

Bouře ve sklenici vody

Mezi uživateli RSA nedávno vzbudila značný rozruch práce profesora Bernsteina o návrzích na zlepšení faktorizačních metod. Neporozumění základním matematickým vztahům totiž způsobilo, že její dopad byl přeceněn, a nebýt zklidňujících zásahů odborníků, mohlo to skončit dokonce odvoláním vydaných certifikátů...

laické veřejnosti je známo, že pokud by se podařilo najít efektivní algoritmus na faktorizaci velkých čísel, byl by prolomen šifrovací algoritmus RSA. Ten je používán s moduly (tedy čísly, která nemá být možné faktorizovat) v různém rozsahu, nejčastěji o 1024 bitech. O problému faktorizace obecně i o faktorizaci 512bitového čísla konkrétně jsme už v Chipu psali, v [5] jsme

faktorizace 1024bitového modulu RSA – protože vypočítaná čísla (čas řádu 2^{53} , paměť 2^{36}) byla směšně nízká, kdo by si po takovém vysvětlení neudělal závěr, že algoritmus RSA padl!

Jako obvykle, polínko do ohně nezapomněli přiložit ani rádoby odborní novináři. „Už se spekuluje o tom, co s RSA a asymetrickou kryptografií“, „NSA převádí citlivá

Bernsteinův příspěvek neznamena pro 1024bitové moduly RSA žádné ohrožení.

také podrobně popisovali metodu NFS (GNFS), která je v současnosti nejvýkonnější metodou pro faktorizaci velkých čísel.

Bernstein (viz [4]) přinesl náměty na některá její zlepšení. Někteří „také odborníci“ pak z toho nesprávně vyvozovali dopad „na obrovskou řadu praktických aplikací“. Nezasvěcení byli strašeni příkladem možné

data na ECC“, „Bernstein už shání peníze na své experimenty“, a dokonce i „Podle předběžných odhadů se takto posun bezpečné délky parametrů RSA dostává nad hranici 2000“ – tak a podobně hlásaly novinu do světa nejruznější „zasvěcené“ komentáře. Byla to zkrátka opravdu pěkná kachna, kterou spousta lidí „zbaštila i s navijákem“.

JAK JE TO DOOPRAVDY

Bernsteinův článek i neuvěřitelné výklady k němu by vydaly na humornou povídku – ale jen pro matematiky, ostatní by si hru s matematickými symboly těžko vychutnali. Oč tedy šlo? Bernstein navrhl několik úprav v metodě NFS, které by pro velmi velká n – tedy pro moduly o délce blízké se k nekonečnu – mohly přinést značná zlepšení oproti stávající NFS. Přitom Bernstein definoval efektivitu metody jako součin počtu operací a paměti (což nazývá také *cenou za faktorizaci*). Několika triky (zatím pouze na papíře) pak docílil, že pokud by fungovaly, cena by se snížila.

Velmi zhruba lze jeho závěr vyjádřit tak, že jestliže jsme dříve byli schopni faktorizovat moduly o délce n bitů, pak nyní by to bylo 3^n bitů. Jedná se však o odhady limitní, pro čísla n blízké se k nekonečnu (nezapomeňme, že v limitních úvahách jsou čtvereční kilometry křemíkové plochy celkem bezvýznamnou opovržením hodnou konstantou). Jejich cílem je popsat *asymptotické* chování cenové funkce, nikoliv její konkrétní funkční hodnoty. Vidíme z nich, **jakého druhu** je závislost ceny faktorizace na délce modulu, **nikoliv konkrétní počet** sekund, ■

- megabajtů paměti nebo dolarů, nutných pro faktorizaci modulu dané délky. Bernsteinovy vzorce tedy nelze mechanicky použít na dnešní modul o délce 1024 bitů, ale ani na délku 512 bitů nebo třeba 8192 bitů, protože tyto vzorce se prostě takových směšných čísel netýkají.

Kdo na tuto skutečnost zapomene, může pak snadno usoudit, že pokud už bylo faktorizováno 512bitové číslo, je teď v ohrožení číslo 1536bitové. Takováto (dez)interpretace Bernsteinových výsledků pochopitelně zdvihla vlnu zájmu, protože většina modulů používá délku 1024 bitů. Ke vši smůle navíc (těžko říci, jak) vznikl silný dojem, že už stačí jen nakoupit příslušný hardware, a RSA putuje na smetišť dějin...

Skutečnost je samozřejmě zcela jiná, což dokládáme názory tří odborníků. Prvním je sám profesor Bernstein, druhým je známý bezpečnostní specialista Bruce Schneier, kterého bychom mohli v tomto „sporů“ považovat za nezávislého, a třetím jakoby „poškozený“ Bernsteinovým příspěvkem, tj. společnost RSA Security. Všichni tři se shodují v následujícím faktu, který z jejich obsáhlejších vyjádření (viz literatura, doporučujeme přečíst celá jejich stanoviska) lze shrnout asi takto:

Označme $f(n)$ délku modulu, který Bernsteinova zlepšení metody NFS zvládnou faktorizovat ve stejném čase, jako předchozí stroje faktorizovaly n -bitové moduly metodou NFS bez těchto zlepšení. Vše, co víme, je, že $f(n)$ pro n blízká nekonečnu může být v ideálním případě nejlépe $3n$. Nevíme však nic o $f(n)$ pro malá čísla, například 512, nevíme, zda $f(512)$ není dokonce menší než 512.

Tedy, mimo jiné, pro malá čísla, jako jsou 512, 1024 nebo 4096, mohou Bernsteinova zlepšení ve skutečnosti oproti klasické metodě NFS dokonce **zhoršovat cenu faktorizace**. Bernstein to přímo stvrzuje ve svém e-mailu [2] slovy: „*V současné době nelze ani stanovit cenu za faktorizaci 1024-, 1536- nebo 2048bitového modulu,*“ a podobně reaguje Schneier [1]: „*Je nepravděpodobné, že by Bernsteinova zlepšení byla využitelná ke zlepšení rychlosti faktorizace prakticky použitelných modulů.*“ RSA Laboratories jen lakonicky konstatují [3]: „*Bernsteinův příspěvek nepřinesl pro 1024bitové moduly žádné nové ohrožení.*“

TAKŽE ŽÁDNÝ POPLACH...

Pan profesor Bernstein za nesprávné výklady různých komentátorů samozřejmě nemůže a zaslouží si ocenění za skvělé nápady, kde

by se co dalo doladovat při **realizaci** metody NFS pro faktorizaci. Jsou to nové myšlenky – sice nijak zvlášť převratné, ale osvěžují výzkum na tomto poli. Možná z nich vzejde něco většího, možná o nich za pár let nebude nikdo vědět. Podstatné však je, že Bernsteinův příspěvek RSA nepohřbil, na čemž se odborníci vzácně shodují. Patříte-li tedy k těm uživatelům RSA, kteří po nejrůznějších internetových diskusích na toto téma propadli panice či třeba jen znejistěli, snad jsme vám tímto článkem vrátili klidný spánek.

■ ■ ■ Vlastimil Klíma, *autor@chip.cz*

LITERATURA:

- [1] Schneier B.: CRYPTO-GRAM, March 15, 2002, <http://www.counterpane.com/crypto?gram.html>
- [2] e-mail, 28 Feb 2002, From: "D. J. Bernstein" <djb@cr.yp.to>, Subject: What's going on with factorization
- [3] Has the RSA algorithm been compromised as a result of Bernstein's paper?, April 8, 2002, www.rsasecurity.com/rsalabs/technotes/bernstein.html
- [4] Bernstein D. J.: Circuits for integer factorization: a proposal, <http://cr.yp.to/papers/nfscircuit.ps> (původní článek)
- [5] Klíma V.: Dvě čísla za 200 000 dolarů, Chip 9/01, 10/01, dostupné též na [6]
- [6] Archiv článků: <http://www.decros.cz/bezpecnost/kryptografie.html>