PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **22** (1994/1995)
Številka 6
Strani 354–357

Marija Vencelj:

ŠIFRIRANJE Z JAVNIM KLJUČEM

Ključne besede: matematika, kriptologija, kriptografija, kriptoanaliza, javni ključ, RSA metoda.

Elektronska verzija: http://www.presek.si/22/1238-Vencelj.pdf

ŠIFRIRANJE Z JAVNIM KLJUČEM

V prejšnji številki Preseka smo spoznali nekaj preprostih tajnopisnih metod. Za večino med njimi je eden največjih problemov prenos šifrirnega ključa. Ta pomembni podatek, ki ga potrebuje prejemnik za dešifriranje sporočila, moramo pri teh metodah pogosto menjati, da bi zmedli nepoklicano osebo, ki bi prestregla sporočilo; vsakokrat je treba poskrbeti za varen prenos ključa med pošiljateljem in prejemnikom.

V poznih sedemdesetih letih pa so razvili kriptografske metode, ki ne zahtevajo nikakršnega prenosa ključa. Pravimo jim metode šifriranja z javnim ključem. Srž metode je v tem, da lahko prejemnik povsem javno objavi nekaj števil, ki predstavljajo ključ za šifriranje sporočil, ki bi mu jih kdo želel poslati. Samo on pa pozna skrivna števila, s katerimi je moč ta sporočila dešifrirati.

Med metodami šifriranja z javnim ključem je najbolj znana RSA metoda. Za uspešno (varno) delo s to metodo uporabljajo zelo velika števila, zato so tako za šifriranje kot za dešifriranje potrebni računalniki. Tudi z računalniki pa je praktično nemogoč vdor v šifrirni sistem. Edini način za zlom šifre je namreč odkritje skrivnih dešifrirnih števil, ki jih pozna le prejemnik. V principu je ta števila sicer moč dobiti iz javno objavljenih šifrirnih števil, v praksi pa bi to zahtevalo mesece dela z računalnikom.

Metoda RSA

Metoda nosi ime po začetnicah priimkov Ronalda Rivesta, Adija Shamirja in Leonarda Adlemana s Tehnološkega inštituta Massachusetts v ZDA, ki so jo razvili leta 1978. Njena varnost temelji na dejstvu, da je razmeroma lahko najti zelo velika praštevila in zelo težko razstaviti na prafaktorje števila, ki so produkti velikih praštevil (če poznamo samo produkt). V praksi uporabljajo praštevila, ki se dajo zapisati z najmanj petdeset desetiškimi števkami, njihovi produkti torej z vsaj sto desetiškimi števkami.

Samo težavnost faktoriziranja lahko opazimo celo že pri zelo majhnih številih. Poskusite na primer brez računalnika razstaviti na prafaktorje število 54 053. Videli boste, da je precej teže priti do rezultata $54\,053 = 191 \cdot 283$, kot pa ugotoviti, da sta 191 in 283 praštevili in ju zmnožiti.

Kot pri metodah, ki smo jih spoznali zadnjič, tudi pri metodi RSA nadomestimo besedila sporočil s števili. Vsako črko lahko npr. nadomestimo s številom, ki pomeni njeno mesto v abecedi. Pri tem priredimo črkam od *A* do *I* števila 00 do 09 namesto 0 do 9. Brez tega previdnostnega ukrepa

bi, denimo, ne vedeli, ali pomeni število 12 črko M ali par črk BC (ki bo tako predstavljen z 0102). Besedilo z n črkami tako nadomestim z zlepkom n dvomestnih števil, na katerega lahko gledamo kot na $2n$–mestno število.

Prejemnikova skrivna števila sta dve veliki praštevili p in q ter število N, ki je tuje s produktom $(p-1)(q-1)$. Števili, ki ju prejemnik javno objavi, sta produkt pq in pozitivno število M z lastnostjo, da je ostanek deljenja števila MN s številom $(p-1)(q-1)$ enak 1, torej

$$MN \equiv 1 (\mathrm{mod}\ (p-1)(q-1)).$$

Javno objavi tudi postopek šifriranja. Vsak, ki mu želi poslati tajno sporočilo, katerega predstavlja število x, naj mu posreduje število y, ki je ostanek deljenja števila x^M s produktom pq. Šifra y je torej najmanjše nenegativno število, ki ustreza kongruenci

$$y \equiv x^M (\mathrm{mod}\ pq).$$

Pri tem mora število x izpolnjevati pogoj $0 \leq x < pq$. (Ta pogoj izpolnjuje tudi y.) Če je sporočilo predolgo, ga je potrebno razbiti na kose, ki predstavljajo števila, manjša od pq, in izvesti navedeni račun za vsak kos posebej.

Prejemnik dešifrira sporočilo tako, da izračuna ostanek deljenja števila y^N s produktom pq, kjer je N njegovo skrivno število. Originalno število x (sporočilo) je torej najmanjše nenegativno število, za katerega velja

$$x \equiv y^N (\mathrm{mod}\ pq).$$

Primer. Za ilustracijo metode ne bomo uporabili velikih števil, ki so v navadi v praksi; potek bomo lahko pregledneje predstavili z majhnimi števili. Zaradi preglednosti se bomo tudi izognili podrobnemu računanju, ki ga lahko opravite sami.

Naj si je prejemnik za skrivna števila izbral $p = 11$, $q = 13$ in $N = 7$. Ne spreglejmo, da je število N tuje s številom $(p-1)(q-1) = 120$. Iz teh števil izračuna (z uporabo Evklidovega algoritma ali kako drugače), da je 103 najmanjše pozitivno število M, ki izpolnjuje pogoj $7M \equiv 1 (\mathrm{mod}\ 120)$.

Nato prejemnik objavi naslednje sporočilo: "Kdor mi želi poslati tajno sporočilo, ki ga na običajni način (zamenjava črk z dvomestnimi števili) predstavlja število x, naj mi posreduje ostanek deljenja števila x^{103} s številom 143."

Sedaj je na vrsti pošiljatelj. Recimo, da želi poslati prejemniku sporočilo SOS, ki ga predstavlja število 181518 (S=18, O=15). Ker je število preveliko, ga mora razbiti na tri kose, manjše od 143, to je na števila 18, 15, 18. Nato izračuna, da je $18^{103} \equiv 112 (\mathrm{mod}\ 143)$ in $15^{103} \equiv 141 (\mathrm{mod}\ 143)$. (S tem je kar nekaj dela, če boste računali peš, z računalnikom pa boste hitro gotovi.) Odposlati mora torej števila 112, 141, 112.

Ko pride to sporočilo v roke prejemniku, ta izračuna $112^7 \equiv 18 (\mathrm{mod}\ 143)$ in $141^7 \equiv 15 (\mathrm{mod}\ 143)$ in v nizu 18, 15, 18 prepozna klic na pomoč.

Gotovo ste se ob tem vprašali, zakaj metoda deluje. Kako to, da opisano zaporedje šifrirnega in dešifrirnega postopka vrne na koncu originalno sporočilo? Podrobnejša razlaga razlogov bi bila za večino Presekovih bralcev pretežka. Za tiste radovednejše pa le povejmo, da je skrita v naslednjem izreku.

Izrek. Če sta p in q različni praštevili in je

$$MN \equiv 1 (\mathrm{mod}\ (p-1)(q-1)),$$

potem velja

$$(x^M)^N \equiv x (\mathrm{mod}\ pq).$$

Podpisovanje

Pomemben del tajnega sporočila pa tudi vsakega drugega dokumenta je podpis, ki potrjuje njegovo verodostojnost. Ker pri pošiljanju sporočil po elektronski pošti ne moremo prenašati fizičnega podpisa, je potrebno poskrbeti za drugačno potrjevanje pristnosti.

Ena dodatnih lastnosti metode RSA je prav varno prenašanje podpisa pošiljatelja. Glede na to, da so javna šifrirna števila prejemnika splošno znana, bi npr. lahko kdo prejemniku poslal lažno šifrirano sporočilo, podpisal pa verodostojno drugo osebo in s tem prejemnika zavedel.

Spet si kar na primeru oglejmo, kako lahko z metodo RSA kaj takega preprečimo.

Denimo, da si Urša in Vinko izmenjujeta tajna sporočila. Označimo z M_U in $a_U = (pq)_U$ ter M_V in $a_V = (pq)_V$ Uršini oziroma Vinkovi javni šifrirni števili. Nadalje naj bosta N_U in N_V njuni skrivni dešifrirni števili. Pa naj želi Vinko poslati Urši svoj podpis, ki ga predstavlja število v. V ta namen šifrira podpis s svojim skrivnim številom N_V in svojim javnim številom a_V, to je, izračuna najmanjše nenegativno število z, ki izpolnjuje pogoj $z \equiv v^{N_V} (\mathrm{mod}\ a_V)$. Urša dobljeno sporočilo dešifrira s ključem, ki ga predstavljata Vinkovi javni šifrirni števili M_V in a_V, to je, poišče najmanjše