Číselné algoritmy

RSA a problém faktorizace

1. 3. 2021

Stručný přehled přednášky

1. Faktorizační algoritmy
   - Pollard ϱ
   - Pollard $p-1$
   - ECM
   - CFRAC
   - QS
   - Nebudeme probírat: NFS, SQUFOF, Shorův algoritmus
2. Odmocňování
   - Hledání odmocniny v konečném tělese
   - Aproximace odmocniny celého čísla (řetězové zlomky)
   - Odmocňování a problém faktorizace
3. Diskrétní logaritmus
   - Přehled základních algoritmů
   - Faktorizace a problém diskrétního logaritmu
   - Dolní odhad složitosti generických algoritmů pro výpočet diskrétního logaritmu

Textbook RSA - připomenutí

Máme $p \neq q \in \mathbb{P}$, $N = pq$. Značíme

$$\mathbb{Z}_N^* := \{z \in \mathbb{Z}_N \mid \mathrm{NSD}(z, N) = 1\}$$

(grupa invertibilních prvků okruhu $\mathbb{Z}_N$).
Víme $|\mathbb{Z}_N^*| = \varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$.
Volíme $e \in \mathbb{N}$, $\mathrm{NSD}(e, \varphi(N)) = 1$.
Dopočteme $d \in \mathbb{N}$ tak, aby $ed \equiv 1 \pmod{N}$.

Lemma

Pro každé $m \in \mathbb{Z}_N$ je $(m^e)^d \equiv m \pmod{N}$.

RSA je kryptosystém s veřejným klíčem (N, e) a soukromým klíčem d.
Zpráva $m \in \mathbb{Z}_N$ je zašifrována jako $c := (m^e) \bmod N$.
c lze pak dešifrovat výpočtem $m = c^d \bmod N$.

Důkaz lemmatu - připomenutí CRT

Lemma

Pro každé $m \in \mathbb{Z}_N$ je $(m^e)^d \equiv m \bmod N$.

Důkaz: Máme vlastně dokázat, že v okruhu $\mathbb{Z}_N$ platí rovnost $m^{ed} = m$ pro každé $m \in \mathbb{Z}_N$.
Dále víme, že

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q$$

$$z \mapsto (z \bmod p, z \bmod q)$$

je izomorfismus okruhů. Stačí proto ukázat, že rovnost $m = m^{ed}$ platí v okruhu $\mathbb{Z}_p$ i v okruhu $\mathbb{Z}_q$.
Máme $m \in \mathbb{Z}_p$. Pro $m = 0$ je jistě $m = m^{ed}$.
Pro $m \neq 0$ dává malá Fermatova věta $m^{p-1} = 1$.
Dále $ed \equiv 1 \pmod{(p-1)(q-1)}$, tedy také
$ed \equiv 1 \pmod{(p-1)}$, tedy $ed = k(p-1)+1$ pro $k \in \mathbb{N}_0$
Takže v okruhu $\mathbb{Z}_p$ platí rovnost

$$m^{ed} = (m^{p-1})^k m = m$$

Analogicky dokážeme rovnost $m^{ed} = m$ i v okruhu $\mathbb{Z}_q$.

Hledání soukromého klíče a problém faktorizace

Předpokládejme, že máme k dispozici orákulum, které pro veřejný RSA klíč (N, e) určí $d \in \mathbb{N}$ (rozumně velké např $d \leq N$) tak, aby platilo

$$ed \equiv 1 \pmod{\varphi(N)}.$$

Ukážeme, že pak lze efektivně faktorizovat RSA modulus N.
Budeme dále předpokládat, že N je liché, tedy $4 \mid \varphi(N)$.
Máme tedy $e, d \in \mathbb{N}$ splňující $ed \equiv 1 \pmod{\varphi(N)}$. Označíme

$$s := \max\{t \in \mathbb{N} \mid 2^t \mid ed - 1\}$$

tedy $ed - 1 = 2^s \ell$, kde ℓ je liché.

Řád prvku

Máme konečnou grupu G, $g \in G$. Řád prvku g definujeme jako

$$o(g) := \min\{k \in \mathbb{N} \mid g^k = 1_G\}$$

Mohli bychom si pamatovat, že

- $g^m = 1$ právě když $o(g) | m$
- $o(g) = |\langle g \rangle|$, tedy $o(g) \mid |G|$
- $g^{|G|} = 1_G$, tedy také $g^z = 1_G$ pro $g \in G$ a $|G| \mid z \in \mathbb{Z}$
- $o(g) = 1$ právě když $g = 1_G$
- Je-li H grupa a $\varphi\colon G \to H$ homomorfismus grup, je $o_H(\varphi(g)) \mid o_G(g)$ pro každé $g \in G$ (platí totiž $1_H = \varphi(1_G) = \varphi(g^{o_G(g)}) = \varphi(g)^{o_G(g)}$)

Aplikace v $\mathbb{Z}_N^*$

Tvrzení

Máme $ed - 1 = 2^s \ell$, *kde* ℓ *je liché a* $ed \equiv 1 \pmod{\varphi(N)}$. *Pak pro každé* $a \in \mathbb{Z}_N^*$ *je* $o(a^\ell \bmod N) = 2^i$ *pro nějaké* $i \in \{0, \ldots, s\}$

Důkaz: Pracujeme v grupě $G = \mathbb{Z}_N^*$, tedy pro $x, y \in \mathbb{Z}_N^*$ je $x \cdot y = xy \bmod N$.
Protože $ed - 1$ je násobek $|G| = \varphi(N)$, je $g^{ed-1} = 1$ pro každé $g \in G$. Tedy také $(g^\ell)^{2^s} = 1$.
Pro každé $a \in \mathbb{Z}_N^*$ je řád prvku $a^\ell \bmod N$ v grupě $\mathbb{Z}_N^*$ dělitelem 2^s.

Jak faktorizovat N pomocí vhodného prvku

Tvrzení

Nechť $a \in \mathbb{Z}_N^*$ splňuje

$$o_{\mathbb{Z}_p^*}(a^\ell \bmod p) \neq o_{\mathbb{Z}_q^*}(a^\ell \bmod q)$$

Pak existuje $t \in \{0, \ldots, s-1\}$ takové, že

$$1 < \mathrm{NSD}(N, a^{2^t} - 1) < N$$

Důkaz: Víme, že $o_{\mathbb{Z}_N^*}(a^\ell \bmod N)$ je mocnina dvou.
Máme homomorfismy $\varphi_p \colon \mathbb{Z}_N^* \to \mathbb{Z}_p^*$ a $\varphi_q \colon \mathbb{Z}_N^* \to \mathbb{Z}_q^*$ splňující $\varphi_p(a^\ell \bmod N) = a^\ell \bmod p$, $\varphi_q(a^\ell \bmod N) = a^\ell \bmod q$.
Takže $o_{\mathbb{Z}_p^*}(a^\ell \bmod p)$ i $o_{\mathbb{Z}_q^*}(a^\ell \bmod q)$ jsou mocniny dvou.
Označme $t_1, t_2 \in \{0, \ldots, s\}$ tak, že $o_{\mathbb{Z}_p^*}(a^\ell \bmod p) = 2^{t_1}$ a $o_{\mathbb{Z}_p^*}(a^\ell \bmod p) = 2^{t_2}$.
Z předpokladu máme $t_1 \neq t_2$. Nechť např. $t_1 < t_2$. Pak $\mathrm{NSD}(a^{2^{t_1}} - 1, N) = p$.

Algoritmus

Vstup: RSA klíč (N, e)

Výstup: vlastní dělitel N, nebo neúspěch

Orákulum: $d \in \mathbb{N}$, $ed \equiv 1 \pmod{\varphi(N)}$

1. Zvol $a \in \{1, \ldots, N-1\}$ náhodně
2. spočti $g := \mathrm{NSD}(a, N)$
3. if $g > 1$ then return g
4. urči ℓ, s, $ed - 1 = 2^s \ell$, kde ℓ liché
5. $t := 0$
6. while (g $= 1$) do
   $g := \mathrm{NSD}(a^{2^t \ell} - 1, N)$
   $t := t + 1$
7. if $g < N$ then return g
   else return neúspěch

Složitost algoritmu

Krok 2: $O(\log^2(N))$
Krok 4: Počítáme nejvýše $\log(ed-1)$ dělení číslem 2.
$O(\log^2(ed-1))$
Krok 6: Při inteligentnější implementaci spočteme $a := a^\ell \bmod N$
(v čase $O(\log(\ell)\log^2(N))$)
V každé iteraci pak počítáme $g := \mathrm{NSD}(a-1, N)$ $a := a^2 \bmod N$
opět čas $O(\log^2(N))$ a počet iterací $\leq s \leq \log(ed-1)$.
Tedy při rozumně velkém e, d (např. $e, d \leq N$) bude složitost algoritmu $O(\log^3(N))$.

Pravděpodobnost úspěchu

Tvrzení

Výše uvedený algoritmus vrátí vlastního dělitele N s pravděpodobností alespoň $1/2$.

Důkaz: Ukážeme, že alespoň polovina prvků $a \in \mathbb{Z}_N^*$ splňuje

$$o_{\mathbb{Z}_p^*}(a^\ell \bmod p) \neq o_{\mathbb{Z}_q^*}(a^\ell \bmod q)\,.$$

Necht' $X \subseteq \mathbb{Z}_N^*$ je množina těch prvků $\mathbb{Z}_N^*$, které tuto vlastnost nemají. Pravděpodobnost neúspěchu algoritmu pak můžeme shora odhadnout jako

$$|X|/(N-1) \leq \frac{\varphi(N)}{2(N-1)} \leq \frac{1}{2}$$

Pravděpodobnost úspěchu, pokračování důkazu

Připomenutí: $\mathbb{Z}_p^* \simeq (\mathbb{Z}_{p-1}, +)$ $\mathbb{Z}_q^* \simeq (\mathbb{Z}_{q-1}, +)$.
Necht' $p-1 = 2^{s_1}\ell_1$, $q-1 = 2^{s_2}\ell_2$, ℓ_1, ℓ_2 lichá. Protože $(p-1)(q-1) = \varphi(N) \mid ed-1 = 2^s\ell$, platí $\ell_1, \ell_2 \mid \ell$.

$$\mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^* \simeq (\mathbb{Z}_{2^{s_1}} \times \mathbb{Z}_{\ell_1}) \times (\mathbb{Z}_{2^{s_2}} \times \mathbb{Z}_{\ell_2})$$

$$a \mapsto (a_p, a_q) \mapsto ((\alpha_1, \beta_1), (\alpha_2, \beta_2))$$

$$a^\ell \mapsto (a_p^\ell, a_q^\ell) \mapsto ((\ell\alpha_1 \bmod 2^{s_1}, 0), (\ell\alpha_2 \bmod 2^{s_2}, 0))$$

Protože ℓ je liché, platí $o_{\mathbb{Z}_{2^{s_1}}}(\alpha_1) = o_{\mathbb{Z}_{2^{s_1}}}(\ell\alpha_1 \bmod 2^{s_1})$,
$o_{\mathbb{Z}_{2^{s_2}}}(\alpha_2) = o_{\mathbb{Z}_{2^{s_2}}}(\ell\alpha_2 \bmod 2^{s_2})$.
Tedy $o_{\mathbb{Z}_p^*}(a_p^\ell) = o_{\mathbb{Z}_q^*}(a_q^\ell)$ právě když $o_{\mathbb{Z}_{2^{s_1}}}(\alpha_1) = o_{\mathbb{Z}_{2^{s_2}}}(\alpha_2)$.

Pravděpodobnost úspěchu, dokončení důkazu

Máme $X = \{a \in \mathbb{Z}_N^* \mid o_{\mathbb{Z}_p^*}(a^\ell \bmod p) = o_{\mathbb{Z}_q^*}(a^\ell \bmod q)\}$.
Chceme ukázat $|X| \leq \frac{1}{2}|\mathbb{Z}_N^*|$. Najdeme prosté zobrazení z X do $\mathbb{Z}_N^* \setminus X$.
Pokud prvek a odpovídá prvku $((\alpha_1, \beta_1), (\alpha_2, \beta_2))$, přiřadíme mu prvek odpovídající prvku $((\alpha_1, \beta_1), (\alpha_2 + 1 \bmod 2^{s_2}, \beta_2))$.
Pokud $a \in X$, je $o_{\mathbb{Z}_{2^{s_1}}}(\alpha_1) = o_{\mathbb{Z}_{2^{s_2}}}(\alpha_2)$ a zřejmě prvky α_2 a $(\alpha_2 + 1) \bmod 2^{s_2}$ mají v grupě $\mathbb{Z}_{2^{s_2}}$ různé řády.

Konec první přednášky

Informace k přednášce
`http://artax.karlin.mff.cuni.cz/~ppri7485/algoritmy/`