RSA a teorie čísel

Jakub „šnEk“ Opršal

Definice. *Buď n přirozené číslo. Řekneme, že čísla $a, b \in \mathbb{N}$ jsou kongruentní modulo n pokud $n \mid (a-b)$. Ekvivalentně pokud a a b dávají stejný zbytek po dělení n. Zapisujeme $a \equiv b \pmod{n}$*

Věta. (Fermat) *Nechť $a \in \mathbb{N}$ a p je prvočíslo, navíc platí $p \nmid a$ pak platí:*

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

Důkaz. Uvažme množinu čísel $\{a, 2a, \ldots, (p-1)a\}$. Tyto čísla dávají po dvou různý zbytek po dělení p, neboť kdyby ne, tj. $ka \equiv la \pmod{p}$) pro nějaká $k, l \in 1, 2, \ldots p-1$ a $k > l$, pak dostáváme $p \mid (ka - la) = (k-l)a$. Tedy p dělí buď a, což je ve sporu s předpokladem věty, nebo $k - l$, což je číslo menší než p, každopádně dostáváme spor. Z toho lze také vidět, že všechna dávají nenulový zbytek po dělení p. Tedy nabývají všech zbytků, proto platí:

$$(p-1)! = 1 \cdot 2 \cdots 3 \equiv a \cdot 2a \cdots (p-1)a = (p-1)! \cdot a^{p-1} \pmod{p}$$

Protože $(p-1)!$ je nesoudělné s p mohu tuto kongruenci pokrátit a dostanu tvrzení věty. □

Věta. (Euler) *Nechť $a, n \in \mathbb{N}$ jsou dvě nesoudělná čísla a $\varphi(n)$ je počet čísel menších nebo rovných n, která jsou s n nesoudělná, pak platí:*

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

Lemma. (Výpočet Eulerovy funkce) *Nechť $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ je prvočíselný rozklad čísla n (tedy p_i jsou po dvou různá prvočísla a α_i jsou přirozená). Pak platí:*

$$\begin{aligned}\varphi(n) =& (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1} = \\ =& n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)\end{aligned}$$

Definice. *Nechť n je přirozené a p prvočíslo, pak řádem čísla n modulo p nazveme nejmenší takové přirozené číslo k, že $n^k \equiv 1 \pmod{p}$.*

Lemma. *Nechť p je prvočíslo a n je přirozené číslo nesoudělné s p a k jeho řád. Čísla a a b jsou libovolná nezáporná celá. Pak platí:*

(i) $n^{ka} \equiv 1 \pmod{p}$
(ii) $n^a \equiv n^b \pmod{p} \iff a \equiv b \pmod{k}$
(iii) $k \mid (p-1)$

Definice. *Nechť n je přirozené číslo. Přirozené číslo a nazveme primitivním prvkem modulo n, pokud je řádu $\varphi(n)$. Ekvivalentně pokud $a, a^1, \ldots, a^{\varphi(n)}$ dávají všechny zbytky modulo n, které jsou s n nesoudělné.*

Lemma. *Je-li p liché prvočíslo, pak existuje primitivní prvek modulo p.*

Věta. *Nechť p je prvočíslo, pak platí:*

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

Věta. (Rabin-Millerův test prvočíselnosti) *Pokud n je přirozené číslo, pak platí implikace:*

$$n \text{ je prvočíslo} \Longrightarrow \forall a \in \{1, 2, \ldots, n-1\} : a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$$

Definice. *Přirozené číslo n nazveme Carmichealovým pokud pro něj platí:*

$$\forall a \in \mathbb{N} : a^n \equiv a \pmod{n}$$

Carmichaelova čísla mají význam v tom, že co se týče prvočíselných testů jsou velmi těžko rozeznatelná oproti prvočíslům (díky tomu se jim říká pseudoprvočísla). Nejmenší Carmichaelova čísla jsou $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$ a $1729 = 7 \cdot 13 \cdot 19$.

RSA

Šifrovací algoritmus RSA patří mezi asymetrické šifry, tedy pro zašifrování a odšifrování jsou použity dva různé (tedy relativně různé) algoritmy. Kvůli tomuto se musí vygenerovat dva klíče a to soukromý a veřejný. Klíče se generují následovně:

(i) Vybereme dost velká a dostatečně náhodná prvočísla p a q.
(ii) Spočítáme $n = pq$ a hodnotu Eulerovy funkce $\varphi(n) = (p-1)(q-1)$. n bude použito jako část obou klíčů, bude se používat jako modul pro veškeré operace.
(iii) Zvolíme náhodné e takové, že $1 < e < \varphi(n)$ a e je nesoudělné s $\varphi(n)$, toto e bude součástí veřejného klíče.
(iv) Ze znalosti $\varphi(n)$ spočteme d tak, že $de \equiv 1 \pmod{\varphi(n)}$, d bude použito jako součást soukromého klíč.

Tedy máme veřejný klíč a to dvojici čísel (n, d) a soukromý klíč, dvojici (n, e).

Algoritmy na zašifrování a odšifrování jsou jednoduché. Tajnou zprávu, kterou převedeme do nějakého rozumného číselného formátu, zašifrujeme tak, že ji umocníme na e modulo n. Odšifrujeme tak, že šifrový text umocníme na d opět modulo n.

Uveďme ještě jeden nereálný, zato o to čitelnější, příklad použití RSA. Nejdříve si vymyslíme dvě prvočísla, třeba $p = 17$ a $q = 29$, spočítáme $n = 17 \cdot 29 = 493$ a $\varphi(n) = 448$ Zvolme si nějaký rozumný veřejný klíč $e = 33$ (e musí být nesoudělné s $\varphi(n) = 448$) a spočítáme k němu soukromý $ed + k\varphi(n) = 1$, použijeme Euklidův algoritmus na čísla $e = 33$ a $\varphi(n) = 448$ a vyjde nám $d = 353$ a jako balast $k = -26$.

A nyní si vyzkoušejme naše klíče s tajnou zprávou $m = 42$. Nejdříve zašifrujeme:

$$s = m^e \bmod n = 42^{33} \bmod 493 = 93,$$

a pak odšifrujeme:

$$m = s^d \bmod n = 93^{353} \bmod 493 = 42.$$

Takže to funguje ;-) (Proč, to už určitě tušíte.)