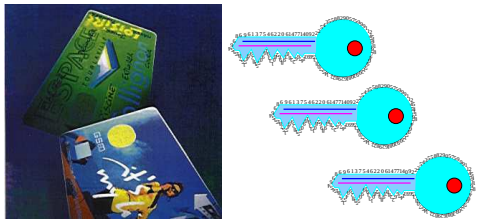
KRIPTOGRAFIJA IN TEORIJA KODIRANJA

Aleksandar Jurišić

Laboratorij za kriptografijo in računalniško varnost
FRI

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



Uvod Pametne kartice in javna kriptografija . 1
1. Klasična kriptografija 45
2. Shannonova teorija 96
3. Simetrični kriptosistemi 136
4. RSA sistem in faktorizacija 204
5. Drugi javni kriptosistemi 301
6. Sheme za digitalne podpise 391
7. Zgoščevalne funkcije 459
8. Upravljanje ključev 519
9. Identifikacijske sheme 614
10. Kode za overjanje 648
11. Sheme za deljenje skrivnosti 710
21. Teorija kodiranja 777
12. Generator psevdo-naključnih števil 850
13. Dokazi brez razkritja znanja 877
Priloga A Gostota praštevil 912-943

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

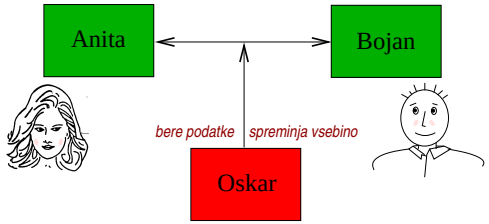
(če je seveda pravilno implementirana ter uporabljana)

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:

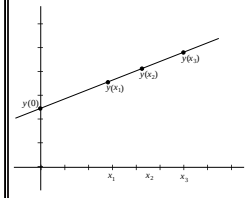
Kako vohun prepriča "stražarja", da pozna geslo, ne da bi ga izdal morebitnemu vsiljivcu/prisluškovalcu?

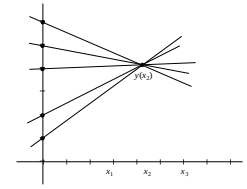
Deljenje skrivnosti

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**.

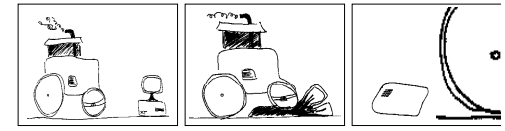




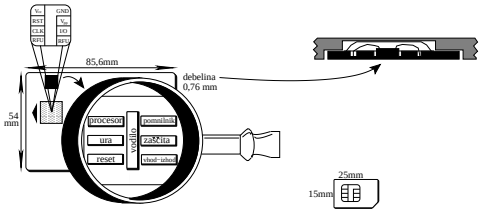
Vsak dobi le y-koordinato svoje točke.
Program v trezorju ima še ustrezne od 0 različne x- koordinate, zato lahko izračuna ključ $y(0)$.
Vsaki točki natanko določata premico in s tem ključ.

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.

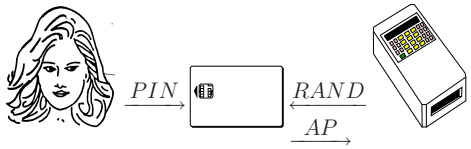
Dodaten, pomemben, del pametne kartice je **non-volatile spomin (ROM)**, t.j. spomin, ki se ga ne da spremeniti in ostane prisoten tudi po prekinitvi napajanja.

Zagotovitev varnosti

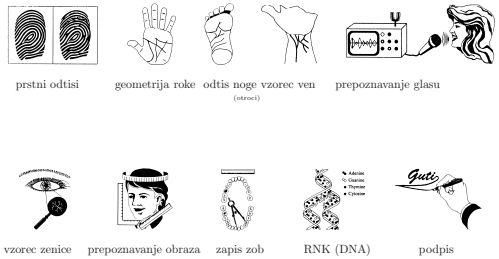
Identifikacija se opravi v dveh delih:

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

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



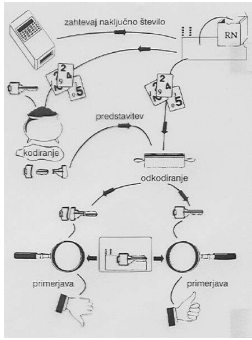
Biometrični testi



Pametna kartica zgenerira naključno število, ter ga pošlje čitalniku.

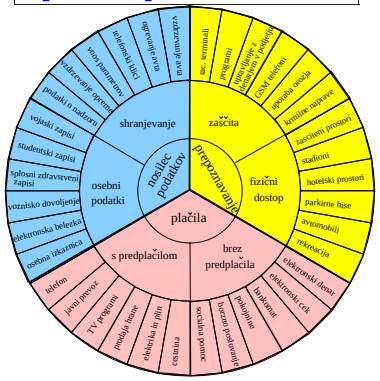
Ta ga zašifrira z zasebnim ključem in rezultat pošlje pametni kartici.

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

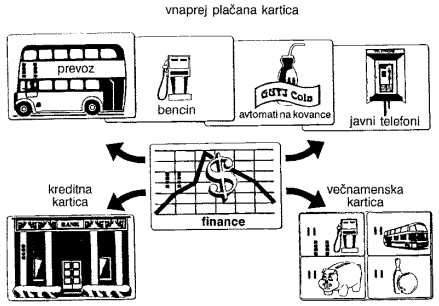


Enak proces poteka v nasprotni smeri.

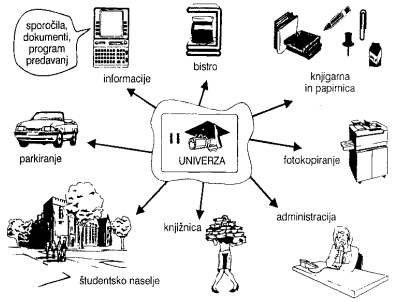
Uporaba pametnih kartic



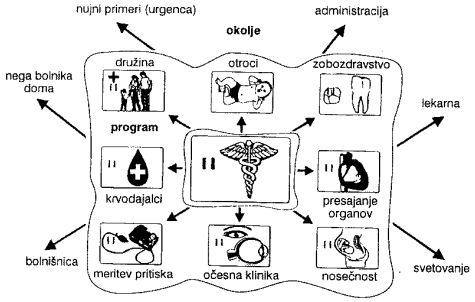
Plačilne, kreditne in večnamenske kartice, ki se uporabljajo na področju *financ*.



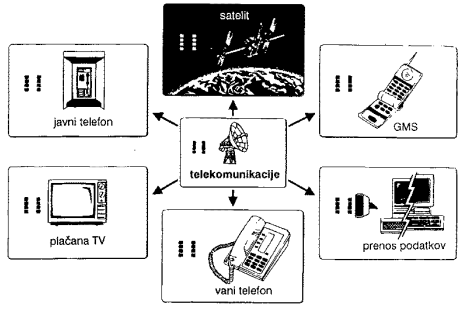
Uporaba pametnih kartic na *univerzi/fakulteti*, ki je ponekod mesto v malem.



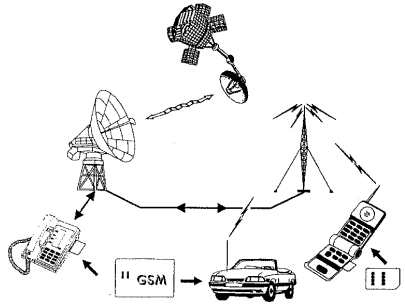
Področja v *zdravstvu*, kjer se uporabljajo pametne kartice.



Uporaba pametne kartice v *telekomunikacijah* in uporabniški elektrotehniki.



GSM (globalni sistem za prenosno komuniciranje)



Javna kriptografija

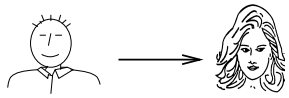
Glede na pomembnost podatkov, ki jih varujemo, se moramo odločiti za ustrezno obliko zaščite:

- 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]**.

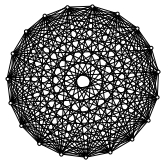
Predpostavimo, da se Anita in Bojan prej dogovorita za **skupen ključ**, ki ga ne pozna nihče drug (simetričen kriptosistem).

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:

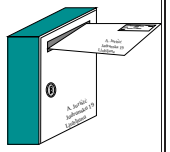
1. Anita in Bojan se morata *prej* dogovoriti za skupen ključ,
2. upravljanje s ključi v omrežju z n uporabniki je kradratne zahtevnosti $\binom{n}{2}$, vsak uporabnik pa mora hraniti $n-1$ ključev.



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.



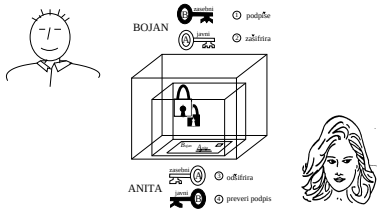
To omogoči lastniku, da en ključ objavi, drugega pa hrani v tajnosti (npr. na pametni kartici). Zato imenujemo ta ključa zaporedoma **javni** in **zasebni**.

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.

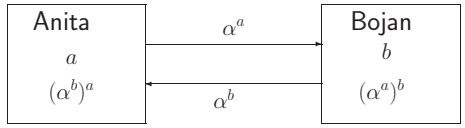
Le nekaj se jih je obdržalo in jih lahko danes smatramo za varne in učinkovite.

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.