## Pametne kartice – 2. del

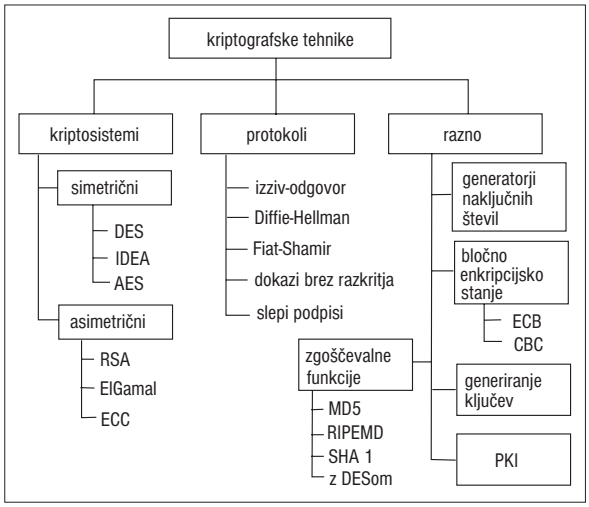
# Zasebno življenje javnih ključev

*Odkar so ljudje pričeli komunicirati, pa naj si bo to z govorom, pisavo, po radiu, telefonu, televiziji ali računalniku, so želeli tudi skriti vsebino sporočil. Ta nuja ali že kar obsedenost s tajnostjo je imela izjemen 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, če bi prišla njihova sporočila v napačne roke, izdala dragocene skrivnosti nasprotnikom in jim odkrila vitalne informacije. Danes vse to velja tudi za vodstva uspešnih podjetij in zato postaja informacijska ali računalniška varnost ena najbolj pomembnih zahtev informacijske dobe.*

Vlade, industrija in posamezniki shranjujejo informacije v digitalnem zapisu. Ta oblika nam omogoča številne prednosti pred fizičnimi oblikami: je zelo kompaktna, prenese se tako rekoč v trenutku, hkrati pa je mogoč tudi organiziran dostop do raznovrstnih zbirk podatkov. Z razvojem telekomunikacij, računalniških omrežij in obdelave informacij pa je precej laže prestreči in spremeniti elektronsko informacijo od informacije, napisane na papir. Prav zato so se povečale zahteve po varnosti. Pametne kartice lahko odigrajo odločilno vlogo ter prek računalniških omrežij združijo telekomunikacije in računalnike.

## Računalniška varnost

Informacijska in računalniška varnost (glej tudi Monitor, marec 2000, str. 108, in Sistem, marec 2001, str. 14) obsega vse preventivne postopke in sredstva, s katerimi preprečujemo nepooblaščeno uporabo elektronskih podatkov ali sistemov, ne glede na to, ali gre pri tem za razkritje, spreminjanje, zamenjavo, uničenje ustreznih podatkov ali za preverjanje verodostojnosti informacij, kot sta digitalni denar (vrednost) in digitalni podpis (prepoznavanje). Niti eden od številnih predlaganih ukrepov ne zagotavlja 100 % varnosti. Med preventivnimi ukrepi, ki so danes na voljo, omogočajo kriptografija (tajnopisje) in kriptografski sistemi (glej sliko 1), če so seveda pravilno izvedeni in uporabljeni, največjo stopnjo varnosti glede na prilagodljivost digitalnim nosilcem.




Slika 1: Delitev kriptografskih tehnik, ki se uporabljajo za pametne kartice.

V širšem smislu kriptografski sistem pretvori elektronske podatke v obliko, ki lastniku zagotavlja njihovo varnost. Glede na varnostne zahteve ali potrebe zagotovila pomenijo, da podatkov ni moč spremeniti, ne da bi kdo opazil, ali pa da je informacija prikrita vsem nepooblaščenim osebam. Pri kriptografiji upoštevamo Kerckhoffov princip, poimenovan po Augustu Kerckhoffu (1835–1903), ki pravi, da

**»nasprotnik« pozna kriptosistem in algoritme, ki jih uporabljamo, ne pa tudi ključev, ki nam zagotavljajo varnost.**

Posledica tega splošno znanega (čeprav pogosto tudi zanemarjenega) načela je, da

# logije

**stran 44** Pametne kartice
Pomemben in razširjen sistem varnosti je sistem kombinacije javnih in zasebnih ključev.

**stran 52** GPRS
GPRS poleg večjih hitrosti nudi tudi učinkovitejšo izrabo omrežne infrastrukture in primernejše obračunavanje storitve.

**stran 56** HSCSD in GPRS v praksi
Preizkusili smo, kako hitri sta novi tehnologiji pri prenosu podatkov.

je večina algoritmov, ki jih uporabljamo v civilnem sektorju, objavljenih in tudi standardiziranih. S tem preverimo njihovo pravo moč, zagotovimo večjo povezanost in nižje stroške.

Nasprotje Kerckhoffovega principa pa je zagotavljanje varnosti s skrbnim varovanjem algoritmov. V tem primeru torej napadalec ne pozna niti sistema, niti tega, kako deluje. To je zelo zastarel pristop, ki pa se še danes uporablja. Doslej je bil vsak sistem, katerega varnost je slonela samo na tem principu, razbit (običajno v zelo kratkem času). V današnji informacijski družbi je izjemno težko dalj časa skrivati tehnične podrobnosti in tajne sisteme.

## Osnove kriptografije

Preden se poglobimo v varnost, bomo naredili kratek uvod v kriptografijo (tajnopisje), tako klasično kakor moderno, glej sliko 1. Dostop do svojega računa na računalniku običajno zavarujemo z geslom. Le-to je v večini primerov shranjeno na disku, zašifrirano s simetričnim kriptosistemom (npr. DES) ali pa zgoščeno z zgoščevalno funkcijo (npr. SHA-1). Vedno obstaja možnost (pa če še tako majhna), da geslo kdo ugane. Da bi dobili občutek, za kakšne možnosti gre, ko si pri tem pomagamo še z današnjim računalnikom, si oglejmo tabelo 1. Velja pa omeniti, da je za shranjevanje gesel na disku bolje uporabljati čim počasnejšo funkcijo, saj sekunda čakanja med preverjanjem gesla ni predolga, medtem ko je ena sekunda za preizkus vsakega potencialnega gesla precejšna ovira za morebitnega napadalca.

| primer | število znakov | zahtevnost | dolžina gesla | čas za razbijanje |
|---|---|---|---|---|
| mucka | 5 | 25 (majhne črke) | 24 bitov | 40 minut |
| br1a9Az | 7 | 62 (črke in številke) | 42 bitov | 22 let |
| TH,X1lb<V+ | 10 | 95 (znaki na tipkovnici) | 65 bitov | nedosegljivo |

▲ Tabela 1: Uganjevanje fraz, ki jih uporabljamo za gesla.

Klasičen problem mnogih varnostnih sistemov se pojavi, ko napadalec izve geslo. Ne glede na to, ali je do njega prišel z grožnjami, izsiljevanjem, prisluškovanjem, podkupovanjem ali krajo, je poznavanje gesla dovolj, da ogrozi varnost sistema. Ker torej geslo ni idealna izbira za zaščito pametnih kartic, se pogosto odločimo še za biometrične preizkuse.

Če že ne moremo imeti 100 % varnosti, pa nam je na voljo vsaj popolna varnost, kar pomeni, da je za napadalca vsak ključ enako verjeten in se zato ne more odločiti za pravega. Enkratni ščit (angl. *one time pad*) je najbolj znana izvedba popolne varnosti. Leta 1917 ga je patentiral Gilbert Vernam za avtomatizirano šifriranje in odšifriranje telegrafskih sporočil. Poenostavljeno ga predstavimo kar v binarni obliki, kjer šifriranje in odšifriranje potekata tako, da sporočilu ali tajnopisu z »ekskluzivnim ali« (XOR) prištejemo enako dolgo naključno zaporedje. Čeprav se ta sistem v praksi uporablja še danes, pa je njegova slaba stran dolžina ključa in dejstvo, da nimamo več popolne varnosti, če isti ključ uporabimo več kakor enkrat. Namesto na popolno varnost smo se v praksi prisiljeni zanašati na računsko varnost, t.j. na takšne kriptosisteme, pri katerih so prostorske ali pa časovne potrebe za razbijanje večje od tistih, ki jih ima na voljo napadalec.

Sedaj pa predstavimo glavna junaka kriptografije. To sta Anita in Bojan, ki želita komunicirati. Seveda Anita in Bojan nista nujno osebi. Po vsej verjetnosti sta računalnika v nekem omrežju, kot je na primer internet. Moderna kriptografija, ki jo uporabljamo v praksi, poskuša rešiti naslednje probleme:

- **Zasebnost**: sporočila, ki ga Bojan pošlje Aniti, ne more prebrati nihče drug.
- **Overjanje**: Anita ve, da je lahko le Bojan poslal pravkar prejeto sporočilo.
- **Celovitost**: Anita ve, da Bojanovega sporočila ni mogel nihče spreminjati.
- **Zanikanje (preprečevanje tajenja)**: Bojan pozneje ne more trditi, da ni poslal sporočila, prav tako pa tudi Anita pozneje ne more trditi, da ni prejela sporočila.

Prepričajmo se, da so zgornje lastnosti zares pomembne. Kupec Bojan želi kupiti izdelek od prodajalke Anite prek interneta in zato ji pošlje podatke, ki vsebujejo številko njegove kreditne kartice in podrobnosti o plačilu in izdelku. Kupec Bojan zahteva zasebnost, saj ne želi, da bi kdo izvedel številko njegove kreditne kartice ali pa kaj je oziroma bo kupil.

Prodajalka Anita hoče biti prepričana o pristnosti pisma, vedeti mora, da je sporočilo poslal res kupec Bojan in ne kakšen vsiljivec. Oba, Anita in Bojan, morata biti prepričana o celovitosti sporočila, npr. nihče ne sme spremeniti vrednosti plačila. In navsezadnje kupec Bojan ne more zanikati, da je poslal navodila, prodajalka Anita pa trditi, da navodil ni prejela. Torej želimo, da pride v javnem omrežju do transakcije med dvema strankama, ki si medsebojno ne zaupata. Javna omrežja se razlikujejo od zasebnih, ki so se običajno uporabljala v bančništvu (npr. EDI) in so imela hierarhije ključev ter strojno opremo, kar je omogočalo varno shranjevanje ključev.

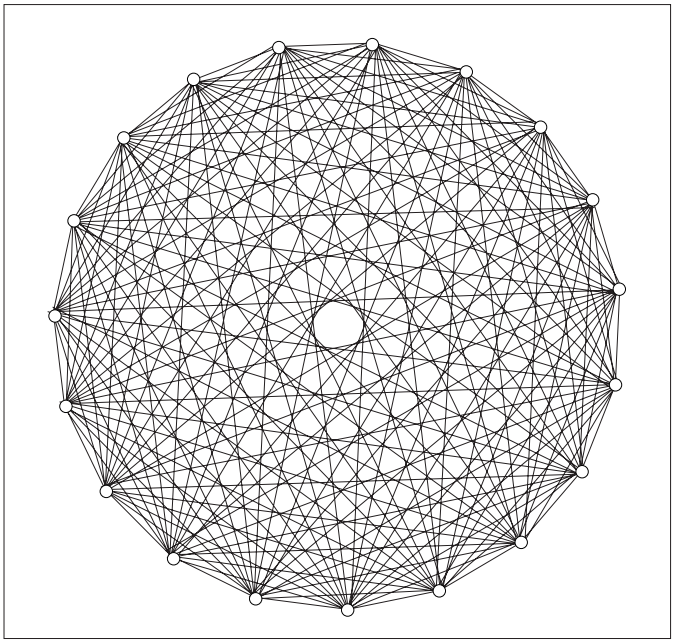
## Simetrični kriptosistemi

Za začetek predpostavimo, da si Bojan in Anita zaupata in da sta se prej dogovorila za skupni ključ, ki ga ne pozna nihče drug. Zaradi simetrije med Anito in Bojanom pravimo, da gre za simetrični kriptosistem (npr. DES ali IDEA). Če Bojan z njim zašifrira pismo, je prepričan, da ga lahko odšifrira le Anita. Hkrati pa je tudi Anita zadovoljna, saj je prepričana, da pismo izvira od Bojana.

V zadnjem času je prišlo do večjega napredka pri simetričnih kriptosistemih. *National Institute of Standards and Technology (NIST)* je v letu 2000 za nov *Federal Information Processing Standard (FIPS)* izbral belgijski bločni kriptosistem Rijndael (dolžina ključev ali blokov je 128, 196 ali 256). Njegovo ime je *Advanced Encryption Standard (AES)* in bo pri ameriški vladi nadomestil DES, glej

http://csrc.nist.gov/encryption/aes/round2/r2report.pdf. Kljub teoretični rešitvi je pristop s simetričnim kriptosistemom problematičen v praksi vsaj iz dveh razlogov:

- Anita in Bojan se morata prej dogovoriti za skupen ključ,



Slika 2: Če v simetričnem sistemu predstavimo uporabnike s točkami, je ključ za vsak par predstavljen z ustrezno povezavo. Že pri dvajsetih uporabnikih postane prostor okrog vsakega uporabnika precej zapolnjen.

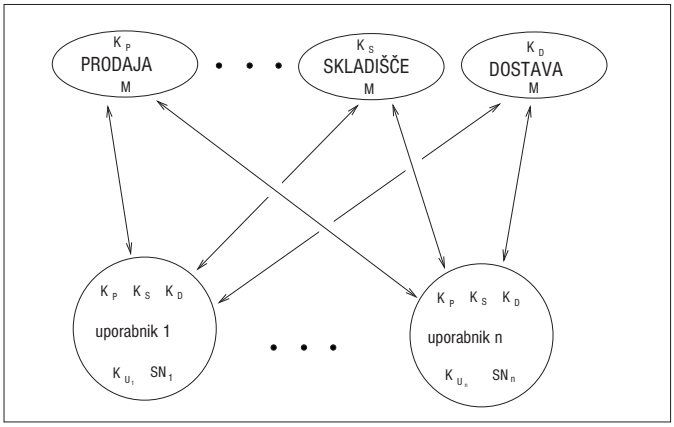
- z večanjem omrežja narašča zahtevnost upravljanja ključev v omrežju za vsakega uporabnika.

Da dobimo občutek, kakšen problem predstavlja prostor za shranjevanje ključev, si najprej oglejmo sliko 2, nato pa predpostavimo, da za shranjevanje ključev uporabljamo pametne kartice z 8 Kb pomnilnikom.

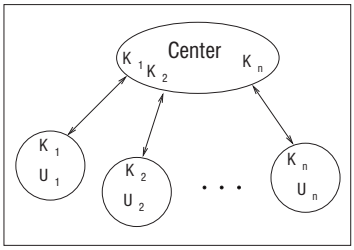
Ob predpostavki, da uporabljamo 128-bitne ključe, lahko v ta prostor shranimo 512 ključev. Če bi hoteli tak sistem uporabljati na primer v velikem trgovskem podjetju, na pošti ali v zdravstvu in bi želeli, da poljubna dva uslužbenca komunicirata varno, bi bilo 512 ključev absolutno premalo. Zato se v praksi problemu s prostorom izognemo tako, da uporabnike razdelimo v skupine. Za lažjo predstavo si oglejmo sliko 3.

Vsak uporabnik ima svoj ključ in ključe vsake skupine. Vsaka skupina ima ključ za to skupino in t.i. »glavni« ključ (angl. master key), s katerim lahko iz serijske številke uporabnika izračuna uporabnikov ključ. S temi ključi se uporabnik in skupina medsebojno overita s protokolom vrste izziv-odgovor, glej sliko 4.

Vendar pa imajo vsi sistemi, ki temeljijo na takšni simetrični shemi, kar nekaj pomanjkljivosti. Ena večjih je ta, da varnost celotnega sistema temelji na varnosti ene same kartice. Če namreč uspemo razbiti varnost uporabniške kartice, se dokopljemo do vseh skupinskih ključev, zato se lahko predstavimo preostalim uporabnikom kot katerakoli skupina, ne da bi uporabnik lahko posumil, da ne komunicira s pravim članom skupine. Če pa se dokopljemo do glavnega ključa, potem lahko preprosto ponarejamo uporabniške kartice, saj si serijsko številko izmislimo, us-




Slika 3: Delitev na skupine v trgovskem podjetju. S *K* so označeni posamezni ključi, glavni ključ je označen z *M*. Vsak uporabnik ima tudi enolično serijsko številko $SN_i$.



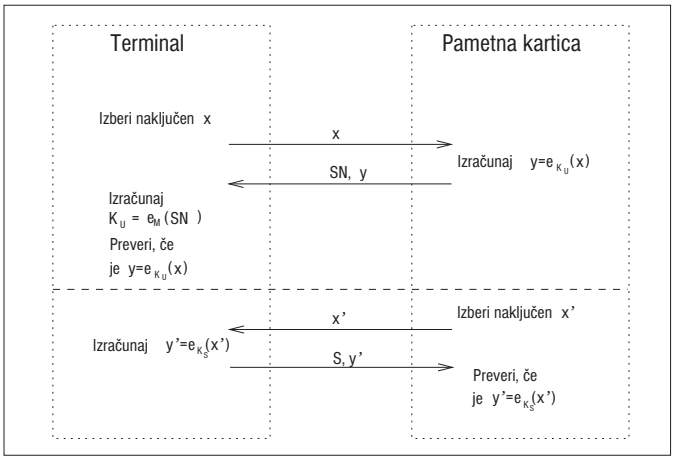

Slika 5: Centralna rešitev s simetričnim sistemom.

trezni uporabnikov ključ pa nato z glavnim ključem preprosto izračunamo.

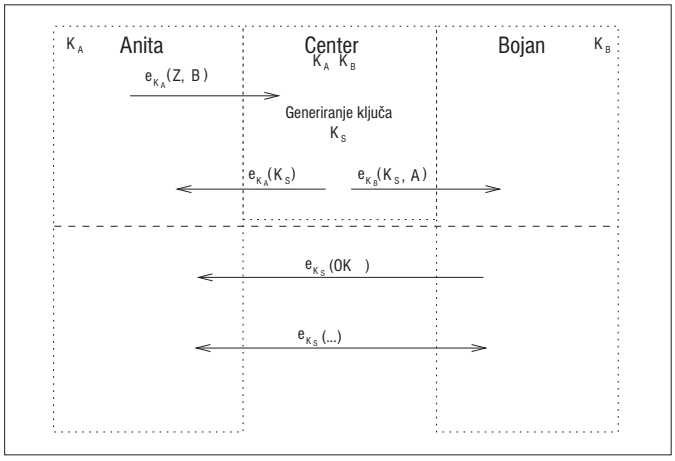
Druga pomanjkljivost je ta, da so si vse osebe znotraj ene skupine enakovredne, t.j., če uporabnik komunicira npr. z osebo iz skladišča, lahko katerakoli oseba iz skupine skladišča prisluškuje pogovoru. Poleg tega je shema povsem neuporabna, če nimamo naravne hierarhične zgradbe, ki nam omogoča delitev na skupine.

Druga rešitev problema s prostorom je prikazana na sliki 5.

V tem primeru imamo center, s katerim si vsak uporabnik deli skrivni




Slika 4: Zgled preprostega protokola vrste izziv-odgovor. Pametna kartica predstavlja uporabnika, terminal pa skupino. V zgornjem delu terminal overi pametno kartico z glavnim ključem *M* in serijsko številko kartice (*SN*), v spodnjem delu pa kartica overi terminal s skupinskim ključem $K_S$. Kartica vsebuje samo $K_U$ in $K_S$ ne pa tudi *M*, medtem ko terminal ne pozna $K_U$, ampak ga izračuna z *M*. Šifrirna funkcija *e* je simetrični kriptosistem.




Slika 6: V prvem koraku Anita pošlje centru zašifriran zahtevek za pogovor z Bojanom. Center nato ustvari sejni ključ in ga zašifriranega pošlje obema. Bojanu tudi sporoči, kdo želi komunicirati z njim. Bojan pošlje sporočilo Aniti, da potrdi sprejetje ključa. Nato se začne komunikacija.

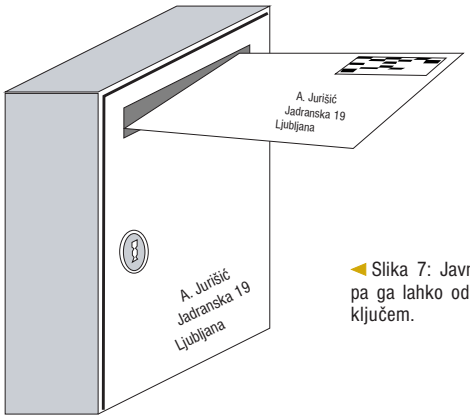
ključ. Ko želi Anita komunicirati z Bojanom, pošlje centru zašifriran zahtevek. Center generira sejni ključ in zašifriranega pošlje Aniti in Bojanu. Bojan nato obvesti Anito, da je prejel ključ in komunikacija se lahko začne. Celoten potek je prikazan na sliki 6.

Očitna pomanjkljivost te sheme je, da moramo vsakič, ko želimo komunicirati, najprej vzpostaviti povezavo s centrom. Pogosto to ni zaželeno ali sploh ni možno. Če uporabniški ključi v centru niso primerno zaščiteni, je varnost celotne sheme ogrožena.

Zaradi teh pomanjkljivosti se sheme, ki temeljijo na simetričnih sistemih, uporabljajo bodisi v zaprtih okoljih bodisi tam, kjer ni velike potrebe po varnosti. Takšne sheme se na primer uporabljajo za kartice, na katerih so shranjeni administrativni podatki, tako da ni treba ročno vnašati podatkov v formularje. Za shranjevanje občutljivih podatkov pa so takšne sheme primerne le v zaprtih okoljih, kjer so vsi uporabniki ves čas povezani v omrežje.V nadaljevanju bomo spoznali boljše sheme, ki omogočajo komunikacijo med poljubnima uporabnikoma in so dovolj varne tudi za najbolj občutljive podatke.

## Koncept javne kriptografije

Leta 1976 sta Whit Diffie in Martin Hellman v članku *New Directions in Cryptography*, (Institute of Electrical and Electronics Engineers Journal) predstavila revolucionarni koncept kriptografije z javnimi ključi. Le-ta za razliko od simetričnega sistema uporablja dva različna ključa,

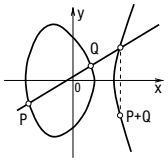



◄ Slika 7: Javno dostopen nabiralnik, ki pa ga lahko odpremo samo z zasebnim ključem.

## Kriptosistemi z eliptičnimi krivuljami (ECC)

Eliptična krivulja je množica točk, ki rešijo enačbo $y^2 = x^3 + ax + b$. Točke na krivulji lahko seštevamo po »sekantnem in tangentnem« pravilu, kot to prikazuje spodnja slika.

Eliptične krivulje se uporabljajo v asimetrični kriptografiji. Njihova varnost temelji na problemu diskretnega logaritma. Še posebej so privlačne zato, ker so dolžine ključev občutno krajše kakor pri sistemu RSA – 160-bitni ključ v kriptosistemih z eliptičnimi krivuljami zagotavlja enako varnost kakor 1024-bitni ključ v sistemu RSA. To omogoča večje hitrosti. Pomembna prednost je tudi, da za učinkovito izvajanje na pametnih karticah ne potrebujemo posebnih kripto-soprocesorjev, kakor jih na primer potrebuje RSA. Z ECC minimaliziramo programsko kodo, dolžine ključev in velikost podpisa, zato je za uporabne programe na voljo več prostora.



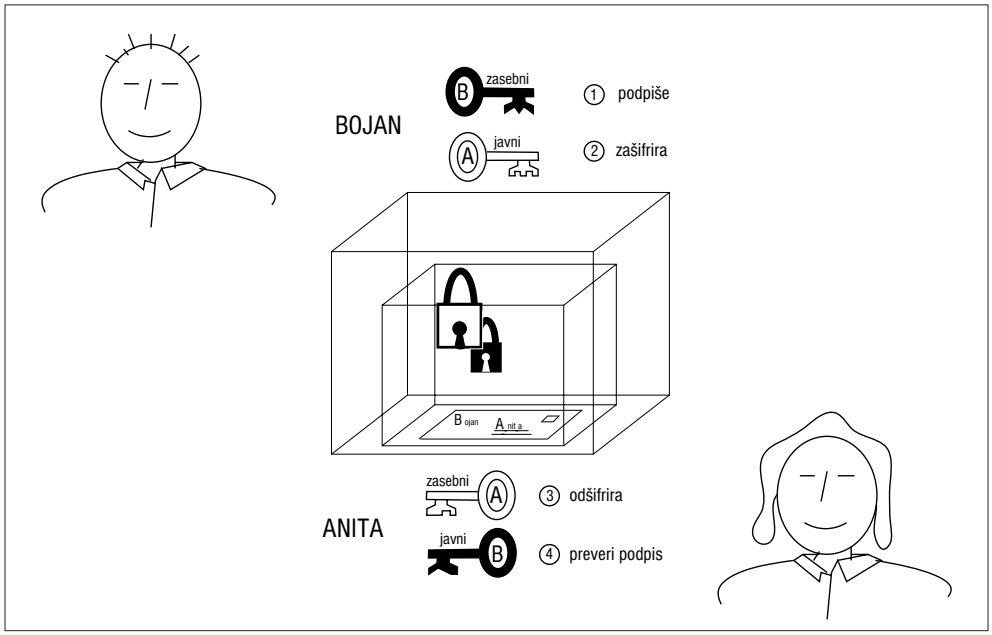

◄ Eliptična krivulja. Da seštejemo točki $P$ in $Q$, potegnemo skoznju premico in poiščemo tretje presečišče, ki ga nato še prezrcalimo prek osi $x$ (v primeru podvajanja točke $P$ pa začnemo s tangento v točki $P$).

ECC so iz dneva v dan bolje sprejeti kot izbrana metoda za varovanje podatkov v omejenih okoljih in so vključeni v številne standarde (IEEE P1363, ANSI X9, ISO in NIST). ECC so uspešno uporabila razna podjetja po svetu, kot so Siemens, Certicom Corp., Thompson in NeXT Computer. Tudi v Sloveniji spremljamo razvoj ECC. Že četrto leto namreč poteka seminar iz kriptografije na Inštitutu za matematiko, fiziko in mehaniko v Ljubljani, glej http://valjhun.fmf.uni-lj.si/~ajurisic/seminar.

zasebnega ter javnega, in tako ji pravimo tudi asimetrična kriptografija. Če se torej Anita in Bojan še nista nikoli dogovorila za tajni ključ, lahko uporabita kriptografijo z javnimi ključi. Tu ima za razliko od simetričnega sistema vsak uporabnik po dva različna ključa, en podatke zaklepa, drugi pa jih odklepa. Pomembna lastnost tega sistema je, da ključ, ki zaklene podatke, ne more leteh tudi odkleniti in nasprotno, tisti ključ, ki podatke odklene, ne more leteh tudi zakleniti. To omogoči lastniku, da objavi en ključ, drugega pa shrani v tajnosti (npr. na pametni kartici). Zato imenujemo ta ključa zaporedoma javni in zasebni, kriptosistemu pa pravimo tudi asimetrični kriptosistem.

Ta pristop omogoča veliko presenetljivih načinov uporabe, npr. omogoča ljudem varno komuniciranje, ne da bi se predhodno srečali zaradi izmenjave oziroma 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.

Nekaj podobnega so poštni nabiralniki. Vsakdo, ki ve, kje stoji nabi-




▲ Slika 8: Namesto operacij šifriranja in odšifriranja s ključi $Z_A$, $J_A$ in $Z_B$, $J_B$ si je morda lažje predstavljati konkretne modele. V ta namen vidimo zgoraj dve škatli s ključavnicama. V črni ključavnici lahko uporabljamo le črna ključa (Bojanov zasebni in javni ključ), v beli pa le bela (Anitin zasebni in javni ključ).

ralnik, lahko vanj vrže pošiljko, ne more pa je vzeti ven. To lahko stori le lastnik nabiralnika, ki ima ključ.

Če torej Anita objavi svoj javni ključ in z njim Bojan zašifrira pismo, namenjeno Aniti, bo le Anita lahko odšifrirala to pismo. Tako smo dosegli zasebnost. Če pa Bojan najprej zašifrira pismo z zasebnim ključem, bo vsak, ki dobi ta tajnopis, znal brati (odšifrirati) Bojanovo pismo, nihče pa ne bo znal impersonirati Bojana, t.j. njegovega »podpisa«. Torej smo dosegli pristnost Bojanovega pisma. Če torej želi Bojan poslati Aniti podpisano zasebno pismo, ga najprej zašifrira s svojim zasebnim ključem $Z_B$, nato si priskrbi Anitin javni ključ $J_A$, da z njim zašifrira že podpisano pismo in le-to pošlje Aniti, glej sliko 8. Anita prejeto pošiljko najprej odšifrira s svojim zasebnim ključem $Z_A$. Nato si priskrbi Bojanov javni ključ $J_B$ ter z njim preveri podpis, t.j. z Bojanovim javnim ključem odšifrira zašifrirano pismo.

***Pametne kartice omogočajo stopnjo varnosti, ki je potrebna, da računalniška omrežja zares zaživijo, ter združijo telekomunikacije in računalnike.***

Diffie in Hellman sta v zgoraj omenjenem članku zapisala, da smo na robu revolucije v kriptografiji in zaželela, da se jima pridružijo še drugi pri delu na tem fascinantnem področju, ki je bilo tiste čase pod popolnim monopolom in nadzorom vlade. Izvajala ju je ameriška vladna organizacija National Security Agency – NSA, ki skrbi za komunikacijsko varnost in odgovarja ministrstvu za obrambo (angl. *Department of Defence – DoD*). Še vedno nadzoruje tuje komuniciranje in razbija šifre, razvija nove kriptografske algoritme in omejuje uporabo znanih algoritmov. Čas je pokazal, da sta imela Diffie in Hellman prav. Njuno delo je povzročilo pravo eksplozijo neodvisnega raziskovanja v kriptografiji, s tem pa so tako civilni sektor kakor preprosti ljudje dobili možnost, da si zagotovijo pravico do zasebnosti.

V razvoju javne kriptografije je bilo predlaganih in razbitih veliko kriptosistemov. Le nekaj se jih je obdržalo, ki jih lahko danes štejemo za varne in učinkovite. Glede na matematični problem, na katerem temeljijo, so razdeljeni v tri skupine:

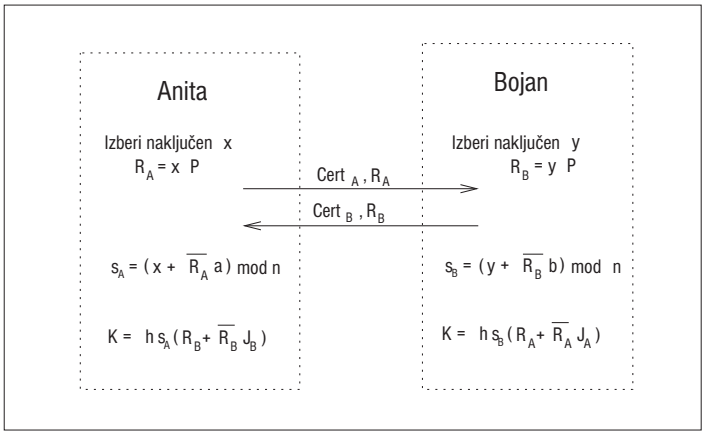
- **kriptosistemi faktorizacije celih števil**, npr. RSA,
- **kriptosistemi diskretnega logaritma**, npr. digitalni podpis, ki ga je prispevala vlada ZDA (angl. *Digital Signature Algorithm – DSA*),
- **kriptosistemi z eliptičnimi krivuljami** (angl. *Elliptic Curve Cryptosystems – ECC*), npr. ECDSA.

Zadnji dve skupini sta varianti ElGamalovih kriptosistemov, a njuna varnost temelji na popolnoma različnih problemih diskretnega logaritma.

Žal so postopki za zagotavljanje zasebnosti z javnimi ključi tudi do 1000-krat počasnejši od simetričnih, tako da jih uporabljamo samo za izmenjavo simetričnega ključa ali pa šifriranje zelo kratkih sporočil. Po drugi strani pa znamo digitalni podpis (angl. *digital signature*), ki se uporablja za ugotavljanje pristnosti, celovitosti in za preprečevanje zanikanja v elektronskem poslovanju, izpeljati le s kriptosistemi z javnimi ključi (glej Monitor, okt. 2000, str. 100). Pravna veljava digitalnega podpisa je ponavadi določena z zakonom. Digitalnim podpisom včasih pravimo tudi elektronski podpisi, vsekakor pa pri tem ne mislimo na digitalni ali elektronski zapis običajnega podpisa. Digitalni podpis je lahko dodan čitljivemu besedilu na tak način, da prestane preizkus le, če vsebina podpisanega sporočila ostane nespremenjena. V ta namen uporabimo na sporočilu zgoščevalno funkcijo (angl. *hash function*). To je postopek za stiskanje podatkov z enosmerno funkcijo, tako da iz rezultata ni moč izračunati prvotnih podatkov. Rezultat ima fiksno dolžino ne glede na količino vhodnih podatkov. Vsako spreminjanje podatkov zelo verjetno spremeni tudi rezultat zgoščevalne funkcije. SHA-1 je njen tipičen predstavnik.

## PKI in certifikati

O infrastrukturi javnih ključev (PKI) je bilo v Monitorju že kar nekaj napisanega (glej npr. Sistem, april 2001). Tukaj bomo zato samo poka-




▲ Slika 9: Zgled protokola MQV, ki ga uporabljamo v asimetričnih kriptosistemih. Omogoča hkratno izmenjavo sejnega ključa in overitev obeh strani, udeleženih v pogovoru. Izveden je na eliptičnih krivuljah, javna ključa sta JA = a P in JB = b P, kjer sta a in b zasebna ključa. P je javna točka na krivulji, h je število, odvisno od krivulje, n pa označuje število točk na krivulji. Vidimo, da je ključ K na obeh straneh enak h sA sB.

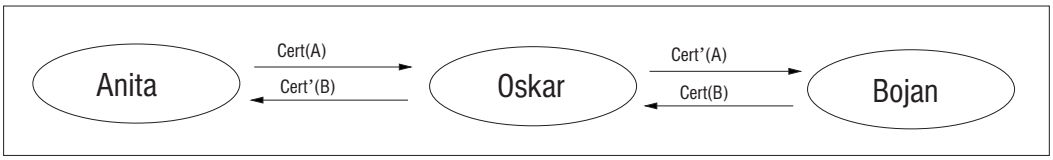
## Amaterskim sestavljalcem šifer

Iznašli ste novo šifro. V tem ste novi, nihče še ni slišal za vas. Želite, da priznani kriptografi pogledajo vaše delo. Kaj lahko naredite? Na žalost je pred vami težka pot. Neprestano se pojavljajo nove šifre, ki so jih sestavili amaterski kriptografi. Verjetnost, da je katera od šifer *varna*, je **zelo majhna**. Verjetnost, da je katera od njih dejansko *vredna*, pa je praktično **enaka nič**. Vsakdo, od najbolj nepodkovanega amaterja do najboljšega kriptografa, lahko sestavi algoritem, ki ga sam ne zna razbiti. Kaj takega niti ni težko. Težko pa je sestaviti algoritem, ki ga ne more razbiti nihče, celo po nekaj letih analize. Edini način, da se prepričamo o varnosti algoritma, je, da ga temeljito preverijo tudi drugi kriptoanalitiki.

Med kriptologi kroži zgodba o kriptoanalitiku in amaterju, ki ga je nenehno nadlegoval s šifro, ki jo je izumil. Kriptoanalitik mu razbije šifro, amater jo »popravi«, kriptoanalitik pa jo spet razbije. Ta izmenjava se je nekajkrat ponovila, dokler kriptoanalitik ni imel dovolj. Ko ga je amater spet obiskal, da bi izvedel, česa se je kriptoanalitik domislil, je slednji položil na mizo tri ovojnice in rekel: »V vsaki od teh ovojnic je en napad na vašo šifro. Izberite si eno in preberite moj napad. Ne vračajte se, vse dokler ne najdete še drugih dveh napadov.« Amater se ni prikazal nikoli več.

Ne želimo biti popolnoma črnogledi. Sem ter tja ljudem uspe sestaviti močno šifro. Celo amaterski kriptografi jo lahko sestavijo. Toda prvi korak do sestavljanja šifer je razbijanje obstoječih. Šele ko jih nekaj razbijete, se lahko lotite pisanja novih. Pri tem poskrbite, da bo šifra odporna proti vsem znanim napadom, hkrati pa bo učinkovita tako na močnih računalnikih kakor na majhnih napravah, npr. pametnih karticah.

zali, zakaj potrebujemo PKI in kakšne prednosti ima pred sistemi, ki temeljijo na simetričnih kriptosistemih. Spomnimo se, da je PKI sestavljen iz agencije za certifikate (CA), ki izdaja certifikate in vodi seznam preklicanih certifikatov. Zgled protokola, ki ga uporabljamo za komunikacijo, je prikazan na sliki 9.




▲ Slika 10: Problem srednjega napadalca: Oskar ponaredi Anitin in Bojanov certifikat. Anita je prepričana, da se pogovarja z Bojanom, Bojan pa, da govori z Anito. Na enak problem smo naleteli tudi v vohunovi dilemi.

Da laže razumemo, zakaj potrebujemo CA, si oglejmo naslednji napad, prikazan na sliki 10.

Denimo, da se želita Anita in Bojan pogovarjati. Anita pošlje Bojanu svoj certifikat, ki pa ga prestreže Oskar. Ta nato zamenja Anitin javni ključ v njenem certifikatu s svojim in ga pošlje Bojanu. Bojan nato pošlje svoj certifikat Aniti, ki ga spet prestreže Oskar. V tem certifikatu pa Oskar zamenja Bojanov javni ključ s svojim. Tako spremenjen certifikat pošlje Aniti. Ko začneta Anita in Bojan komunicirati, Oskar vsako sporočilo prestreže, ga odšifrira in nato zašifrira z ustreznima ključema. Če Anita in Bojan ne moreta preveriti veljavnosti certifikatov, lahko Oskar vedno prisluškuje njunemu pogovoru. Torej je nujno, da certifikate izdajajo samo pooblaščene CA, ki vsak certifikat digitalno podpišejo in s podpisom jamčijo, da je certifikat pristen.

***Digitalni podpis ni digitalni ali elektronski zapis običajnega podpisa.***

Kakšne so torej prednosti asimetričnih sistemov pred simetričnimi? Videli smo, da moramo pri simetričnem sistemu za vsako komunikacijo najprej vzpostaviti povezavo s centrom, ki nam izda sejni ključ. Tako so torej onemogočene nepriključne (off-line) transakcije. Zaradi visokih cen telekomunikacij, predvsem v Evropi, obstaja močna želja ravno po takšnih transakcijah. Pogosta so tudi plačila manjših zneskov, kjer se strošek transakcije ne razlikuje bistveno od vrednosti transakcije. Seveda moramo tudi pri asimetričnem sistemu vzpostaviti povezavo s centrom, če želimo preveriti, ali je bil certifikat preklican. Vendar pa tega ni treba narediti pri vsaki komunikaciji. Pogosto to opravimo npr. ob koncu dneva, hkrati pa še prenesemo podatke o transakcijah celotnega dne v centralno zbirko. Na ta način močno zmanjšamo stroške komuniciranja in obremenjenost omrežja. S certifikati lahko tudi uspešno rešimo vohunovo dilemo, opisano v prvem delu.

V drugem delu smo spoznali nekaj kriptografskih protokolov, ki jih uporabljamo za varno komunikacijo in e-poslovanje. V tretjem delu pa si bomo ogledali pasti, na katere naletimo, če jih poizkusimo uporabiti na pametnih karticah, in kako se tem pastem izognemo.

*Aleksandar Jurišić*
*Jernej Tonejc*