RSA pro začátečníky

Jakub „Roman“ Klemsa

Abstrakt. RSA je moderní (1977) asymetrická šifrovací metoda, na které je postavena většina dnešních šifrovacích systémů. Cílem přednášky bude ukázat princip fungování na základě Eulerovy věty a ukázka na konkrétním příkladě. Předvedeme si i některé způsoby zlomení této šifry, taktéž na příkladech.

Tvrzení. *Pro libovolná dvě celá čísla a, b, kde alespoň jedno je nenulové, platí*

$$\mathrm{NSD}(a,b) = \mathrm{NSD}(a-b,b).$$

My toto tvrzení budeme používat pouze pro dvě přirozená čísla.

Pozorování. *Pro každé přirozené číslo a platí:*[1] $\mathrm{NSD}(a,1) = 1$, $\mathrm{NSD}(a,0) = a$.

Eukleidův algoritmus

Eukleidův algoritmus převádí hledání NSD dvou přirozených čísel na hledání NSD, kde jedno číslo je ostře menší. BÚNO předpokládejme $a > b$ a postupujme takto, dokud jsou oba členy NSD nezáporné:

$$\mathrm{NSD}(a,b) = \mathrm{NSD}(a-b,b) = \ldots = \mathrm{NSD}(a-k_1 b, b).$$

Označíme $r_1 := a - k_1 b = a \bmod b$ a víme, že $0 \leq r_1 < b$. Pokud $r_1 = 0$, algoritmus končí s hodnotou b, pokud ne, opakujeme algoritmus pro dvojici b, r_1:

$$\mathrm{NSD}(a,b) = \mathrm{NSD}(r_1,b) = \mathrm{NSD}(r_1, b-k_2 r_1) = \mathrm{NSD}(r_1,r_2),$$

kde $r_2 = b \bmod r_1$. Rekurzivně opakujeme, dokud nedojdeme k $\mathrm{NSD}(r_k,0) = r_k$.

Tvrzení. *Eukleidův algoritmus skončí po konečném počtu kroků ve stavu, kdy* $\mathrm{NSD}(a,b) = \mathrm{NSD}(r_k,0) = r_k$.

Klíčová slova. Eukleidův algoritmus, Malá Fermatova věta, Eulerova funkce, Eulerova věta, RSA, Fermatova a Pollardova metoda.

[1] $(\forall k \in \mathbb{N})(k \mid 0)$

Tvrzení. *Zpětným postupem dokážeme z Eukleidova algoritmu najít celá čísla x_0, y_0 taková, že* $\mathrm{NSD}(a,b) = ax_0 + by_0$. *Protože* $k(ab - ba) = 0$ *a každé z čísel* a, b *je dělitelné* $\mathrm{NSD}(a,b)$, *najdeme zbývající řešení pomocí*

$$\mathrm{NSD}(a,b) = k\left(a\frac{b}{\mathrm{NSD}(a,b)} - b\frac{a}{\mathrm{NSD}(a,b)}\right) + ax_0 + by_0$$

ve tvaru $x = x_0 + k(b/\mathrm{NSD}(a,b))$, $y = y_0 - k(a/\mathrm{NSD}(a,b))$, *kde* $k \in \mathbb{Z}$. *Ukazuje se, že toto jsou již všechna řešení rovnice* $ax + by = \mathrm{NSD}(a,b)$.

Cvičení. Pomocí Eukleidova algoritmu najděte $\mathrm{NSD}(432, 234)$ a dvě „nejbližší“ dvojice celých čísel x, y, aby $\mathrm{NSD}(432, 234) = 432x - 234y$.

Základní aritmetické věty

Tvrzení. (Malá Fermatova věta) *Pro libovolné prvočíslo* p *a přirozené číslo* a *nesoudělné s* p *platí*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Definice. (Eulerova funkce) Hodnotu Eulerovy funkce $\varphi\colon \mathbb{N} \to \mathbb{N}$ definujeme pro n jako počet přirozených čísel nepřevyšujících n, která jsou s n nesoudělná, tedy

$$\varphi(n) := \#\{k \in \mathbb{N} : k \leq n,\ k \perp n\}.$$

Cvičení. Spočítejte hodnotu Eulerovy funkce, kde p, q prvočísla, $k \in \mathbb{N}$: $\varphi(1)$, $\varphi(p)$, $\varphi(p^k)$, $\varphi(pq)$.

Tvrzení. (Eulerova věta) *Pro libovolná dvě přirozená čísla* a, n, $a \perp n$, *platí*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Poznámka. Eulerova věta pro n prvočíslo přechází v Malou Fermatovu větu.

Asymetrická šifra RSA

Šifrovací metodu RSA navrhli roku 1977 matematici Rivest, Shamir a Adleman. Jedná se o šifru s jedním veřejným šifrovacím klíčem a jedním soukromým, dešifrovacím, odtud asymetrická.

Pro šifrování pomocí RSA budeme potřebovat dvě velká (ale opravdu velká) prvočísla p a q, jejich vynásobením dostáváme tzv. modulus $n = pq$. Odtud známe i hodnotu Eulerovy funkce $\varphi(n) = (p-1)(q-1)$. Dále vygenerujeme veřejný exponent e takový, aby $e \perp \varphi(n)$, $1 < e < \varphi(n)$. Nesoudělnost ověříme Eukleidovým algoritmem, odkud zjistíme i koeficienty d a k takové, že $ed - k\varphi(n) = 1$. Najdeme d takové, že $1 < d < \varphi(n)$. Toto d pak bude náš soukromý exponent.

Shrňme si, co uveřejníme a co naopak přísně utajíme: dvojici (n, e) uveřejníme jako veřejný klíč, dvojici (n, d) uchováme jako soukromý klíč a prvočísel p, q společně s hodnotou $\varphi(n)$ se bezpečně zbavíme.
Postup šifrování:

(i) od příjemce naší zprávy si necháme poslat veřejný klíč (n, e)
(ii) zprávu reprezentovanou číslem $m < n$ zašifrujeme do $c = m^e \bmod n$
(iii) příjemce naši šifrovanou zprávu c rozšifruje pomocí soukromého klíče (n, d) stejným způsobem: $m = c^d \bmod n$

Tvrzení. *Pro m, e, d, n splňující požadavky RSA platí*

$$c^d = m^{ed} \equiv m \pmod{n}.$$

Na tomto tvrzení stojí funkčnost RSA. Její bezpečnost jsme však tímto neukázali.

Příklad. Kelišová chce poslat Cecilce nový drb podléhající vysokému utajení. Cecilka proto vygeneruje dvě „velká“ prvočísla 11 a 13, spočítá $n = 143$, $\varphi(n) = 120$ a vygeneruje $e = 13$. Eukleidovým algoritmem dostane

$$\begin{aligned} 120 &= 9 \cdot 13 + 3, \\ 13 &= 4 \cdot 3 + 1, \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

Odtud $120 \perp 13$ a zná rozklad $1 = 13 - 4 \cdot 3 = 13 - 4 \cdot (120 - 9 \cdot 13) = 37 \cdot 13 - 4 \cdot 120$ neboli $d = 37$. Dvojici $(143, 13)$ pošle Kelišce jako veřejný klíč. Kelišová bude chtít, jak jinak, poslat šifrovanou zprávu 42, postupovat bude takto:

(i) z důvodu zjednodušení výpočtu rozepíše $13 = 2^3 + 2^2 + 2^0$
(ii) $42^{13} = ((42^2)^2)^2 \cdot (42^2)^2 \cdot 42$
(iii) $42 \bmod 143 = 42$
(iv) $42^2 \bmod 143 = 1764 \bmod 143 = 48$
(v) $(42^2)^2 \bmod 143 = 48^2 \bmod 143 = 2304 \bmod 143 = 16$
(vi) $((42^2)^2)^2 \bmod 143 = 16^2 \bmod 143 = 256 \bmod 143 = 113$
(vii) $42^{13} \bmod 143 = (113 \cdot 16 \cdot 42) \bmod 143 = 75936 \bmod 143 = 3$

Kelišová odešle zpět Cecilce zašifrovanou zprávu 3. Cecilka ji stejným způsobem dešifruje svým soukromým klíčem $d = 37$ a vyjde jí dychtivě očekávaná 42.

Jak RSA rozlousknout?

(i) faktorizace n, výpočet $\varphi(n)$, pomocí e pak dopočteme i d
(ii) využití chyby při šifrování (více exponentů k jednomu modulu apod.)
(iii) využití některé slabiny prvočíselné dvojice p, q – viz dále

Faktorizace malých n problém není, problém je ve složitosti algoritmu. Neznáme algoritmus se složitostí nižší než exponencielní (v závislosti na délce modulu), proto

nám stačí číslo n o několik cifer prodloužit a nepříteli bude trvat několikanásobně déle rozklad najít. To činí RSA tak bezpečnou.

Fermatova metoda

Tato metoda předpokládá malý rozdíl p a q, označíme $D := \frac{p-q}{2}$. Všimneme si, že

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2,$$

odtud $n + D^2 = \left(\frac{p+q}{2}\right)^2$. Zkoušíme tedy pro malá D, jestli číslo $n + D^2$ je čtverec. Jakmile takové D najdeme, dopočteme snadno p a q ze soustavy rovnic jako

$$p, q = \sqrt{n + D^2} \pm D.$$

Pollardova $p - 1$ metoda

Pollardova $p - 1$ metoda předpokládá, že alespoň pro jeden faktor n (ozn. p) má číslo $p - 1$ všechny své faktory relativně malé (omezené nějakým b). Nyní můžeme odhadnout[2] například $k = b!$ jako násobek $p - 1$, neboli $p - 1 \mid k$. Dle Fermatovy věty pro dané a nesoudělné s p (což není vůbec problém, např. $a = 2$) platí

$$a^{p-1} \equiv 1 \pmod{p}.$$

Protože $p - 1 \mid k$, můžeme tuto kongruenci umocnit do tvaru

$$a^k \equiv 1 \pmod{p}.$$

Odtud $p \mid \mathrm{NSD}(a^k - 1, n)$, neboli můžeme předpokládat, že $p = \mathrm{NSD}(a^k - 1, n)$. Pokud vyjde 1, náš odhad k nebyl násobkem $p - 1$ ani $q - 1$, pokud vyjde n, odhad k byl násobkem obou. Tímto se dále řídíme a zlepšujeme odhad k. Pro silná p, q je toto hádání velmi obtížné, protože dokud nenatipujeme všechny faktory $p - 1$ (BÚNO), dostáváme jako NSD 1 a o $p - 1$ nadále nic nevíme. A pokud ano, je dost pravděpodobné, že máme i všechny faktory $q - 1$ a dostaneme jako NSD n.

Cvičení. (Za čokoládu) „Kapříci připluli!“ ozvalo se z telefonu. Spolu s tím i dvě čísla, 6901 a 725. Z druhé strany zaznělo 42. Otázkou pro vás je, kolik „kapříků“ letos vylovíme?

Literatura a zdroje

[1] Z. Masáková, *Diskrétní matematika I*, FJFI ČVUT, Praha, 2010.
[2] Wang Baocang, Liu Shuanggen, Hu Yupu, *New weak keys in RSA*, WUJNS, Wuhan, 2006.
[3] Ľ. Balková, *RSA (Úvod do kryptologie)*, FJFI ČVUT, Praha, 2011.

[2] Lze provést i jiný odhad čísla, které by mohlo být násobkem $p - 1$.