Prof. dr. A. Jurišić o testiranju praštevilskosti

# Ključna vloga v kriptografiji

*Dr. Mojca Pavšič*

*»Odkar sta leta 1976 W. Diffie in M. Hellman predstavila koncept javne kriptografije, je sledil pravi razcvet kriptografije, tega več tisočletij starega področja, ki je bilo prej skoraj izključno pod nadzorom tajnih služb. Tokrat smo priča izjemnemu dosežku, nekateri ga postavljajo ob bok učinkoviti rešitvi linearnega programa iz sedemdesetih let preteklega stoletja. Formalno sicer sodi na področje teorije algoritmične oziroma računske zahtevnosti, a verjamem, da bomo posledice začutili tudi v kriptografiji, posebno če bodo držale napovedi avtorjev, da je mogoče učinkovitost njihovega algoritma še izboljšati,« meni o odkritju treh indijskih znanstvenikov prof. dr. Aleksandar Jurišić iz Centra za kriptografijo in računalniško varnost na Politehniki v Novi Gorici.*

Foto Voranc Vogel

*Prof. dr. Aleksandar Jurišić*

***Profesorja Jurišić, ali ste tudi vi preverili pravilnost tega algoritma?***

Dan po tem, ko mi je kolega prof. dr. Bojan Mohar poslal novico o tem čudovitem dosežku indijskih matematikov in sem z interneta »snel« rešitev, sem odšel na Nizozemsko na konferenco iz geometrijske in algebraične kombinatorike. Prvi predavatelj, sloviti A. E. Brouwer, nas je presenetil in namesto svojega napovedanega predavanja predstavil zgoraj omenjeno rešitev. Gre za izjemno lepo uporabo končnih obsegov in teorije števil.

V času interneta so se razmere razširjanja informacij precej spremenile. V enem dnevu si je na domači strani avtorjev članek ogledalo več kot 30.000 ljudi. Zares sem vesel, da bom lahko končno v svoja predavanja vključil tudi deterministični dokaz preverjanja praštevilskosti.

Kot nekdanji udeleženec matematičnih tekmovanj bi rad omenil še to, da sta mlajša avtorja še leta 1997 med pripravami na olimpiado reševala olimpijske naloge (za katere jima je bilo rečeno, da jih ni rešil nihče na mednarodni matematični olimpiadi), zdaj pa sta uspešno sodelovala pri reševanju več sto let starega problema!

***Kakšen je pomen tega odkritja za kriptografijo?***

Metode za ugotavljanje, ali je neko število praštevilo, so pritegovale matematike od antičnih časov dalje. Razumeti praštevila je namreč ključnega pomena za reševanje številnih pomembnih matematičnih problemov. V zadnjem času pa se je pozornost usmerila na teste, ki jih lahko zaženemo na računalniku, saj takšne teste uporabljamo pri šifriranju digitalnih podatkov in pri digitalnih podpisih. Na primer testiranje praštevilskosti igra ključno vlogo v vseh razširjenih kriptosistemih z javnimi ključi, na primer RSA, DH, EC-DH. Varnost prvega je zasnovana na težavnosti iskanja deliteljev danega števila, varnost preostalih dveh pa na podlagi težavnosti diskretnega logaritma. Ti kriptosistemi se uporabljajo za varne transakcije in digitalno podpisovanje po internetu ali s pametnimi karticami.

Pogosto moramo izbrati praštevilo na določenem intervalu. Toda ko ga najdemo, kako lahko dokažemo, da je v resnici praštevilo? Eden največjih matematikov, Karl Friedrich Gauss (1777–1855), je v svoji knjigi *Disquistiones Arithmeticae* (1801) zapisal: »Menim, da čast znanosti narekuje, da z vsemi sredstvi iščemo rešitev tako elegantnega in tako razvpitega problema.« Od leta 1960 se je s prihodom računalnikov premaknil poudarek z iskanja matematične formule na iskanje učinkovitega algoritma (recept za iskanje po korakih).

***Ali tudi vi menite, tako kot matematik Ian Stewart, da bo ta metoda pomagala matematikom rešiti nekatere probleme, pri katerih so zaradi uporabe drugih tehnik zašli v slepo ulico?***

Čeprav mnogi znanstveniki menijo, da so matematični problemi, na katerih je zasnovana varnost pravkar omenjenih kriptosistemov z javnimi ključi, bistveno težji, jih bodo zdaj znova napadli z različnih koncev.

***Ko ste končali podoktorski študij v Kanadi in se vrnili domov, ste začeli voditi seminar iz kriptografije ter s tem začeli v Sloveniji razvijati čedalje bolj pomembno področje kriptografije, nato pa ste ustanovili še Center za kriptografijo in računalniško varnost.***

Na Oddelku za kombinatoriko in optimizacijo Univerze v Waterlooju sem preživel devet let. Veliko tega časa sem posvetil tudi uporabnim področjem, kot so kriptografija, teorija kodiranja in statistični dizajn. Pridobljeno znanje sem želel prenesti domov in tako zdaj tudi v Sloveniji aktivno spremljamo razvoj kriptografije. Kmalu se bo namreč začelo že šesto leto delovanja seminarja iz kriptografije na Inštitutu za matematiko, fiziko in mehaniko v Ljubljani (glej http://valjhun.fmf.uni-lj.si/~ajurisic/seminar). Vsi, ki jih zanima kriptografija, so vabljeni, da se oglasijo.

Vsako drugo leto je na podiplomskem študiju Fakultete za računalništvo in informatiko v Ljubljani ponujen izbirni predmet Kriptografija in računalniška varnost, na Oddelku za matematiko, FMF, pa smo imeli tudi že dva tečaja iz kriptografije za podiplomce.

Na Oddelku za kombinatoriko in optimizacijo v Kanadi so leta 1997 ustanovili Center za uporabne kriptografske raziskave. Ta je izredno poživil aktivnosti. Na Politehniki Nova Gorica nas je to spodbudilo, da tudi mi ustanovimo Center za kriptografijo in računalniško varnost in tako poskušamo doseči večjo povezanost med matematiko, računalništvom in elektrotehniko.

***Kje je težišče vašega raziskovalnega dela?***

Ukvarjam se z uporabo algebre in geometrije v diskretni matematiki ter s kriptografijo in računalniško varnostjo. V kriptografiji so me zaradi uporabnosti in elegance najbolj pritegnili kriptosistemi z javnimi ključi in eliptičnimi krivuljami.

Da bi se približala konkretnim uporabam, naša skupina preučuje tudi pametne kartice. Tako smo na primer izvedli preliminarno študijo varnosti zdravstvene kartice. Zadnje čase pa se ukvarjamo tudi s študijo varnosti kriptografskih protokolov.

***Nam lahko opišete kakšen konkreten primer?***

Na primer ko želimo vstopiti v neko pisarno, urad, trgovino, moramo najprej ob primernem času najti prava vrata, stavbo, nato potrkati, pozvoniti, počakati na povabilo, vstopiti, pozdraviti in se morda še predstaviti pred vstopom ali po njem. To je primer protokola, ki se ne razlikuje kaj dosti od protokola, po katerem se morata obnašati dve napravi, ki želita sodelovati prek interneta. Če nato obiskovalec želi prevzeti določeno blago ali overiti svojo prisotnost, mora še plačati oziroma se podpisati. V času mrež pa si želimo zmožnosti plačevanja in overjanja tudi prek interneta ali pa brez neposrednega dostopa do podatkovnih baz, kot so sodni oziroma matični registri in banke. Seveda ne gre brez zapletov. Ker so naše računske in spominske možnosti precej omejene, si v drugem primeru običajno pomagamo s pametno kartico, ki lahko predstavlja računalnik v našem žepu, a tudi s precej omejenim pomnilnikom in procesorsko močjo. V obeh primerih pa ne gre brez kriptografije in učinkovitega izbiranja naključnih praštevil. ■

## Vohunova dilema


Da bi lažje razumeli potrebo po varnem načinu sporazumevanja, si oglejmo primer problema, ki lahko nastopi, če za varnost ni dovolj poskrbljeno oziroma če je protokol pomanjkljiv.

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:

– »Geslo ali streljam ...«

Kako naj vohun ve, s kom ima opravka? Kako lahko prepriča »stražarja«, da pozna geslo, ne da bi ga pri tem izdal morebitnemu vsiljivcu/prisluškovalcu?

**Profesor Jurišić, ki se je rodil leta 1963 v Ljubljani, je po letu magistrskega študija na domači univerzi leta 1988 nadaljeval študij na Oddelku za kombinatoriko in optimizacijo na Univerzi Waterloo v Kanadi. Leta 1990 je magistriral in 1995. doktoriral. Sledil je dveletni industrijski podoktorski študij na istem oddelku in v podjetju Certicom Corp., Mississauga, ter v šolskem letu 1997/98 še postdoc na Inštitutu za matematiko, fiziko in mehaniko (IMFM) v Ljubljani. Od leta 1998 predava matematiko na Politehniki Nova Gorica (PNG) in vodi seminar iz kriptografije na IMFM. Leta 2000 je na PNG ustanovil Center za kriptografijo in računalniško varnost.**