Kratek pojmovnik skrivnoslovja*

Vladimir Batagelj
Univerza v Ljubljani
FNT, oddelek za matematiko in mehaniko

Kdor ima pravočasno in točno informacijo se lahko bolje odloča. Za nekatere stvari ne bi radi, da bi drugi zanje vedeli. Zagotavljanje tajnosti sporočil in zaupnih spisov je bilo še nedavno vprašanje, s katerim so se ubadali predvsem diplomati, vojaki in vohuni. S prodorom računalnikov na področje hranjenja, izmenjave in obdelave podatkov pa se (bodo) ta vprašanja vsebolj dotikajo(la) vsakogar izmed nas, naše zasebnosti in varnosti (osebni podatki, statistike, poslovno-tehnični podatki, intelektualna lastnina, računalniška pošta, naročanje in plačevanje, ...).

Skrivnoslovje ali **kriptologija** (*kryptos* gr. skrit) je veda, ki se ukvarja (**skrivnopisje, kriptografija**) s postopki prikrivanja ali inkripcije[1] vsebine sporočil in (**kriptanaliza**) z nasprotnimi postopki **razkrivanja** ali **dekripcije**. Pri tem se naslanja na druge vede, predvsem matematiko in jezikoslovje, ob izdatni podpori računalniške tehnologije. **NSA** (No Such Agency/National Security Agency) je največji naročnik zmogljive računalniške opreme in zaposlovalec matematikov. Pomembno vlogo pri razkrivanju skrivnih sporočil pa imata tudi sreča in navdih.

nazaj do odprtega sporočila s, poznati poleg **razkrivnega postopka** R še ključ K_2.

Včasih se lahko do prikritih sporočil dokoplje **prestrezalec**, ki bi rad zvedel njihovo vsebino. Zato poskuša **razbiti** skrivnopisni sestav. **Napad** na skrivnopisni sestav imenujemo metodo, ki, opirajoč se na poznavanje prikritih sporočil in morda delčkov pripadajočih odprtih sporočil, poskuša odkriti kaj več o odprtem sporočilu.

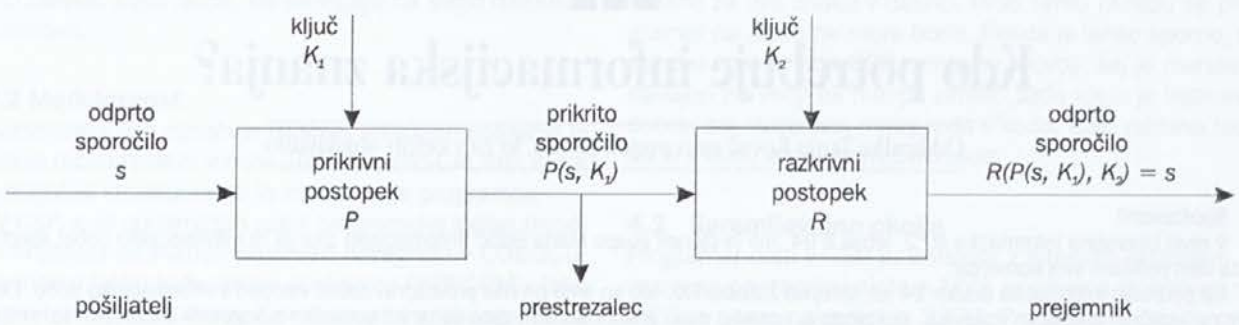
Pri načrtovanju skrivnopisnih sestavov predpostavimo **najneugodnejše razmere**: prestrezalec pozna v podrobnosti zgradbo sestava, je zbral večjo količino prikritih sporočil in pozna (uspe uganiti) posamezne delce pripadajočih odprtih sporočil (npr. vsa začenjajo z *Dragi Janez*,). Pri ocenjevanju sestavov pa se opremo na **Shannonove kriterije**: stopnja tajnosti, velikost ključa, učinkovitost postopkov prikrivanja in razkrivanja, razširjanje napak, podaljšanje zapisa sporočila.

Sporočila imajo lahko različne **oblike**: niz znakov, slika, zvok, ... V nadaljnjem se bomo omejili na sporočila zapisana z nizi znakov.

Eden najzgodnejših prikrivnih postopkov je **Cezarjev**, pri katerem zamenjamo vsako črko v sporočilu s (krožno) tretjo naslednjo črko v abecedi. Tako:

INFORMATIKA → LRISTPČZLNČ

Znane so tudi skrivnopisne zabeležke Leonarda da Vincija; skrivni dnevnik Samuela Pepysa (1660-69); plesoči možički, s katerimi se je ubadal Sherloch Holmes, ...nemški prikrivni stroj **Enigma** iz druge svetovne vojne. Velike dosežke, čeprav ne gre za prava prikrita sporočila, predstavljajo tudi razkritja pisav starih kul-



Slika 1: *Skrivnopisni sestav*

Uporaba skrivnopisnih postopkov je le ena od oblik varovanja zaupnih podatkov. Ukvarja se z varovanjem pri prenosu in hranjenju. **Stopnjo** varovanja določamo glede na pomembnost podatkov in glede na obdobje, v katerem naj bi ostali tajni. Podjetje Accessdata prodaja programski paket, ki je kos skrivnopisnim postopkom, ki jih ponujajo programi WordPerfect, Lotus 1-2-3, Quatro-Pro, Excel, Paradox, ...

Na sliki je prikazana osnovna zgradba **skrivnopisnega sestava**. **Pošiljatelj** pošlje **svoje (odprto)** sporočilo s skozi **prikrivni postopek** P, ki ga glede na pošiljateljev **ključ** K_1 predela v **prikrito sporočilo** ali **skrivnopis** $P(s,K_1)$. **Prejemnik** mora, zato da pride tur (npr. Champollion 1822, egipčanski hieroglifi).

Sestav prenosa prikritih sporočil mora zagotavljati **zasebnost in pristnost** – pošiljatelja mora ščititi pred **prisluškovanjem** in pred **spreminjanjem** sporočil (virusi, potvarjanje).

Navadni skrivnopisni sestavi temeljijo na enem ključu, $K_1 = K_2$, ki ga poznata le pošiljatelj in prejemnik. Pravimo tudi, da je tak sestav **simetričen**, ker je potrebno poznati isti ključ pri prikrivanju in razkrivanju sporočila.

Tak sestav je bil v ZDA določen s **FIPS** 46 (Federal Information Processing Standard) leta 1977. Sestav so, po izkušnjah z **LUZIFER**jem, razvili pri IBMu in je poznan pod kratico **DES** (Data

Encryption Standard). Spremlja ga **DEA** (Data Encryption Algorithm). Leta 1988 je bila objavljena njuna posodobitev FIPS 46.1.

Navadni sestavi so nerodni za širšo uporabo. Veliko primernejši so **sestavi javnih ključev**, ki sta si jih leta 1976 izmislila Diffie in Hellman. V teh sestavih ima vsak uporabnik po en **javni** in en **tajni** ključ. Javni ključi so objavljeni v imeniku. Z javnim ključem prikrijemo sporočilo, s tajnim pa ga razkrijemo, kar zagotavlja, da le naslovnik (lastnik tajnega ključa) lahko prebere prikrito sporočilo. Pogosto se, zaradi hitrosti prenosa, sestav javnih ključev uporablja le za prenos ključa za navadni sestav, v katerem se opravi prenos pravega sporočila.

Kadar se sestav javnih ključev uporablja za **overovljanje**, se pošiljateljev tajni ključ uporabi za **podpisovanje** in njegov javni ključ za preverjanje pristnosti podpisa -- nihče, razen pošiljatelja, ne more podpisati sporočila.

Takemu sestavu pravimo, da je **asimetričen**, ker brez poznavanja tajnega ključa lahko opravimo le ali prikrivanje ali razkrivanje, ne pa obojega.

Javni sestav naj bi omogočil tudi zanesljivo omrežno poslovanje (naročanje, plačevanje, računalniške spise, ...). Pri tovrstnih uporabah je potrebno sporočila opremiti tudi s **časovnim žigom**, za kar naj bi skrbeli posebni **strežniki-notarji**. Poseben problem v javnem sestavu predstavljata **upravljanje** in **izmenjava** ključev.

Za izvedbo Diffie in Hellmanove zamisli potrebujemo **zaklopne enosmerne** preslikave. Za dani argument je vrednost take preslikave lahko izračunati, njen obrat pa zelo težko, razen če ne poznamo posebne **zaklopne** informacije. Predlaganih je bilo več tovrstnih preslikav. Med njimi je najbolj znan sestav **RSA**, ki je dobil ime po začetnicah njegovih tvorcev Rivest, Shamir in Adleman, 1978. Temelji na domnevi, da je za dano število, ki je produkt dveh praštevil, zelo težko ugotoviti, kateri števili sta to; brez težav pa iz znanega produkta in enega od členov izračunamo drugega.

Na mednarodnih računalniških omrežjih je mogoče dobiti program (tudi v izvorni obliki) **PGP** (Pretty Good Privacy), ki podpira tak javni sestav.

NIST (National Institute of Standards and Technology) je konec avgusta leta 1991 dal v razpravo predlog svojega sestava javnih ključev **DSS** (Digital Signature Standard) in spremljajoči **DSA** (Digital Signature Algorithm), ki je naletel na precej nasprotovanja v strokovni javnosti. Zato so ga vrnili v nadaljnjo razdelavo.

V ZDA narašča nasprotje med tajnimi službami in računalniško industrijo. Sodobne skrivnopisne sestave je prepovedano prodajati na Vzhod in državam tretjega sveta; težko pa je preprečiti odliv znanja. Zato se že dogaja, da ameriška podjetja zgubljajo posle. Leta 1991 so le s težavo preprečili sprejetje predpisa, za katerim je stal FBI, ki proizvajalcem telekomunikacijske opreme nalaga, da vgrajujejo le take zaščite, ki jih vladne službe obvladujejo – podobno, kot če bi od gradbenikov zahtevali naj v vrata vgrajujejo ključavnice, ki jih odpira univerzalni ključ.

Viri

[1] Beker H., Piper F.: Cipher Systems, The Protection of Communications. Northwood Books, London 1982.

[2] Kahn D.: The Codebreakers, The Story of Secret Writing. Macmillan, New York 1967. (prevod: Šifranti protiv špijuna, 1-4. knjiga. CIP, Zagreb 1979).

[3] Sinkov A.: Elementary Cryptanalysis, A Mathematical Approach. The Mathematical Association of America, Washington 1966.

[4] Encryption Standards: Who Holds the Keys? Communications of the ACM 35(1992)7.

[5] Common Cryptographic Architecture. IBM Systems Journal 30(1991)2.

[6] The Crypt Cabal: Cryptography FAQ (Frequently Asked Questions). version 4 May 1993.

---

* *Sestavek je bil napisan za Mladino, kjer je v predelani in močno skrajšani obliki izšel 2. novembra 1993, str. 33.*

1) *iz francoščine ali nemščine je prišla še beseda šifra, šifriranje (chiffre, fr. številka), vendar jo bomo raje prepustili statistikom -- npr. šifrant poklicev.*

Slovarček skrivnoslovja

Vladimir Batagelj, Borut B. Lavrenčič

algorithm	algoritem, postopek
attack	napad
Alice, Bob, Charlie, David	imena-vloge z začetnicami A, B, C in D
Ann, Bill, Charles, Eve	imena-vloge, IBM
Ann	pošiljatelj
Bill	prejemnik
Charles	naključni prestrezalec
Eve	namenski prestrezalec
asymmetric encryption	asimetrično prikrivanje
authentic	pristen
authentication	preverjanje pristnosti, overovljanje
block cipher	prikrivanje po delih/kosih/blokih, bločno prikrivanje
certificate	izkaz/spričevalo/potrdilo/certifikat
cipher	skrivna/tajna pisava
* system	skrivnopisni sestav, kriptografski sestav
* text → cryptogram	
code	koda
confidential	zaupen
cryptX	skriti/tajni X
*analysis	razkrivanje, kriptanaliza
*ology	skrivnoslovje, kriptologija
*ography	skrivnopisje/prikrivanje, kriptografija
*ogram	skrivno/prikrito sporočilo/besedilo, skrivnopis
*osystem	skrivnopisni sestav, kripto-sistem
deciphering → decryption	
decryption	razkrivanje, dekripcija; dekriptati
EDI	RIP -- računalniška izmenjava podatkov
electronic mail, e-mail	računalniška/elektronska pošta
enciphering → encryption	
encryption	prikrivanje, inkripcija; inkriptati
falsification	potvarjanje
file	datoteka
armor *	oklepljena datoteka
compressed *	stisnjena datoteka
* encryption	prikrivanje/inkripcija datoteke
deleted *	izločena datoteka

wiped *	pobrisana datoteka
hash	zgoščanje
id	oznaka/ime, identifikator
integrity	celovitost
interceptor	prestrezalec
key	ključ
* certificate	izkaz/spričevalo/potrdilo/certifikat ključa
* exchange	izmenjava ključev
* file	datoteka ključev
* fingerprint	odtis ključa
* generation	ustvarjanje/tvorba ključev
hexadecimal *	šestnajstiški ključ
* management	upravljanje s ključi
public *	javni ključ
* ring	obroč ključev
secret *	tajni ključ
* space	prostor ključev
symmetric *	simetrični ključ
message	sporočilo
* digest → hash	
nonrepudiation	nezatajljivost
one way	enosmeren
password	geslo
pass phrase	geslo, tajni izraz, dolgo geslo
public	javni
plain text → message	odprto sporočilo/besedilo
printable ASCII	natisljivi/izpisljivi znaki
privacy	zasebnost
protocol	dogovor/protokol
recipient	prejemnik
security	varnost
secure erasure	varno brisanje
secrecy system	skrivnopisni sestav
server	strežnik
signature	podpis
digital *	računalniški podpis
electronic *	računalniški podpis
sniffer	vohljač
spoofing	pretvarjanje
stream cipher	tokovno/sprotno prikrivanje
symmetric encryption	simetrično prikrivanje
text	besedilo
time stamp	časovni žig
* server	časovni strežnik, notar
transmission	prenos
trapdoor	zaklopka, zaklopna; loputa
user id	oznaka uporabnika

Nekaj pogostih kratic

ECC	Eliptic Curve Cryptography
CCA	Common Cryptographic Architecture
CRC	Cyclic Redundancy Check
DH	Diffie, Hellman
DES	Data Encryption Standard
DEA	Data Encryption Algorithm
DSS	Digital Signature Standard
DSA	Digital Signature Algorithm
MAC	Message Authentication Code
MIC	Message Integrity Check
NSA	National Security Agency
PIN	Personal Identification Number
RSA	Rivest, Shamir, Adelman

Navodila avtorjem

Prispevke pošiljajte v predpisani obliki na naslov Slovensko društvo Informatika, 61000 Ljubljana, Vožarski pot 12, s pripisom za revijo Uporabna informatika.

Če je možno, naj bo članek lektoriran. V uredništvu bomo opravili korekturo in se po presoji posvetovali z avtorjem, da članek tudi lektoriramo.

Prispevek naj bo v obsegu največ avtorska pola (30.000 znakov) za strokovne članke in približno 2 do 3 tiskane strani za druge prispevke. Vsak strokovni članek naj ima na začetku povzetek v slovenskem in v angleškem jeziku.

Pošljite ga na disketi in odtisnjenega na papirju. Napisan je lahko v kateremkoli urejevalniku besedil, vendar naj bo na disketi tudi kopija v ASCII formatu. Na disketi označite, kateri urejevalnik ste uporabili, in ime datoteke. Datoteko imenujte s svojim priimkom, n. pr. Novak. doc ali Novak.txt.

Slike, ki ste jih izdelali z grafičnim programom, označite podobno. Na natisnjenem izvodu članka naj bo jasno vidno, kam sodi posamezna slika. Lahko priložite tudi originalne predloge, ki jih na hrbtni strani označite s številkami, tako kot v natisnjenem besedilu.

Pišite v razmaku vrstic 1, brez posebnih ali poudarjenih črk ali podčrtovanja, za ločilom na koncu stavka napravite samo en prazen prostor, ne uporabljajte zamika pri odstavkih.

Za vsa vprašanja se obračajte na tehnično urednico Katarino Puc, 61000 Ljubljana, Ulica Gubčeve brigade, tel. 1271-579, elektronska pošta Katarina.Puc@uni-lj.si