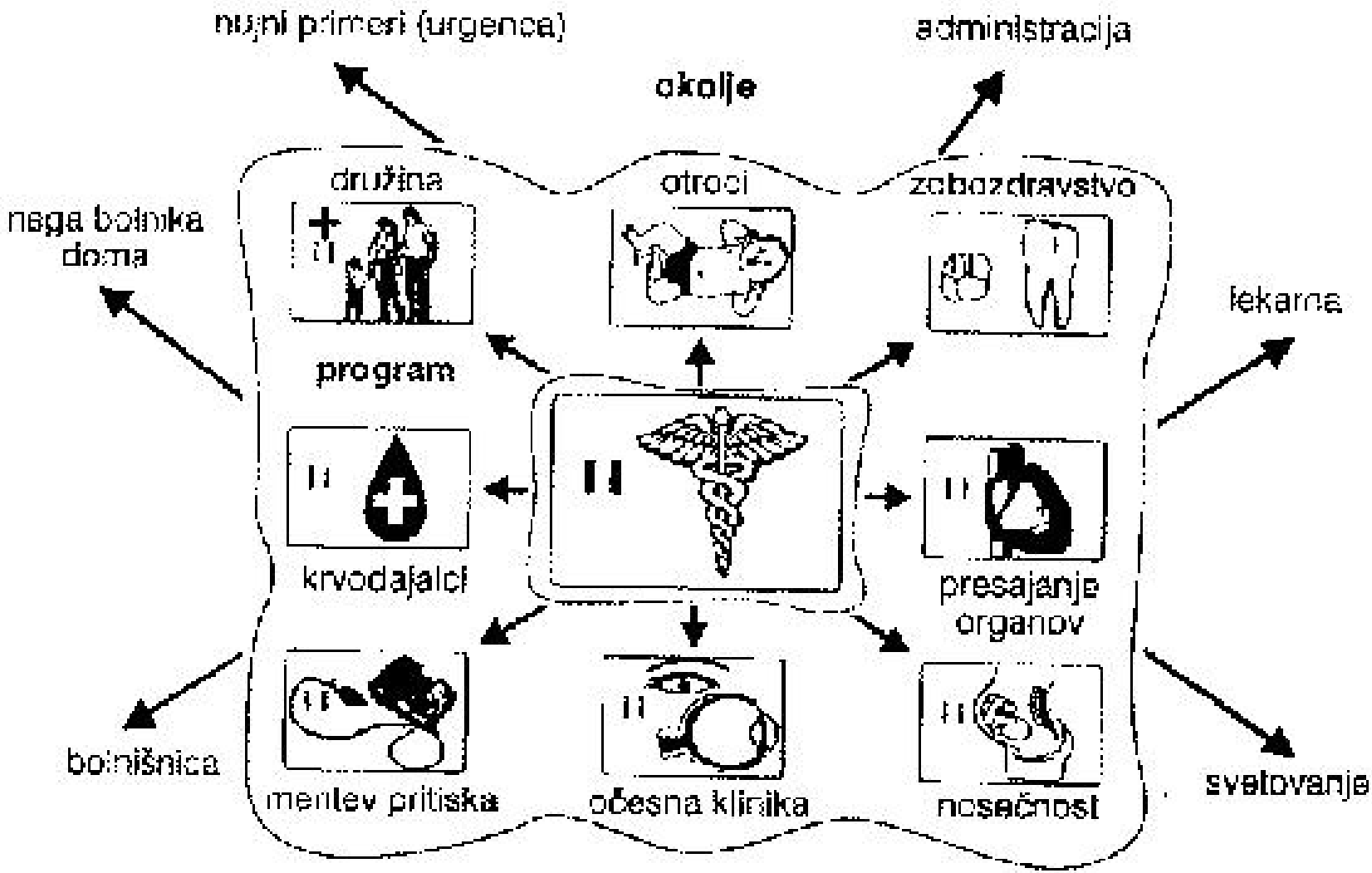
Plačilne, kreditne in večnamenske kartice, ki se uporabljajo na področju *financ*.



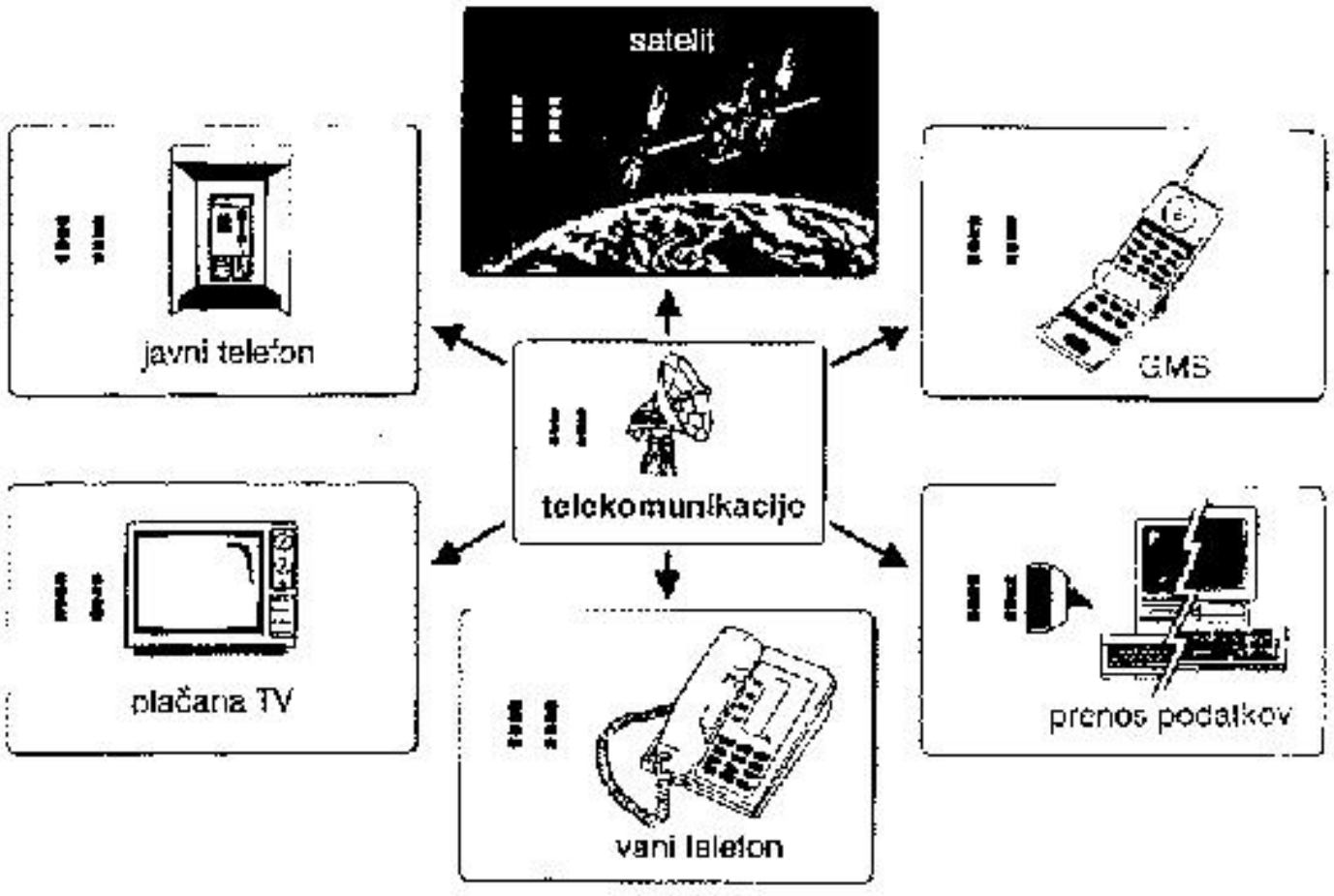
Uporaba pametnih kartic na *univerzi/fakulteti*, ki je ponekod mesto v malem.



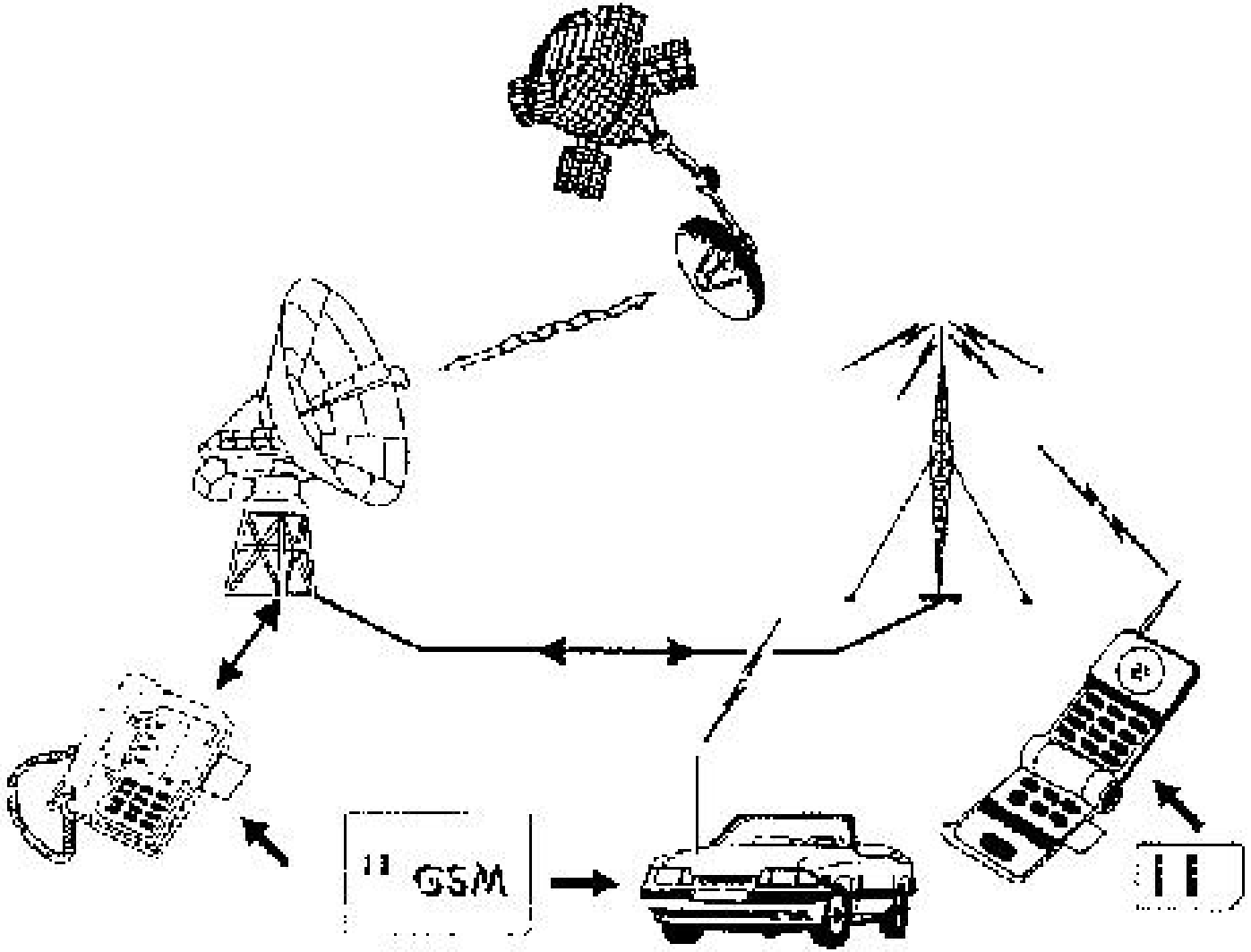
Področja v *zdravstvu*, kjer se uporabljajo pametne kartice.



Uporaba pametne kartice v *telekomunikacijah* in uporabniški elektrotehniki.



GSM (globalni sistem za prenosno komuniciranje)



Kriptografija javnih ključev

Glede na pomembnost podatkov, ki jih varujemo,
se moramo odločiti za ustrezno obliko zaščite:

- Geslo (PIN) in zgoščevalne funkcije
  predstavljajo osnovno zaščito,
- AES (Advanced Encryption Standard)
  simetrični kriptosistemi nudijo srednji nivo,
- javna kriptografija (Public Key Scheme)
  pa visok nivo zaščite.

Odlična uvodna knjiga o moderni kriptografiji je:
Albrecht Beutelspacher, **Cryptology**, MAA, 1994.