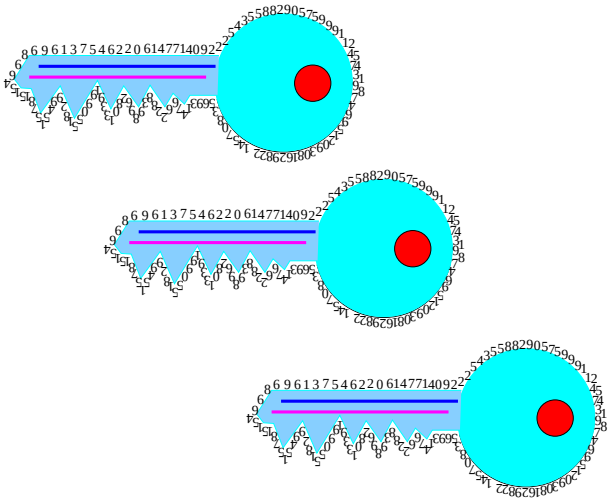
KRIPTOGRAFIJA IN RAČUNALNIŠKA VARNOST

Aleksandar Jurišić

FRI

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



Uvod Pametne kartice in javna kriptografija . 1
1. Klasična kriptografija 63
2. Shannonova teorija 110
3. Simetrični kriptosistemi 149
4. RSA sistem in faktorizacija 195
5. Drugi javni kriptosistemi 272
6. Sheme za digitalne podpise 369
7. Zgoščevalne funkcije 417
8. Distribucija ključev 475
9. Identifikacijske sheme 526
10. Kode za overjanje 560
11. Sheme za deljenje skrivnosti 586
12. Generator psevdo-naključnih števil 637
13. Dokazi brez razkritja znanja 664
Priloga A Gostota praštevil 700

Uvod

Pametne kartice 2
Kaj je pametna kartica 3
Vrste pametnih kartic 6
Zakaj pametne kartice (princip identifikacije) . . 8
Uporaba pametnih kartic 15
Certicomova kartica za digitalni podpis 21

Javna kriptografija in eliptične krivulje 25
Koncept javne kriptografije 27
ElGamalovi protokoli in digitalni podpis (DSA) . 29
Eliptične krivulje in digitalni podpis (ECDSA) . 42
Napadi na DSA in ECDSA in varnost le teh . . 47

Kaj je kriptografija (cilji, kontekst, gradniki) **53**

1. poglavje

Klasična kriptografija

Zgodovina (prikrita šifra) 64
Zamenjalna šifra 70
Pomična, afina, Vigenerjeva in Hillova šifra . . . 84
Kerckhoffov princip in stopnje napadov 91
Napad na Vigenerjeva šifra 93
Napad na Hillovo šifro 98
Tokovna šifra 100

2. poglavje

Shannonova teorija:

Popolna varnost 111
Entropija 124
Lastnosti entropije 130
Ponarejeni ključi in enotska razdalja 136
Produktni kriptosistemi 145

3. poglavje

Simetrični kriptosistemi

Nekaj zgodovine o DES-u 150
Produktna in Fiestelova šifra 151
Opis DES-a 153
Načini delovanja (ECB,CBC,CFB,OFB) in MAC 159
Napadi in velika števila 163
3-DES, DESX in drugi simetrični sistemi . . . 171
Diferenčna kriptoanaliza 172
– požrešna metoda in metoda z urejeno tabelo
– diferenčna metoda (za 1, 3, 6 in 16 ciklov)

4. poglavje

RSA kriptosistem in faktorizacija

Uvod (kriptografija z javnimi ključi) 196
Teorija števil (razširjen Evklidov algoritem) . . 198
Opis in implementacija RSA 207
Gostota praštevil 215
Generiranje praštevil 227
Probabilistično testiranje praštevilčnosti . . . 231
(Monte Carlo, Solovay-Strassen in Miller-Rabin)
Gaussov izrek (o kvadratni recipročnosti) . . . 237
Napadi na RSA (Las Vegas algoritem) 247
Rabinov kriptosistem 252
Algoritmi za faktorizacijo 260

5. poglavje

Drugi javni kriptosistemi

ElGamalovi kriptosistemi in Massey-Omura shema 278
Problem diskretnega logaritma in napadi nanj 289
Metoda velikega in malega koraka 290
Pohlig-Hellmanov algoritem 293
Index calculus 303
Varnost bitov pri diskretnem logaritmu . . . 310
Končni obsegi in eliptične krivulje 317
Eliptični kriptosistemi 328
Merkle-Hellmanov sistem z nahrbtnikom . . . 351
Kriptosistem McEliece 359

6. poglavje

Sheme za digitalne podpise

Uvod (podpis z RSA sistemom) 371
ElGamalov sistem za digitalno podpisovanje . 385
Digital Signature Standard 394
Enkratni podpis 398
Slepi podpisi 404
Podpisi brez možnosti zanikanja 406
Fail-stop podpisi 412

7. poglavje

Zgoščevalne funkcije

Zgoščevalne funkcije brez trčenj 419
Verjetnost trčenja 424
Napad s pomočjo paradoksa rojstnih dnevov . 429
Zgoščevalna funkcija z diskretnim logaritmom . 435
Razširitev zgoščevalne funkcije 442
Zgoščevalne funkcije iz kriptosistemov 453
MD4 zgoščevalna funkcija 456
SHA, RIPEMD-160 466
HMAC 470
Časovne oznake 472

8. poglavje

Distribucija ključev

Blomova shema 482
Diffie-Hellmanova distribucija ključev 492
Kerberos 499

in uskladitev ključev

Diffie-Hellmanova shema 505
MTI protokoli 516
Girault ova shema 524

9. poglavje

Identifikacijske sheme

Uporaba in cilji identifikacijskih shem 527
Protokol z izzivom in odgovorom 529
Schnorrova identifikacijska shema 530
Okomotova identifikacijska shema 541
Guillou-Quisquater 551
Pretvarjanje identifikacijske sheme 557
v shemo za digitalni podpis

10. poglavje

Kode za overjanje

Uvod 561
Računanje verjetnosti prevare 566
Kombinatorične ocene 572
– pravokotne škatle
– konstrukcije in ocene za
Ocene entropije 585

11. poglavje

Sheme za deljenje skrivnosti

Uvod 587
Stopenjske sheme za deljenje skrivnosti . . . 594
Strukture dovoljenj 601
Vizualne sheme za deljenje skrivnosti 612
Formalne definicije 617
Stopenjske sheme iz pravokotnih škatel 623
Ekvivalenca stopenjske sheme in OA 628
Informacijska mera 635

12. poglavje

Generator psevdo-naključnih števil

Kaj je naključno število 638
Algoritmično naključno število 643
Uporaba in primeri 648
Generator $1/P$ 654
Algoritem za prevdonaključne bite 659
Problem C-kvadratnih ostankov 660
Blum-Blum-Shub generator 662

13. poglavje

Dokazi brez razkritja znanja

Sistemi za interaktivno dokazovanje 666
Popolni dokazi brez razkritja znanja 671
Zapriseženi biti 689
Računski dokazi brez razkritja znanja 695
Argumenti brez razkritja skrivnosti 699

Priloga A

Dokaz izreka o gostoti praštevil

nekaj pomožnih izrekov z dokazi 702
iz analitičnega izreka izpeljemo dve posledici . 721
izrek o gostoti praštevil izpeljemo direktno iz druge posledice analitičnega izreka . 726

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

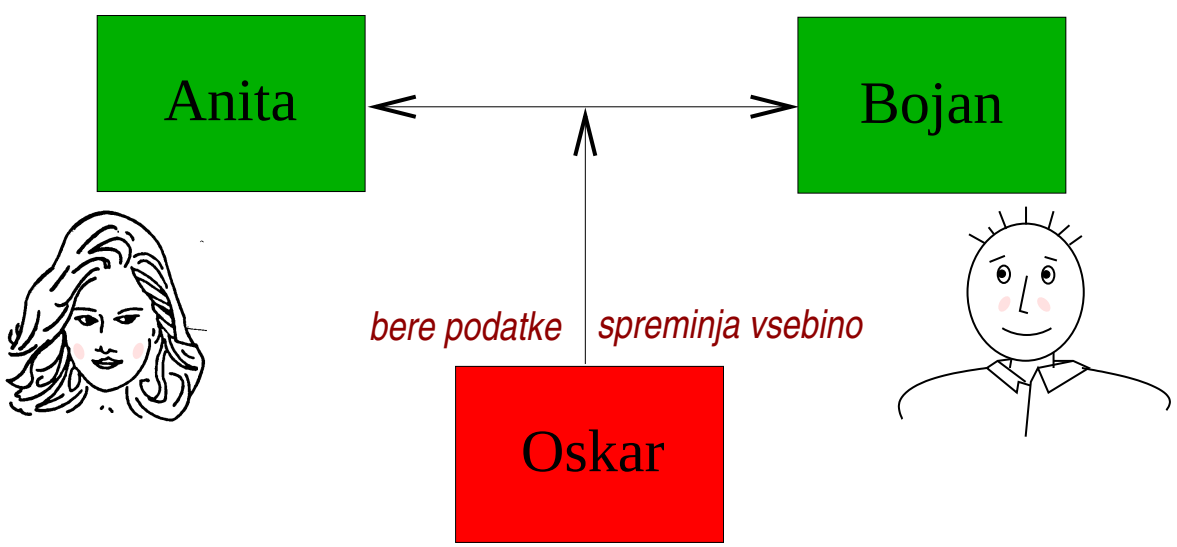
(če je seveda pravilno implementirana ter uporabljana)

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

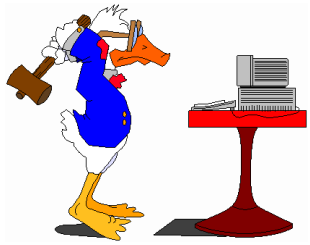
Kakšna zagotovila varnosti so na voljo? In kako?

- **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:

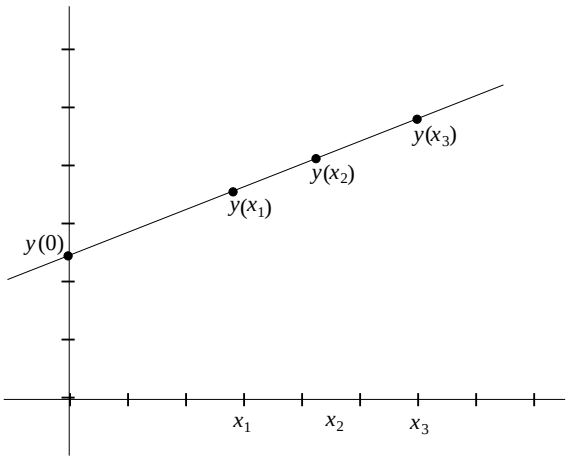
Kako vohun prepriča "stražarja", da pozna geslo, ne da bi ga izdal morebitnemu vsiljivcu/prisluškovalcu?

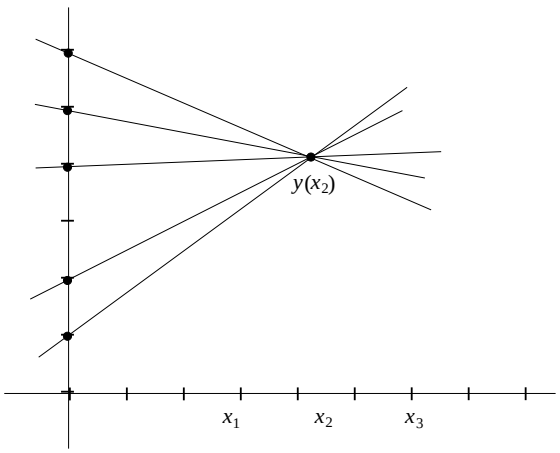
Deljenje skrivnosti

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**.

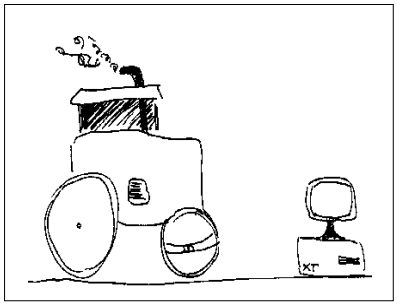


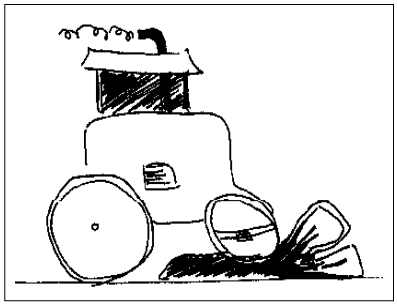
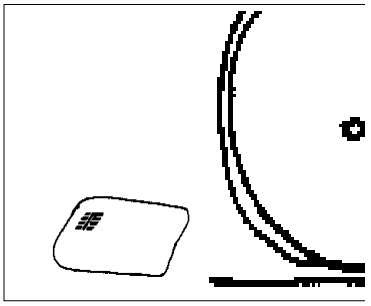


Vsak dobi le y-koordinato svoje točke.
Program v trezorju ima še ustrezne od 0 različne x- koordinate, zato lahko izračuna ključ $y(0)$.
Vsaki točki natanko določata premico in s tem ključ.

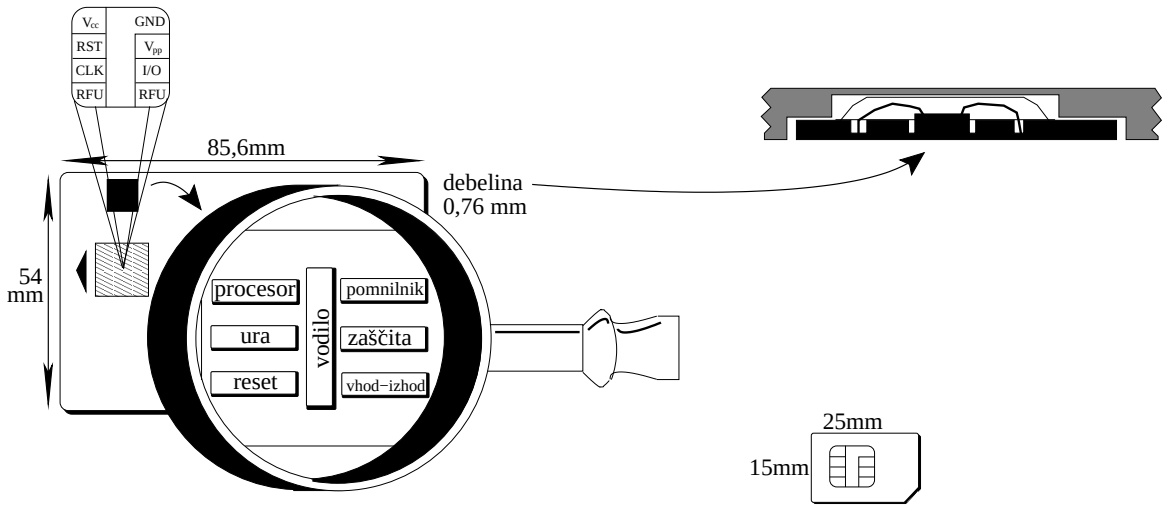
Če imamo eno samo točko, ne moremo ugotoviti, kateri ključ je pravi, saj so vsi videti enako dobri.

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.

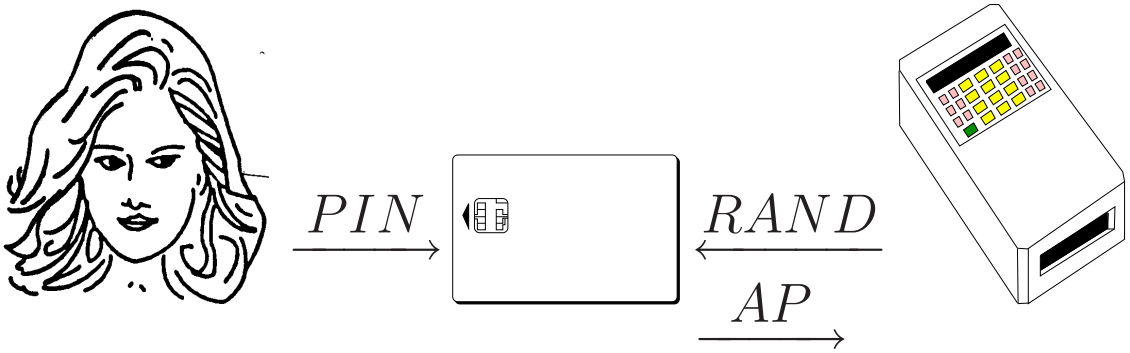
Dodaten, pomemben, del pametne kartice je **non-volatile spomin (ROM)**, t.j. spomin, ki se ga ne da spremeniti in ostane prisoten tudi po prekinitvi napajanja.

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).

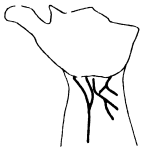


Biometrični testi

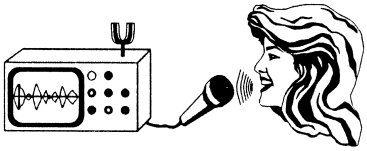
prstni odtisi

geometrija roke

odtis noge



vzorec ven
(otroci)

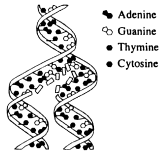


prepoznavanje glasu

vzorec zenice

prepoznavanje obraza

zapis zob



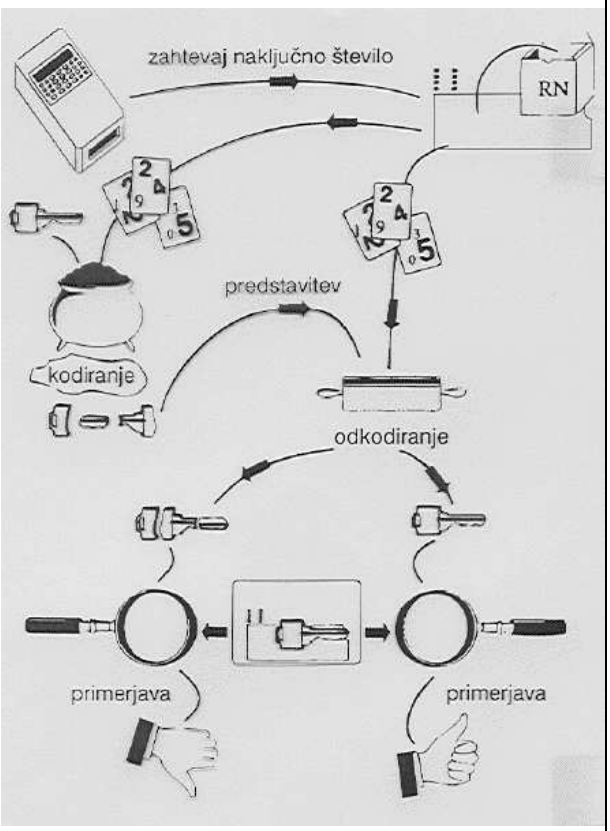
RNK (DNA)

podpis

Pametna kartica zgenerira naključno število, ter ga pošlje čitalniku.

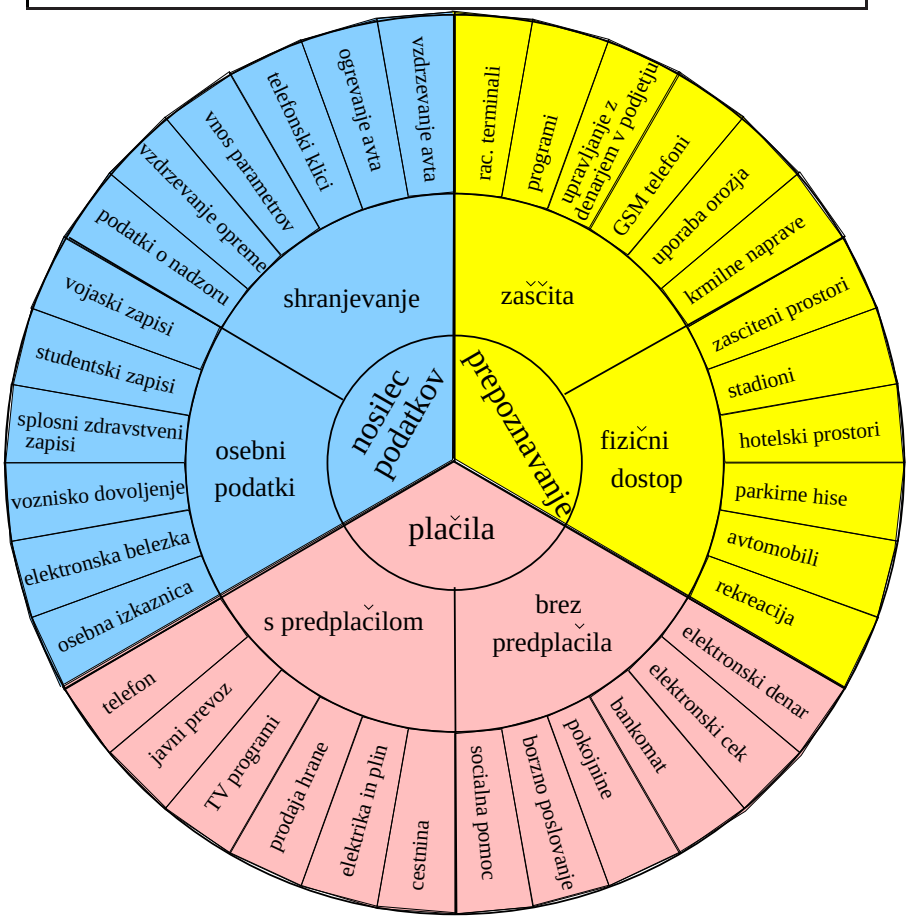
Ta ga zašifrira z zasebnim ključem in rezultat pošlje pametni kartici.

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

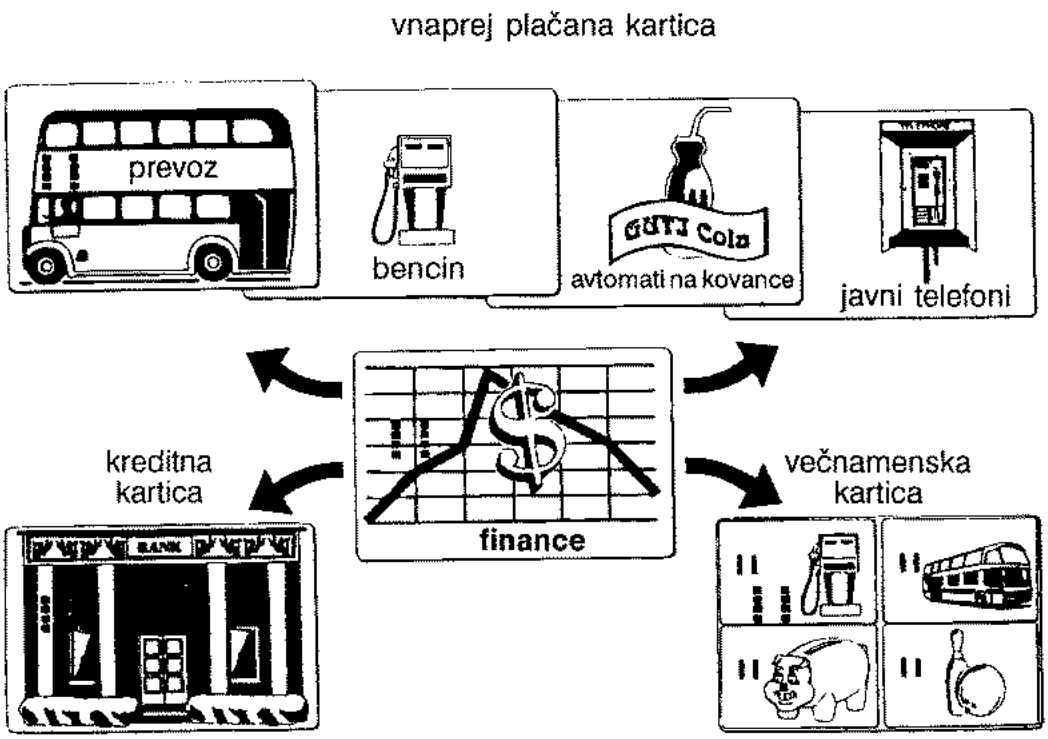


Enak proces poteka v nasprotni smeri.

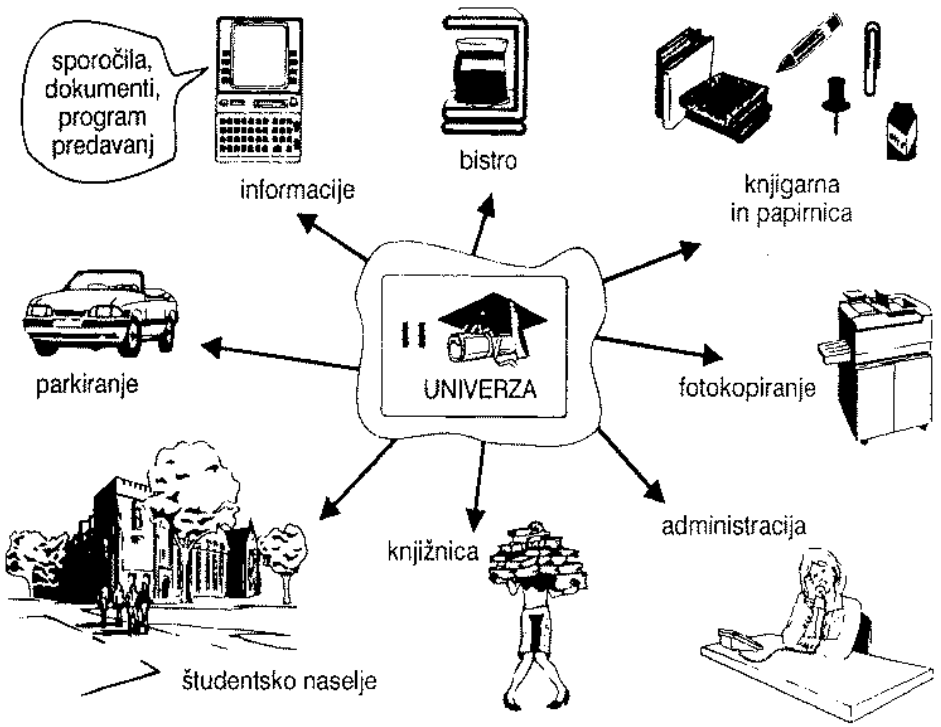
Uporaba pametnih kartic



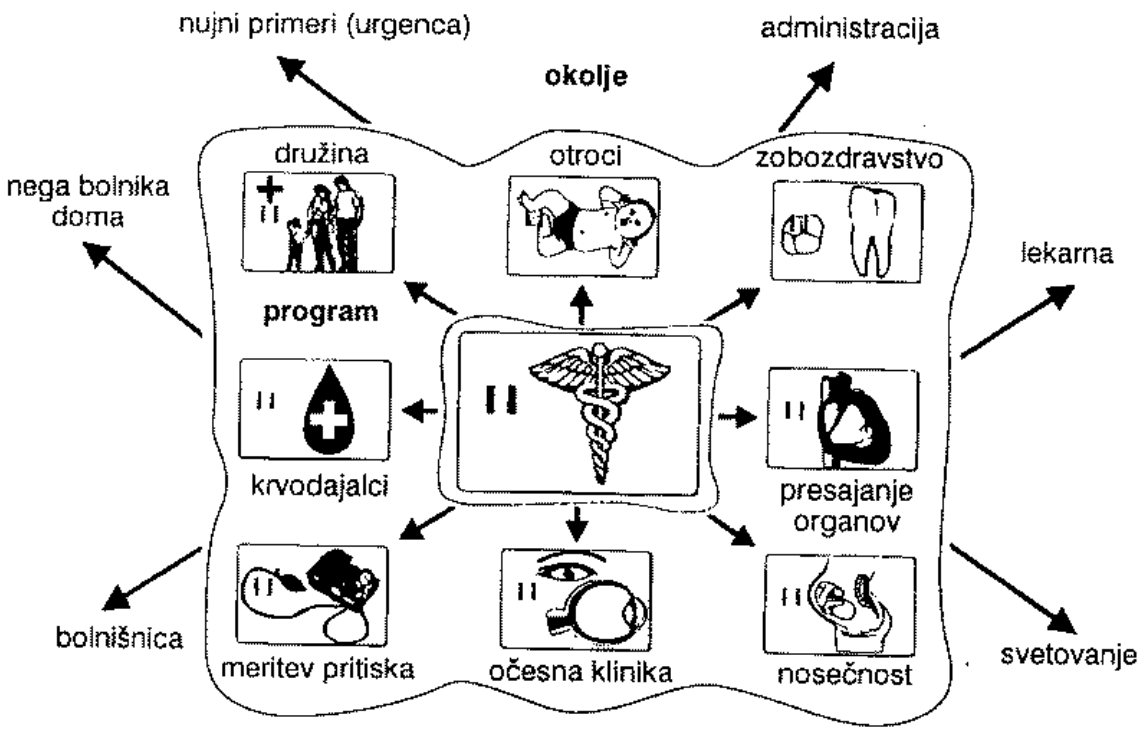
Plačilne, kreditne in večnamenske kartice, ki se uporabljajo na področju *financ*.



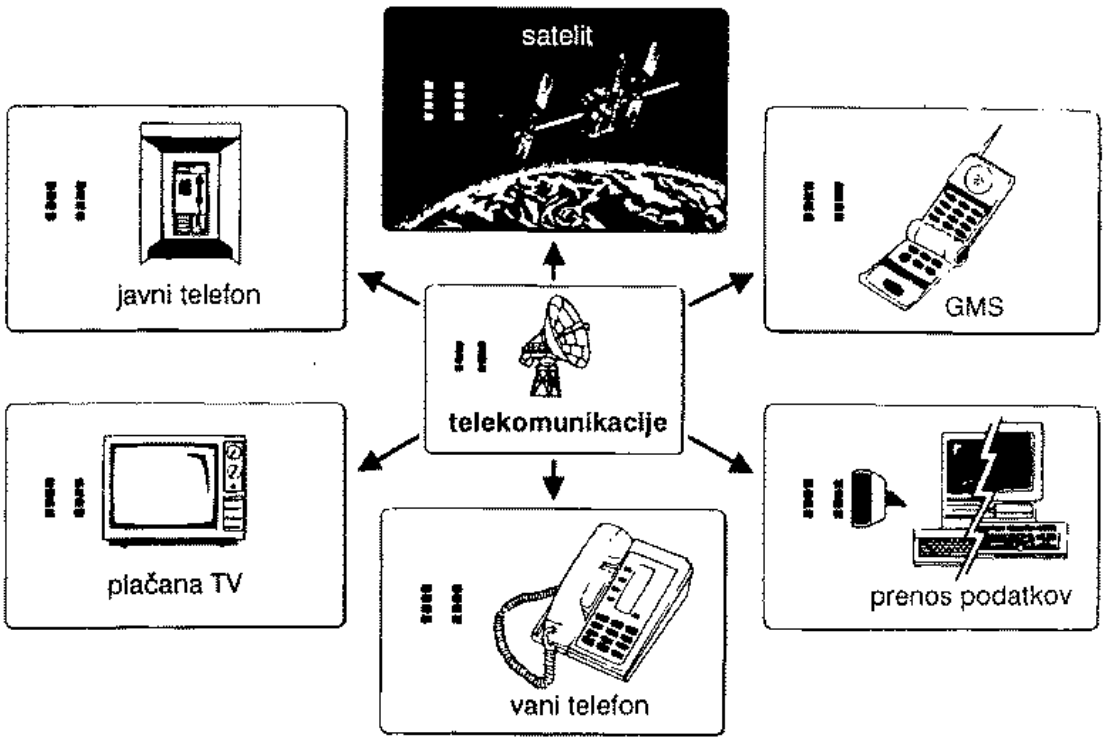
Uporaba pametnih kartic na *univerzi/fakulteti*, ki je ponekod mesto v malem.



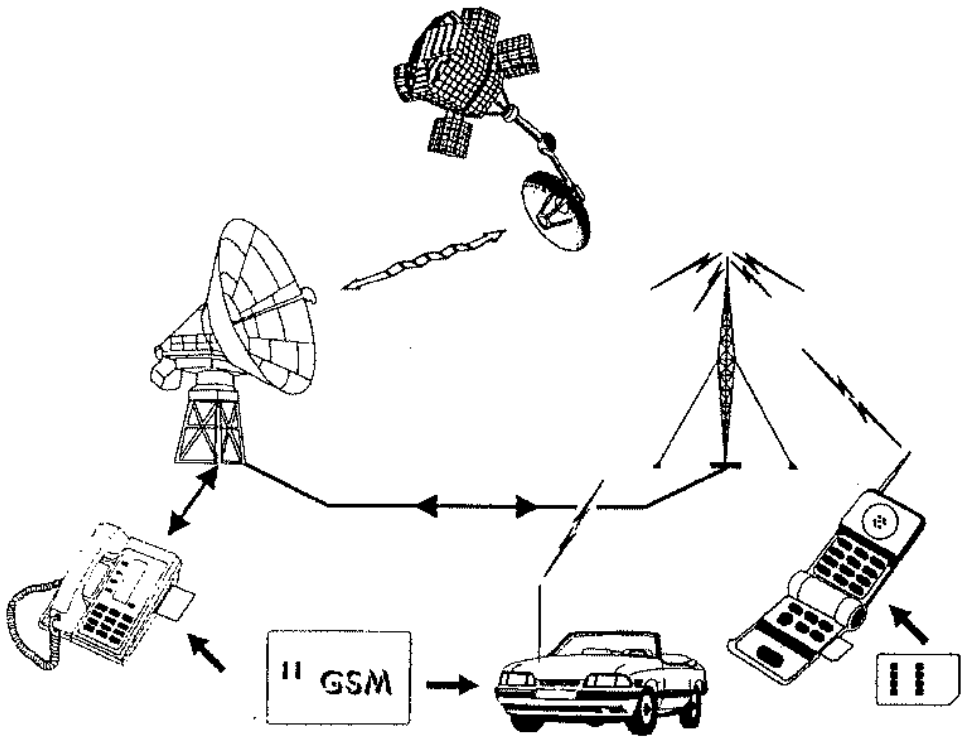
Področja v *zdravstvu*, kjer se uporabljajo pametne kartice.



Uporaba pametne kartice v *telekomunikacijah* in uporabniški elektrotehniki.



GSM (globalni sistem za prenosno komuniciranje)



Javna kriptografija

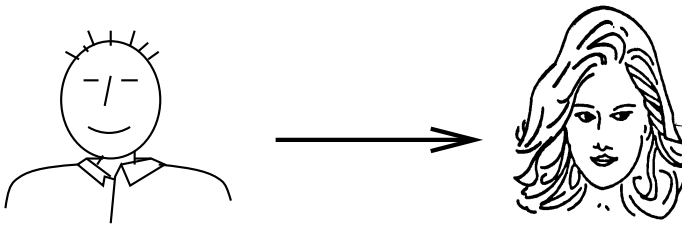
Glede na pomembnost podatkov, ki jih varujemo, se moramo odločiti za ustrezno obliko zaščite:

- 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.

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]**.

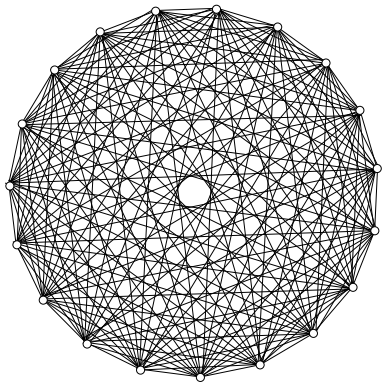
Predpostavimo, da se Anita in Bojan prej dogovorita za **skupen ključ**, ki ga ne pozna nihče drug (simetričen kriptosistem).

Če Bojan z njim zašifrira pismo, je lahko prepričan, da ga lahko odklene le Anita.

Hkrati pa je tudi Anita zadovoljna, saj je prepričana, da ji je pismo lahko poslal le Bojan.

Tak pristop je problematičen vsaj iz dveh razlogov:

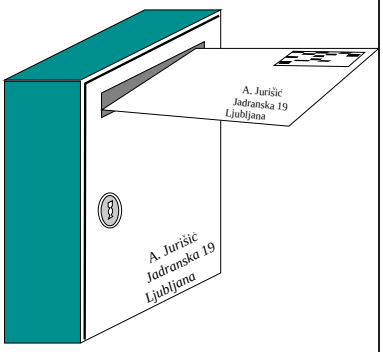
1. Anita in Bojan se morata *prej* dogovoriti za skupen ključ,
2. upravljanje s ključi v omrežju z n uporabniki je kradratne zahtevnosti $\binom{n}{2}$, vsak uporabnik pa mora hraniti $n-1$ ključev.



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.



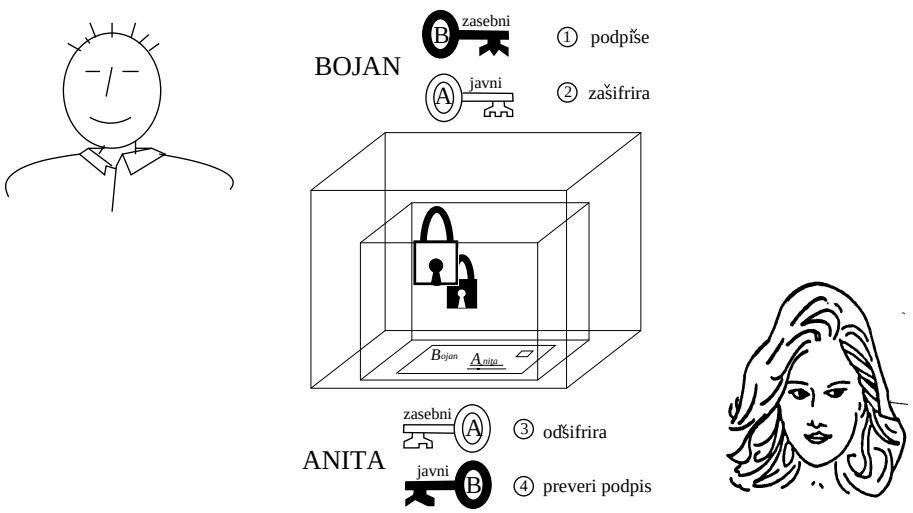
To omogoči lastniku, da en ključ objavi, drugega pa hrani v tajnosti (npr. na pametni kartici). Zato imenujemo ta ključa zaporedoma **javni** in **zasebni**.

Ta pristop omogoča veliko presenetljivih načinov uporabe, npr. omogoča ljudem varno komuniciranje, ne da bi se predhodno srečali zaradi izmenjave/dogovora o tajnem ključu.

Vsak uporabnik najprej objavi svoj javni ključ, zasebnega pa zadrži zase. Vsak lahko nato z javnim ključem zašifrira pismo, bral (odšifriral) pa ga bo lahko le lastnik ustreznega zasebnega ključa.

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.

V razvoju javne kriptografije je bilo predlaganih in razbitih veliko kriptosistemov.

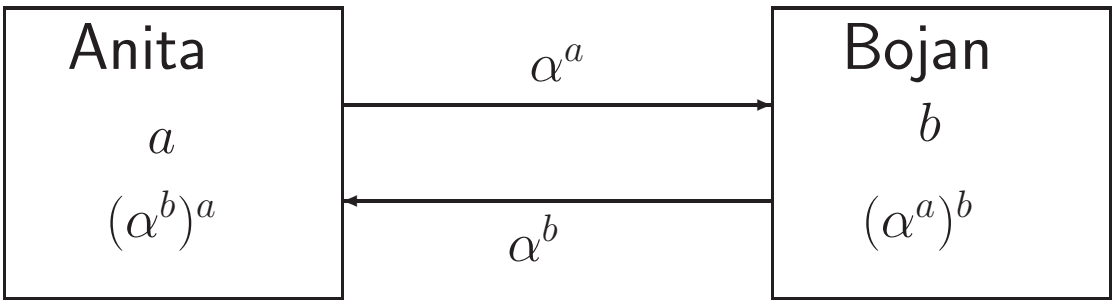
Le nekaj se jih je obdržalo in jih lahko danes smatramo za varne in učinkovite.

Glede na matematični problem na katerem temeljijo, so razdeljene v tri skupine:

- **Sistemi faktorizacije celih števil**
  npr. RSA (Rivest-Shamir-Adleman).
- **Sistemi diskretnega logaritma**
  npr. DSA.
- **Kripto sistemi z eliptičnimi krivuljami**
  (Elliptic Curve Cryptosystems)

Izmenjava ključev

(Diffie-Hellman)



Anita in Bojan si delita skupni element grupe: α^{ab}.

Končne grupe so zanimive zato, ker računanje potenc lahko opravimo učinkovito, ne poznamo pa vedno učinkovitih algoritmov za logaritem (za razliko od $\mathbb{R}$).

Kaj je kriptografija

- cilji kriptografije
- širši pogled na kriptografijo
- gradniki kriptografije

Osnovna motivacija za naš študij je uporaba kriptografije v realnem svetu.

Cilje kriptografije bomo dosegali z matematičnimi sredstvi.

Cilji kriptografije

1. **Zasebnost/zaupnost/tajnost:**
   varovanje informacij pred tistimi, ki jim vpogled ni dovoljen, dosežemo s šifriranjem.
2. **Celovitost podatkov:**
   zagotovilo, da informacija ni bila spremenjena z nedovoljenimi sredstvi (neavtoriziranimi sredstvi).

3. **Overjanje sporočila (ali izvora podatkov):**
   potrditev izvora informacij.
4. **Identifikacija:**
   potrditev identitete predmeta ali osebe.
5. **Preprečevanje tajenja:**
   preprečevanje, da bi nekdo zanikal
   dano obljubo ali storjeno dejanje.

6. **Drugi kriptografski protokoli:**

1. grb/cifra po telefonu
2. mentalni poker
3. shema elektronskih volitev
   (anonimno glasovanje brez goljufanja)
4. (anonimni) elektronski denar

Cilji kriptografije:

1. *zasebnost/zaupnost/tajnost*
2. *celovitost podatkov*
3. *overjanje sporočila (ali izvora podatkov)*
4. *identifikacija*
5. *preprečevanje nepriznavanja*
6. *drugi kriptografski protokoli*

NAUK: Kriptografija je več kot samo širfiranje (enkripcija).

Širši pogled na kriptografijo – varnost informacij

Kriptografija je sredstvo, s katerim dosežemo varnost informacij, ki med drugim zajema:

(a) Varnost računalniškega sistema

tj. tehnična sredstva, ki omogočajo varnost računalniškega sistema, ki lahko pomeni samo en računalnik z več uporabniki, lokalno mrežo (LAN), Internet, mrežni strežnik, bankomat, itd.

Med drugim obsega:

- varnostne modele in pravila, ki določajo zahteve po varnosti, katerim mora sistem ustrezati
- varen operacijski sistem
- zaščito pred virusi
- zaščito pred kopiranjem
- kontrolne mehanizme (beleženje vseh aktivnosti, ki se dogajajo v sistemu lahko omogoči *odkrivanje* tistih kršitev varnostnih pravil, ki jih ni mogoče preprečiti)
- analiza tveganja in upravljanje v primeru nevarnosti

(b) Varnost na mreži

Zaščita prenašanja podatkov preko komercialnih mrež, tudi računalniških in telekomunikacijskih.

Med drugim obsega:

- protokole na internetu in njihovo varnost
- požarne zidove
- trgovanje na internetu
- varno elektronsko pošto

Širši pogled na kriptografijo – varnost informacij

1. *varnost računalniškega sistema*
2. *varnost na mreži*

NAUK: Kriptografija je samo majhen del varnosti informacij.

Gradniki kriptografije

1. **matematika** *(predvsem teorija števil)*
2. **računalništvo** *(analiza algoritmov)*
3. **elektrotehnika** *(hardware)*
4. **poznavanje aplikacij** *(finance,...)*
5. **politika** *(restrikcije, key escrow, NSA,...)*
6. **pravo** *(patenti, podpisi, jamstvo,...)*
7. **družba** *(npr. enkripcija omogoča zasebnost, a otežuje pregon kriminalcev)*

NAUK: Uporabna kriptografija je več kot samo zanimiva matematika.

1. poglavje

Klasična kriptografija

- zgodovina (hieroglifi, antika, II. svetovna vojna)
- zamenjalna šifra

Klasične šifre in razbijanje

- prikrita, zamenjalna (pomična, afina), bločna (Vigenerjeva, Hillova)
- Kerckhoffov princip in stopnje napadov
- napad na Vigenerja (Kasiski test, indeks naključja)
- napad na Hillovo šifro
- tokovne šifre

Zgodovina

Kriptografija ima dolgo in zanimivo zgodovino:

– Hieroglifi, Špartanci, Cezar, ...

D. Kahn, **The Codebreakers**
(The Story of Secret Writing),
hrvaški prevod: (K. and M. Miles),
Šifranti protiv špijuna,
Centar za informacije i Publicitet, Zagreb 1979.
(429+288+451+325=1493 strani).

Hieroglifi

Razvili so jih antični Egiptčani.
Komunicirali so v jeziku
sestavljenemu iz sličič namesto besed.

Najbolj izobraženi ljudje so jih razumeli,
toda v religioznemu kontekstu
– **npr. napisi na grobovih** –
so njihovi duhovniki uporabljali tajne
kriptografske verzije znakov, da bi bila vsebina
več vredna (saj je šlo za božje besede) in bolj mistična.

Mnoge religije so uporabljale tajne znake,
ki so jih razumeli le določeni izbranci.

Razbijalci šifer

Obstajajo od kar poznamo šifriranje.

L. 1799 so v Egipčanski Rosetti
našli skoraj 2.000 let star kamen.
Na njemu so bili trije teksti:

- hieroglifi,
- pisava egiptčanov (demotic) in
- starogrščina.

Del kamna iz Rosette, na katerem je bila neznana pisava, dokler je arheologi niso odšifrirali.

Ko je bil končan prevod iz Grščine,
je bilo možno razvozlati tudi hieroglife,
iz katerih smo izvedeli o zgodovini antičnega Egipta.

Še ena antična: o obriti glavi

Medtem, ko je bil genialni Histius na perzijskem sodišču, je hotel obvestiti Aristagorasa iz Grčije, da dvigne upor. Seveda je bilo pomembno, da nihče ne prestreže sporočilo.

Da bi zagotovil tajnost, je Histius obril sužnja, ki mu je nabolj zaupal, mu vtetoviral na glavo sporočilo [sužnju so rekli, da mu začenjajo zdraviti slepoto] in počakal, da mu zrastejo lasje.

Sužnju je bilo ukazano, da reče Aristagorasu:

"*Obrijte mojo glavo in poglejte nanjo.*"

Aristagoras je nato zares dvignil upor.

To je primer **prikrite šifre**,
sporočilo je prisotno, a na nek način prikrito.

Poznamo mnogo takšnih primerov.

Varnost takega sporočila je odvisna od trika prikrivanja.

Tak trik je lahko odkriti, poleg tega pa ne omogoča hitrega šifriranja in odšifriranja.

To ne pride vpoštev za **resno uporabo**.

Anglija: Sir John dobi sporočilo: Worthie Sir John:- Hope, that is ye beste comfort of ye afflicted, cannot much, I fear me, help you now. That I would saye to you, is this only: if ever I may be able to requite that I do owe you, stand not upon asking me. 'Tis not much that I can do: but what I can do, bee ye verie sure I wille. I knowe that, if dethe comes, if ordinary men fear it, it frights not you, accounting it for a high honor, to have such a rewarde of your loyalty. Pray yet that you may be spared this soe bitter, cup. I fear not that you will grudge any sufferings; only if bie submission you can turn them away, 'tis the part of a wise man. Tell me, an if you can, to do for you anythinge that you wolde have done. The general goes back on Wednesday. Restinge your servant to command. - R.T.

Če vam uspe "med vrsticami" prebrati:

PANEL AT EAST END
OF CHAPEL SLIDES

verjetno ne boste občutili enakega olajšanja kot Sir John Trevanion, njemu pa je vsekakor uspelo pobegniti, sicer bi ga v gradu Colcester gotovo usmrtili prav tako, kot so Sir Charlesa Lucasa ter Sir Georga Lislea.

Druga svetovna vojna

– Enigma (Nemčija),

– Tunny (Nemčija),

– Purple (Japonska),

– Hagelin (ZDA).

Zamenjalna šifra

Tomaž Pisanski, Skrivnostno sporočilo
Presek V/1, 1977/78, str. 40-42.

```
YHW?HD+CVODHVTHVO-!JVG:CDCYJ(JV/-V?HV(
-T?HVW-4YC4(?-DJV/-(?S-VO3CWC%J(-V4-DC
V!CW-?CVNJDJVD-?+-VO3CWC%J(-VQW-DQ-VJ+
V?HVDWHN-V3C:CODCV!H+?-DJVD-?+CV3JO-YC
```

(črko Č smo zamenjali s C, črko Ć pa z D)

Imamo 26! = 403291461126656355840000000
možnosti z direktnim preizkušanjem,
zato v članku dobimo naslednje nasvete:

(0) Relativna frekvenca črk in presledkov v slovenščini:
presledek 173,

E	A	I	O	N	R	S	L	J	T	V	D
89	84	74	73	57	44	43	39	37	37	33	30

K	M	P	U	Z	B	G	Č	H	Š	C	Ž	F
29	27	26	18	17	15	12	12	9	9	6	6	1

(1) Na začetku besed so najpogostejše črke
N, S, K, T, J, L.

(2) Najpogostejše končnice pa so
E, A, I, O, U, R, N.

(3) Ugotovi, kateri znaki zagotovo predstavljajo samoglasnike in kateri soglasnike.

(4) V vsaki besedi je vsaj en samoglasnik
ali samoglasniški R.

(5) V vsaki besedi z dvema črkama je ena
črka samoglasnik, druga pa soglasnik.

(6) detektivska sreča

```
(0)  V  -  C  D  J  ?  H  W  O  (  +  3
    23 19 16 12 11 10  9  7  6  6  5  4

     Y  4  !  /  Q  :  %  T  N  S  G
     4  3  3  2  2  2  2  2  2  1  1
```

Zaključek `V --> ' '` (drugi znaki z visoko frekvenco ne morejo biti).

Dve besedi se ponovita: `03CWC%J(-`, opazimo pa tudi eno sklanjatev: `D-?+-` ter `D-?+C`.

Torej nadaljujemo z naslednjim tekstom:

```
YHW?HD+C ODH TH O-!J G:CDCYJ(J /- ?H
(-T?H W-4YD4(?-DJ /-(?S- O3CWC%J(- 4-DC
!CW-?C NJDJ D-?+- O3CWC%J(- QW-DQ- J+
?H DWHN- 3C:CODC !H+?-DJ D-?+C 3JO-YC
```

(3) Kanditati za samoglasnike e,a,i,o so znaki z visokimi frekvancami. Vzamemo:

$$\{\text{e,a,i,o}\} = \{\text{-,C,J,H}\}$$

(saj D izključi -,H,J,C in ? izključi -,H,C,
znaki -,C,J,H pa se ne izključujejo)

Razporeditev teh znakov kot samoglasnikov izgleda prav verjetna. To potrdi tudi gostota končnic, gostota parov je namreč:

AV	CV	HV	JV	VO	?H	-D	DC	JM	W-	DJ	UC	CW	-?	VD
7	5	5	5	4	4	4	3	3	3	3	3	3	3	3

(5) Preučimo besede z dvema črkama:

```
   Samoglasnik na koncu
1) da ga na pa ta za (ha ja la)
2) če je le me ne se še te ve že (he)
3) bi ji ki mi ni si ti vi
4) bo do (ho) jo ko no po so to
5) ju mu tu (bu)
6) rž rt
```

```
   Samoglasnik na začetku
1) ar as                (ah aj au)
2) en ep                 (ej eh)
3) in iz ig
4) on ob od os on        (oh oj)
5) uk up uš ud um ur (uh ut)
```

in opazujemo besedi: /- ?H
ter besedi: J+ ?H.

J+ ima najmanj možnosti, + pa verjetno ni črka n, zato nam ostane samo še:

```
J+ ?H          DWHN-
/- ?H
iz te        (ne gre zaradi: D-?+C)
ob ta(e,o)   (ne gre zaradi: D-?+C)
od te        (ne gre zaradi: D-?+C)
```

tako da bo potrebno nekaj spremeniti in preizkusiti še naslednje:
on bo; on jo; in so; in se; in je; in ta; en je; od tu ...

(6) Če nam po dolgem premisleku ne uspe najti rdeče niti, bo morda potrebno iskati napako s prijatelji (tudi računalniški program z metodo lokalne optimizacije ni zmogel problema zaradi premajhne dolžine tajnopisa, vsekakor pa bi bilo problem mogoče rešiti s pomočjo elektronskega slovarja).

Tudi psihološki pristop pomaga, je svetoval Martin Juvan in naloga je bila rešena (poskusite sami!).

Podobna naloga je v angleščini dosti lažja, saj je v tem jeziku veliko členov THE, A in AN, vendar pa zato običajno najprej izpustimo presledke iz teksta, ki ga želimo spraviti v tajnopis.

V angleščini imajo seveda črke drugačno gostoto kot v slovenščini.

Razdelimo jih v naslednjih pet skupin:

1. E, z verjetnostjo okoli 0.120,
2. T, A, O, I, N, S, H, R, vse z verjetnostjo med 0.06 in 0.09,
3. D, L, obe z verjetnostjo okoli 0.04,
4. C, U, M, W, F, G, Y, P, B, vse z verjetnostjo med 0.015 in 0.028,
5. V, K, J, X, Q, Z, vse z verjetnostjo manjšo od 0.01.

Najbolj pogosti pari so (v padajočem zaporedju): TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI in OF,

Najbolj pogoste trojice pa so (v padajočem zaporedju): THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR in DTH.

Klasične šifre

Transpozicijska šifra

V transpozicijski šifri ostanejo črke originalnega sporočila nespremenjene, njihova mesta pa so pomešana na kakšen sistematičen način

(primer: permutacija stolpcev).

Te šifre zlahka prepoznamo, če izračunamo gostoto samoglasnikov (v angleščini je ta 40%, in skoraj nikoli ne pade zunaj intervala 35%–45%).

Težko jih rešimo, vendar pa se potrpljenje na koncu običajno izplača.

Simetrična šifra *je peterica* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za katero velja:*

1. $\mathcal{P}$ *je končna množica možnih čistopisov*
2. $\mathcal{C}$ *je končna množica možnih tajnopisov*
3. $\mathcal{K}$ *je končna množica možnih ključev.*
4. *Za vsak ključ* $K \in \mathcal{K}$*, imamo šifrirni postopek* $e_K \in \mathcal{E}$ *in ustrezen odšifrirni postopek* $d_K \in \mathcal{D}$*.*

$$e_K : \mathcal{P} \longrightarrow \mathcal{C} \quad \text{in} \quad d_K : \mathcal{C} \longrightarrow \mathcal{P}$$

sta taki funkciji, da je $d_K(e_K(x)) = x$ *za vsak* $x \in \mathcal{P}$*.*

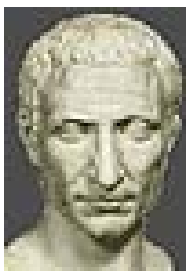
Pomična šifra (angl. shift cipher) je poseben primer zamenjalne šifre.

```
wewillmeetatmidnight

 22  4 22  8 11 11 12  4  4 19  0 19 12  8  3 13  8  6  7 19
  7 15  7 19 22 22 23 15 15  4 11  4 23 19 14 24 19 17 18  4

HPHTWWXPPELEXTOYTRSE
```

Cezarjeva šifra zašifrira njegovo ime v Ehbčt.



Cezar ukazal napad

↓

Ehbčt žnčbčo rčščg

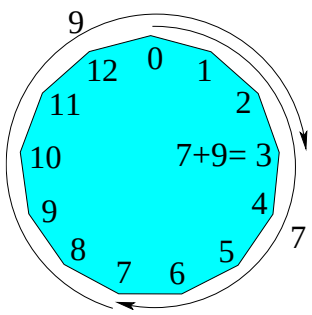
V kriptografiji si na splošno radi omislimo končne množice, kot pri številčnici na uri (npr. praštevilske obsege $\mathbb{Z}_p$).

Kongruence: naj bosta a in b celi števili in m naravno število.

$$a \equiv b \pmod{m} \iff m|b-a.$$

Primer: za $p=13$ velja
$7+_{13}9 = 7+9 \mod 13 = 3$ in
$5 *_{13} 4 = 5 * 4 \mod 13 = 7$

(saj ima pri deljenju s 13
vsota 16 ostanek 3,
produkt 20 pa ostanek 7),
možno pa je tudi deljenje.



Deljenje v primeru $p = 13$:

$*_{13}$	1	2	3	4	5	6	7	8	9	10	11	12
1	**1**	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	**1**	3	5	7	9	11
3	3	6	9	12	2	5	8	11	**1**	4	7	10
4	4	8	12	3	7	11	2	6	10	**1**	5	9
5	5	10	2	7	12	4	9	**1**	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	**1**	7
7	7	**1**	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	**1**	9	4	12	7	2	10	5
9	9	5	**1**	10	6	2	11	7	3	12	8	4
10	10	7	4	**1**	11	8	5	2	12	9	6	3
11	11	9	7	5	3	**1**	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	**1**

Afina šifra:

$$e(x) = ax + b \pmod{26} \qquad \text{za } a, b \in \mathbb{Z}_{26}$$

Za $a = 1$ dobimo pomično šifro.
Funkcija je injektivna, če in samo če je $D(a, 26) = 1$.

Imamo $|\mathcal{K}| = 12 \times 26 = 312$ možnih ključev.

Za pomično šifro in afino šifro pravimo, da sta **monoabecedni**, ker preslikamo vsako črko v natanko določeno črko.