

Faktorizace pomocí RSA exponentů

aneb proč dva uživatelé nesmějí sdílet stejný modulus

Andrew Kozlík

KA MFF UK

Faktorizace pomocí RSA exponentů

- ▶ Známe-li prvočíselný rozklad $N = pq$ ($p, q \in \mathbb{P}$, $p \neq q$), pak
 - ▶ známe $\varphi(N) = (p - 1)(q - 1)$ a
 - ▶ pro každé $e \in \mathbb{Z}_{\varphi(N)}^*$ umíme najít d , aby $de \equiv 1 \pmod{\varphi(N)}$.
- ▶ A co obráceně?
Umíme snadno faktorizovat N , známe-li jen N , e a d ?

Ano!

- ▶ Najdeme netriviální řešení u kongruence $x^2 \equiv 1 \pmod{N}$.
- ▶ Potom $\text{NSD}(u - 1, N)$ je netriviální dělitel čísla N .

Jak vypadají řešení $x^2 \equiv 1 \pmod{N}$?

Kongruenci upravíme:

$$\begin{aligned} & x^2 \equiv 1 \pmod{N} \\ \iff & N \mid x^2 - 1 \\ \iff & p \mid x^2 - 1 \quad \wedge \quad q \mid x^2 - 1 \\ \iff & x^2 \equiv 1 \pmod{p} \quad \wedge \quad x^2 \equiv 1 \pmod{q} \\ \iff & x \equiv \pm 1 \pmod{p} \quad \wedge \quad x \equiv \pm 1 \pmod{q} \end{aligned}$$

Podle Čínské věty o zbytcích jsou celkem 4 řešení:

| $x \pmod{p}$ | $x \pmod{q}$ | $x \pmod{N}$ |
|--------------|--------------|--------------|
| 1 | 1 | 1 |
| 1 | -1 | u |
| -1 | 1 | $-u$ |
| -1 | -1 | -1 |

Proč to funguje?

- ▶ Máme tedy $u \equiv 1 \pmod{p}$ a $u \equiv -1 \pmod{q}$.
- ▶ Čili $p \mid u - 1$.
- ▶ Ale $q \nmid u - 1$.
(Kdyby totiž q dělilo $u + 1$ a zároveň $u - 1$, tak by dělilo i jejich rozdíl $q \mid (u + 1) - (u - 1) = 2$ a N by bylo sudé.)
- ▶ Proto $\text{NSD}(u - 1, N) = p$.

Kde vzít u ?

- ▶ Víme, že $\text{NSN}(p-1, q-1) \mid de-1$.
- ▶ Necht' $k := de-1 = 2^t r$, kde $t, r \in \mathbb{N}$ a r je liché.
- ▶ $t \geq 1$ protože $\text{NSN}(p-1, q-1)$ je sudé a dělí k .
- ▶ Pro každé $a \in \mathbb{Z}_N^*$ platí $a^{2^t r} = a^{de-1} \equiv 1 \pmod{N}$.
- ▶ Když spočteme pro nějaké $a \in \mathbb{Z}_N^*$ posloupnost

$$a^r, a^{2r}, a^{4r}, a^{8r}, \dots, a^{2^t r} \quad (\text{vše mod } N),$$

mocnění na druhou

mohla by se v ní vyskytovat netriviální odmocnina z 1, tj. u .

- ▶ Pokud ano, říkáme, že a je *dobré*.

Příklad

Máme $N = 221$ a známe RSA exponenty $e = 5$ a $d = 77$.
Faktorizujte N .

► Spočteme $k = de - 1 = 384 = 2^7 \cdot 3$.

► Zvolíme libovolné $a \in \mathbb{Z}_N^*$.

Pro zajímavost jich zkusíme několik: $a = 2, 3, 35, 47$.

| i | 3 | 6 | 12 | 24 | 48 | 96 | 192 | 384 | |
|--------|-----|-----|-----|-----|----|----|-----|-----|------------|
| 2^i | 8 | 64 | 118 | 1 | 1 | 1 | 1 | 1 | dobré a |
| 3^i | 27 | 66 | 157 | 118 | 1 | 1 | 1 | 1 | dobré a |
| 35^i | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | špatné a |
| 47^i | 174 | 220 | 1 | 1 | 1 | 1 | 1 | 1 | špatné a |

► Máme $u = 118$.

► Spočítáme $\text{NSD}(u - 1, N) = \text{NSD}(117, 221) = 13$.

► $221 = 17 \cdot 13$.

Tvrzení

Nechť $a \in \mathbb{Z}_N^*$ je zvolené náhodně s rovnoměrným rozdělením. Potom pravděpodobnost, že algoritmus selže, je nejvýše $\frac{1}{2}$.

Důkaz.

- ▶ Ať s je největší číslo, pro které $\exists b \in \mathbb{Z}_N^* : b^{2^s r} \neq 1$. (Takové s jistě existuje, např. $(-1)^{2^0 r} = -1 \neq 1$.)
- ▶ Definujeme

$$G := \{ g \in \mathbb{Z}_N^* : g^{2^s r} = \pm 1 \}.$$

- ▶ G je podgrupa \mathbb{Z}_N^* .
- ▶ G obsahuje všechna špatná a (a možná i nějaká dobrá a).
- ▶ Ukážeme, že G je netriviální podgrupa \mathbb{Z}_N^* , potom

$$|G| \leq \frac{1}{2} |\mathbb{Z}_N^*|, \quad \text{protože } |G| \text{ dělí } |\mathbb{Z}_N^*|.$$

Důkaz (pokračování).

- ▶ Sestrojíme tedy prvek $c \in \mathbb{Z}_N^*$, který neleží v G .
 - ▶ Máme $b^{2^s r} \not\equiv 1 \pmod{N}$, potom (BÚNO pro p nebo q) platí $b^{2^s r} \not\equiv 1 \pmod{p}$.
 - ▶ Podle Čínské věty o zbytcích existuje $c \in \mathbb{Z}_N^*$ takové, že
 - ▶ $c \equiv b \pmod{p}$, (pak $c^{2^s r} \not\equiv 1 \pmod{N}$)
 - ▶ $c \equiv 1 \pmod{q}$, (pak $c^{2^s r} \equiv 1 \pmod{N}$)
- čili $c \notin G$. □

