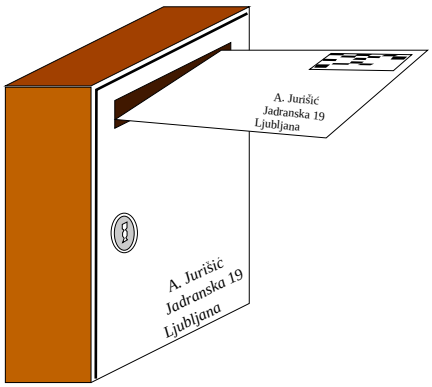
POŠTNI NABIRALNIK IN KRIPTOGRAFSKI PROTOKOLI

Kriptosistemi z javnimi ključi, 3. del

Nadaljujemo zgodbo o dveh vizionarjih Whitfieldu Diffieju in Martinu Hellmanu, ki sta razmišljala o bližajoči se digitalni dobi in odkrila (DH-)dogovor o tajnem ključu (prav neverjetno, a ta ostane tak celo ob nenehni navzočnosti ostrih ušes vohunov).[1] Na srečo se nista ustavila pri tem. Prav nasprotno! Prepričana sta bila, da sta na pravi poti in to jima je dalo svež zagon, ki je bil še kako dobrodošel pri novih odkritjih. Leta 1976 so Whitfield Diffie, Martin Hellman in Ralph Merkle vpeljali revolucionaren koncept **kriptosistemov z javnimi ključi**, ki ga bomo predstavili v tem sestavku. Ideja je v resnici zelo enostavna, dostopna celo osnovnošolcem, če le nanjo pogledamo iz pravega zornega kota.

> *Vsakdo, ki ve, kje je nabiralnik, lahko vanj vrže pošiljko,*
> *ne more pa je vzeti ven – to lahko stori le tisti, ki ima ključ od nabiralnika.*

Nabiralnikov seveda ne skrivamo. Prav nasprotno, običajno so označeni z imenom lastnika in se nahajajo poleg vhoda v blok ali hišo. Večino naslovov prebivalcev lahko najdemo kar v telefonskem imeniku. Zato pravimo, da je taka informacija *javna*.



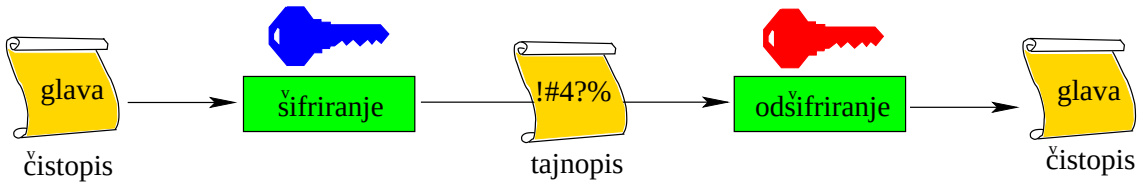
Slika 1: Javno dostopni nabiralnik, ki ga lahko nenasilno odpremo samo z zasebnim ključem.

V nasprotju z zasebnimi oziroma *simetričnimi* kriptosistemi, v katerih se uporablja en sam ključ za šifriranje čistopisa in odšifriranje tajnopisa, ima pri kriptosistemih z javnimi ključi vsak uporabnik (to je lahko tudi naprava, npr. tiskalnik) svoj par ključev:

- *zasebnega*, tj. v našem primeru ključ od nabiralnika, in
- *javnega*, tj. informacijo o tem, kam je postavljen ustrezni nabiralnik oziroma kako je označen (če moramo izbrati med številnimi, na videz enakimi, nabiralniki).

Zato takim sistemom rečemo tudi *asimetrični* kriptosistemi.

[1] DH-dogovor smo predstavili v drugem delu [2], medtem ko smo v prvem delu [1] spoznali simetrične šifre oziroma kriptosisteme, pri katerih prihaja do težav bodisi zaradi velikega števila ključev, ki bi jih moral hraniti vsak posameznik, bodisi zaradi načina njihovega dodeljevanja.



Slika 2: Asimetrični kriptosistem uporablja javni ključ za šifriranje in zasebni za odšifriranje. Uporabnik najprej objavi svoj javni ključ, zasebnega pa spravi na varno. Nato lahko vsakdo z javnim ključem zašifrira pismo, bral oziroma odšifriral pa ga bo lahko le lastnik ustreznega zasebnega ključa.

Če se torej Anita in Bojan želita varno pogovarjati, objavita svoja javna ključa, zasebna pa zadržita zase. Ko želi Anita poslati zaupno sporočilo Bojanu, ga z njegovim javnim ključem zašifrira (tj. vrže pismo v Bojanov nabiralnik), Bojan pa je edini, ki pozna odšifrirni (zasebni) ključ in lahko dobljeno sporočilo odšifrira ter prebere. En ključ podatke zaklepa, drugi pa jih odklepa.

Pomembna lastnost tega sistema je, da ključ, ki zaklepa, ne more odklepati in obratno, ključ, ki odklepa, ne more zaklepati.

Bolj natančno pa bomo rekli, da se iz javnega ključa ne da učinkovito (to pomeni v doglednem času, za katerega želimo zadržati napadalca) izračunati zasebnega ključa. Tako lastnik en ključ objavi, drugega pa hrani na varnem (npr. na pametni kartici, ki jo nosimo že v vsakem mobilnem telefonu). To omogoča ljudem varno komuniciranje, ne da bi se predhodno srečali zaradi izmenjave oziroma dogovora o tajnem ključu.

IDEJA KRIPTOSISTEMA Z JAVNIMI KJUČI

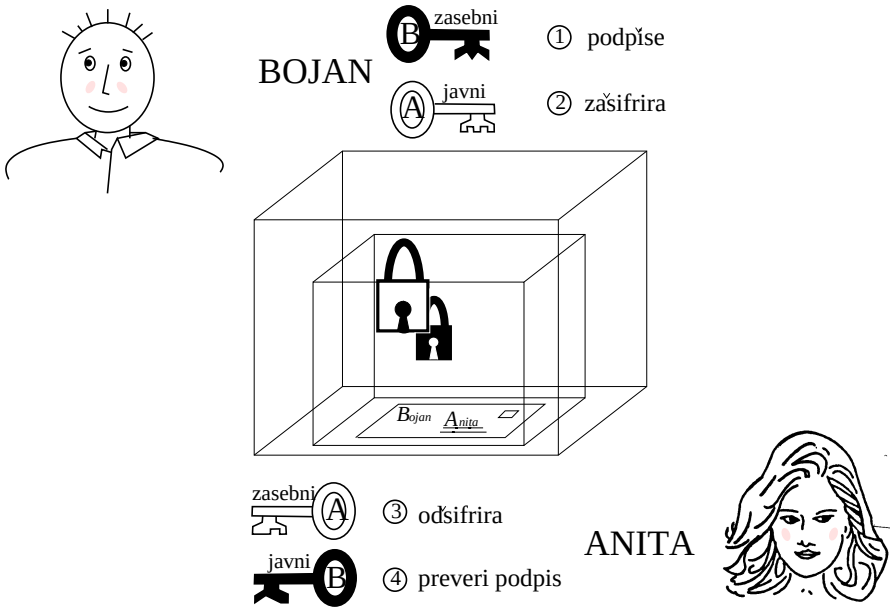
Kriptosistem z javnimi ključi bomo opisali v treh enostavnih korakih:

(a) Ko Anita objavi svoj javni ključ in Bojan z njim zašifrira pismo, namenjeno Aniti, lahko le ona odšifrira to pismo. Tako dosežemo *zasebnost*.

(b) Vlogo ključev lahko tudi zamenjamo in dobimo **digitalni podpis**: če Bojan najprej zašifrira pismo z zasebnim ključem (tj. ga *digitalno podpiše*), lahko vsakdo, ki dobi tajnopis, prebere (odšifrira) zašifrirano pismo, nihče pa ne more ponarediti podpisa, saj ima le Bojan zasebni (šifrirni) ključ. S tem dosežemo *pristnost* Bojanovega pisma.

Sedaj pa združimo zasebnost in pristnost.

(c) Če želi Bojan poslati Aniti podpisano zasebno pismo (glej sliko 3), ga najprej zašifrira s svojim zasebnim ključem Z_B (ga podpiše), nato si priskrbi Anitin (šifrirni) javni ključ J_A, z njim zašifrira že podpisano pismo in ji le-to pošlje. Anita prejeto pošiljko najprej odšifrira s svojim zasebnim ključem Z_A. Nato si priskrbi Bojanov javni ključ J_B ter z njim preveri podpis, tj. z Bojanovim javnim ključem odšifrira zašifrirano pismo ter se prepriča, da ji ga je res poslal Bojan.



Slika 3: V točki (c) smo združili zasebnost in pristnost. Namesto operacij šifriranja in odšifriranja si je morda lažje predstavljati konkretne modele. V ta namen vidimo zgoraj dve škatli s ključavnicama. Za črno ključavnico lahko uporabljamo le črna ključa (Bojanov zasebni in javni ključ), za belo pa le bela (Anitin zasebni in javni ključ).

Ideja je sedaj na mizi, nas pa zanima njena konkretna digitalna izvedba, saj ne želimo biti odvisni od (ne)varnih škatel, kaj šele od fizičnih ključavnic in ključavničarjev.

Kakšno zagotovilo dobimo, da je daljinski ključ za odpiranje garažnih vrat ali parkirišča zares varen? V resnici prav nobenega! Prodajalec nam morda še zna na začetku zamomljati, da gre pri ključavnici za milijone kombinacij. Ko pa mu osnovnošolec odvrne, da to ni prav dosti za današnje računalnike (na običajnem PC-ju lahko preverimo 30 milijonov gesel na sekundo), je zagotovil hitro konec. No, morda nas usmerijo le še na tujega dobavitelja, od katerega pa seveda nikoli ne dobimo jasnih odgovorov.

Se spomnite, da smo tudi v drugem delu [2] omenjali ključavnice (protokol Massey-Omura)? Povedali smo, da jih lahko v digitalnem svetu zamenjamo s parom obrnljivih funkcij, ki med seboj komutirata (tj. zanje velja pravilo o zamenjavi). V istem sestavku smo v deveti nalogi povprašali po takih funkcijah. Ni jih težko najti, saj nas že prištevanje skrivnih števil reši iz zagate. Če tajnemu ključu K Anita prišteje svoje skrivno število a in nato prišteje svoje skrivno število b še Bojan, jih lahko v istem vrstnem redu še odštejeta in tako pride Bojan do ključa K. Po javnem kanalu pa so zaporedoma potovali le števila $K + a$, $K + a + b$ in $K + b$, torej nikoli tajni ključ K. Seveda je v tem primeru dobro uporabiti modularno seštevanje (ni pa nujno). Še vedno dovolj učinkovito je tudi množenje s skrivnimi števili, za računalnike pa je še najbolj primerna operacija ekskluzivni ali (XOR). Vse te funkcije pa ne nudijo dejanske varnosti, saj lahko napadalec izračuna ključ iz znanih količin, npr. $K + b - [(K + a + b) - (K + a)] = K$. Ugotovili smo torej, da učinkovitost ni edini kriterij za take funkcije, saj moramo zagotoviti še, da obratna operacija nima te lastnosti.

Enosmerne funkcije so tiste, ki jih znamo zlahka izračunati (tj. z učinkovitim algoritmom), računanje v obratni smeri pa je težko (ne nujno vedno, v povprečju pa pravgotovo). Morda boste pomislili, da je že množenje s konstanto primer take funkcije, a za računalnike množenje ni kaj dosti bolj počasno (v primeru modularnega množenja to opravimo z razširenjim Evklidovim algoritmom, glej [3]). Tudi funkcijo $f(x) = x^2$ znamo hitro izračunati, vendar pa le-ta še ni prava kandidatka, saj se da relativno hitro izračunati tudi kvadratni koren.

Matematiki in računalnikarji si še vedno niso na jasnem, ali enosmerne funkcije sploh obstajajo. To je eden izmed slovitih odprtih problemov. Obstoj takšnih funkcij ima številne zanimive posledice (za starejše bralce omenimo npr. posledico $\mathbf{P} \neq \mathbf{NP}$).

Funkcije, ki so jih iskali na začetku omenjeni kriptografi, bi naj bile obrnljive le s pomočjo neke skrivnosti (angl. trap-door one-way functions). Npr. če razstavimo zapleteno napravo, jo je zelo težko sestaviti brez načrta, medtem ko z načrtom še nekako gre. Matematični primer pa bi bilo množenje dveh velikih praštevil, ki ga znamo hitro opraviti. Za dan produkt dveh praštevil je tudi preverjanje, ali sta dani praštevili tisti, ki nam dasta pravi produkt, zelo učinkovito. Za dan produkt brez poznavanja praštevil pa je izredno težko najti faktorje.

V razvoju kriptografije z javnimi ključi je bilo predlaganih in razbitih veliko kriptosistemov. Le nekaj jih je prestalo časovni test varnosti in jih lahko danes smatramo za razmeroma varne in učinkovite. Glede na matematični problem, na katerem temeljijo, so razdeljeni v tri skupine:

- *sistemi faktorizacije celih števil*, npr. RSA (Rivest-Shamir-Adleman), glej [4];
- *sistemi diskretnega logaritma*, npr. ElGamal in DSA;
- *kriptosistemi z eliptičnimi krivuljami* (Elliptic Curve Cryptosystems).

Prvi konkreten model kriptosistema z javnimi ključi so prelagali že leta 1977 Ronald Rivest, Adi Shamir in Leonard Adleman. Na drugega je bilo potrebno počakati skoraj celo desetletje (1985) in ga bomo predstavili v 4. delu, tretjega pa sta predlagala neodvisno Victor Miller (1986) in Neal Koblitz (1987).

PROTOKOLI V KRIPTOGRAFIJI

Protokol ni samo nekaj, kar morajo obvladati politiki, pač pa postopek, po katerem opravimo določen pogovor/komunikacijo. Za primer si oglejmo protokol, ki ga moramo poznati, če želimo obiskati učiteljico v njenem kabinetu.

> *Najprej se pozanimamo, kje je njen kabinet in kdaj ima govorilne ure. Nato odidemo tja ob pravem času. Ko želimo vstopiti, najprej potrkamo, počakamo na povabilo (Naprej!), nato odpremo vrata, pozdravimo in običajno še zapremo vrata. (Tudi če ne dobimo vabila, marsikoga zamika, da bi vseeno pritisnil na kljuko, pa čeprav to ni dovoljeno.)*

Tak protokol za vstop v pisarno bi v šoli na zavodu za gluhoneme otroke izgledal povsem drugače. Učenec ne bi mogel slišati povabila, morebitni gluhi učitelj ne bi slišal trkanja, nemi pa bi ga moral povabiti naprej na kakšen drug način. Privzeli smo tudi, da poteka protokol v varnem okolju. Če pa temu ni tako, mora biti protokol seveda precej drugačen, glej zgodbo o volku in sedmih kozličkih ali pa se spomni na mrke redarje, ki pogledajo čez majhno lino v vratih.

Opozoriti velja, da majhna sprememba v protokolu lahko kaj hitro pomeni veliko luknjo za varnost. Tudi računalniki in uporabniki na internetu se morajo držati pravil in s tem zagotoviti vse elemente varnosti, kot so zasebnost, celovitost (tj. zaščita pred spremembo vsebine), pristnost. Temu pravimo *kriptografski protokol*. Dokazati varnost nekega kriptografskega protokola je sila zahtevna naloga. Pogosto je mnogo lažje najti kakšen učinkovit napad (če seveda obstaja).

Za konec pa se vživimo še v en pravljični protokol, ki ga vsi dobro poznamo. Se še spomnite pravljice o lačnem volku in sedmih kozličkih?

Volk in sedem kozličkov (brata Grimm).

Nekoč je živela stara koza, ki je imela sedem kozličkov.
Nekega dne se je odpravila v gozd po krmo,
še prej pa je sklicala vseh sedem otrok in jim rekla:

"*Ljubi otroci, v gozd grem, vi pa se varujte volka!*
Če bi prišel noter, bi vas požrl s kožo in kostmi.
Grdavš se velikokrat pretvarja, da je kdo drug,
toda takoj ga boste prepoznali po
njegovem hripavem glasu in črnih tacah."

"*Ljuba mama, zelo bomo pazili nase, kar brez skrbi pojdi,*" so rekli kozlički.
Koza je zameketala in pomirjena odšla na pot.
Nedolgo zatem je potrkalo na vrata hišice in nekdo je zaklical:

"*Odprite, otročički, vaša mama trka in vsakemu je nekaj prinesla.*"

Toda kozlički so slišali hripavi glas in so takoj vedeli, da je volk. Zaklicali so:

"*Ne odpremo ti! Ti že nisi naša mama.*
Naša mama ima nežen in ljubezniv glas,
tvoj pa je hripav! Ti si volk!"

Volk je takoj odšel k trgovcu in si kupil velik kos krede.
Pojedel jo je in njegov glas je postal nežnejši.
Potem je šel nazaj, še enkrat potrkal na vrata hišice in zaklical:

"*Odprite, otročički, vaša mama trka in vsakemu je nekaj prinesla.*"

Toda kozlički so videli volkovo črno taco na oknu in so zaklicali:

"*Ne odpremo ti! Naša mama nima takih črnih tac kot ti. Ti si volk!*"

Zdaj je volk stekel k peku in mu rekel:

"*Udaril sem se v taco, pomaži mi jo s testom!!*"

Ko mu je pek pomazal taco s testom, je stekel še k mlinarju in mu rekel:

"*Posuj mi taco z belo moko!*"

Mlinar si je misli: "*Tale volk bo gotovo nekoga osleparil,*" in ni hotel narediti tega.

"*Požrl te bom!*"

je zarjul volk in mlinar se je ustrašil in mu ustregel. Takšni so pač ljudje.

Zdaj je šel hudobnež že tretjič do hišice, potrkal je in rekel:

"*Odprite otročički, vaša ljuba mamica je prišla domov in*
vsakemu nekaj prinesla iz gozda."

Kozlički so zaklicali:

"*Najprej nam pokaži taco, da bomo res vedeli, ali si naša ljuba mamica.*"

Volk je položil taco na okno, in ko so kozlički videli, da je bela, so mu verjeli ...

... se nadaljuje v 4. delu!

NALOGE

1. Konkreten model kriptosistema z javnimi ključi predstavlja dobro znani kriptosistem RSA. Preuči ga, nato ga implementiraj za kakšne male vrednosti in končno predlagaj prijatelju, da najde kakšno šibko točko. Če mu uspe, slabost odpravi in ga zopet pozovi k napadanju. To ponavljajta nekaj časa, potem pa vlogi zamenjajta. Običajno je taka igra zelo podobna tudi "tekmi" med kriptografi in kriptoanalisti.

2. Ponovi prejšno nalogo še za kakšen kriptosistem z javnimi ključi (npr. tistega, ki uporablja metodo nahrbtnika).

3. Opiši kakšno pomanjkljivost protokola Massey-Omura. Nato pa poišči kakšno lastnost funkcij, s katerimi izvedeš ta protokol, ki bo to pomanjkljivost odpravila.

4. Bilo je temno kot v rogu, ko se je vohun vračal v grad po opravljeni akciji v sovražnem taboru. Ko se je približal vratom, je zaslišal šepetajoč glas:

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

5. Predlagaj čimveč enosmernih funkcij. Zopet lahko organiziraš tekmo med kriptografi (sestavljalci šifer) in kriptoanalisti (razbijalci šifer).

6. Predlagaj kakšno enosmerno funkcijo, ki je obrnljiva s pomočjo neke skrivnosti (tu bi morala biti tekma med kriptografi in kriptoanalisti morda še bolj zanimiva).

Viri in dodatno branje

[1] A. Jurišić in Urban Perko, Klasične šifre in zdravstvena kartica, *Presek* **33**/1 (2005-06), str. 22–24
[2] A. Jurišić, Diffie-Hellmanov dogovor o ključu *Presek* **34** (2006-07), str. 25–30.
[3] M. Juvan, O Evklidovem algoritmu, *Presek*, **21** (1993-94), str. 116–121.
[4] M. Vencelj, Šifriranje z javnim ključem, *Presek* **22**/6 (1994-05), str. 354-357.

Aleksandar Jurišić