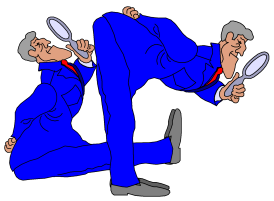
8. Asymetrické šifrovací systémy neboli systémy s veřejným klíčem - Systém s veřejným klíčem se složitostí stejnou jako faktorizace

Jan Paseka

Ústav matematiky a statistiky
Masarykova univerzita

23. listopadu 2023

O čem to bude



Úvod

Uveďme příklad systému s veřejným klíčem, o kterém lze ukázat, že jeho složitost je ekvivalentní s problémem faktorizace.

Tvůrcem systému je **Rabin** (1979).

Každý uživatel systému vybere dvojici (p, q) velkých různých prvočísel, které uchová v tajnosti. Zároveň si vybere přirozené číslo $B < N = p \cdot q$.

Veřejný klíč bude dvojice (B, N), ***soukromý klíč*** bude faktorizace (p, q) čísla N.

Šifrovací funkce e zprávy M, kde M je reprezentovatelná jako přirozené číslo v definičním oboru $\{1, \ldots, N-1\}$ (v případě potřeby se zpráva rozparceluje na více bloků), je

$$e(M) = M \cdot (M + B) \pmod{N}. \tag{1.1}$$

Faktorizace Napadání RSA Algebraické vlastnosti Kongruenční rovnice Kvadráty
Grupa G_m

Úvod

Je-li C výsledný kryptogram, pak dešifrovací problém je nalézt M tak, že

$$M^2 + B \cdot M = C \pmod{N}. \tag{1.2}$$

Kongruenční rovnice a mocninné zbytky I

Poznamenejme nejprve, že platí následující tvrzení

Věta 1.1

Kongruenční rovnice

$$ax = b \,(mod\, m). \tag{1.3}$$

je řešitelná právě tehdy, když $(a, m)|b$.

V tomto případě má rovnice právě (a, m) *navzájem nekongruentních řešení modulo m.*

Důkaz. Výše uvedená podmínka je nutná, neboť v opačném případě nemůže platit rovnost $ax = b + km$ v oboru celých čísel. Buď tedy $d = (a, m)$ a nechť $d|b$.

Kongruenční rovnice a mocninné zbytky II

1. Nechť $d = 1$. Dle Bezoutovy věty existují celá čísla u, v taková, že $au + mv = 1$. Existují tedy celá čísla x, y splňující $ax + my = b$, tj. platí $ax = b \pmod m$. Řešení x je jednoznačně určeno modulo m, neboť je-li x' jiné řešení splňující $ax' = b \pmod m$, máme $a(x - x') = 0 \pmod m$ a tedy $x = x' \pmod m$.
2. Nechť $d > 1$. Protože nutně $d|b$, máme po dosazení do vztahu $ax = b + km$ za $a = a'd$, $b = b'd$, $m = m'd$ a po vydělení číslem d kongruenční rovnici

   $$a'x = b' \pmod{m'}.$$

   Z případu 1 víme, že tato kongruenční rovnice má jediné řešení $x = x_0 \pmod{m'}$. Všechna řešení modulo m tvoří právě d následujících čísel

   $$x = x_0, x_0 + m', \ldots, x_0 + (d-1)m', \pmod m.$$

Kongruenční rovnice a mocninné zbytky III

Budeme chtít vyřešit resp. zjistit, zda následující kongruenční rovnice má řešení v celých číslech pro $n \geq 2$:

$$ax^n = b \pmod{m}. \tag{1.4}$$

Podobně jako v případě lineárních kongruečních rovnic se lze omezit na případ, kdy $(a, m) = 1$. Použitím Eulerovy věty pak obdržíme rovnici $x^n = ba^{\varphi(m)-1} \pmod{m}$.

Buďte tedy m, n přirozená čísla taková, že $m \geq 2$, $n \geq 2$, a celé číslo takové, že $(a, m) = 1$.

Číslo a se nazývá ***n*-tý mocninný zbytek*** modulo m, je-li řešitelná kongruence

$$x^n = a \pmod{m}. \tag{1.5}$$

Kongruenční rovnice a mocninné zbytky IV

Pro zkoumání takovýchto kongruenčních rovnic využijeme následujících tvrzení.

Věta 1.2

Buďte čísla $m_1, m_2, \ldots, m_r$ navzájem nesoudělná, $a_1, a_2, \ldots, a_r$ a $b_1, b_2, \ldots, b_r$ libovolná celá čísla taková, že $(a_1, m_1) = (a_2, m_2) = \cdots = (a_r, m_r) = 1$.

Pak má systém

$$a_i x = b_i \pmod{m_i} \tag{1.6}$$

pro $1 \leq i \leq r$ právě jedno řešení modulo $m = m_1 \cdot m_2, \cdot \cdots \cdot m_r$.

Kongruenční rovnice a mocninné zbytky V

Důkaz. Zřejmě mají jednotlivé kongruenční rovnice právě jedno řešení, které získáme z Euklidova algoritmu pro čísla a_i a m_i - $a_i \cdot u_i + m_i \cdot v_i = 1$.

Pronásobíme-li b_i máme $a_i \cdot x_i + m_i \cdot y_i = b_i$, tj.

$$a_i x = b_i \pmod{m_i}.$$

Předpokládejme, že toto řešení je ve tvaru

$$x = c_i \pmod{m_i} \tag{1.7}$$

pro $1 \leq i \leq r$.

Protože máme $(m_i, m_j) = 1$ pro $i \neq j$, máme $(\frac{m}{m_1}, \frac{m}{m_2}, \ldots, \frac{m}{m_r}) = 1$.

Zejména tedy existují čísla $y_1, y_2, \ldots, y_r$ tak, že

$$\frac{m}{m_1} \cdot y_1 + \frac{m}{m_2} \cdot y_2 + \cdots + \frac{m}{m_r} \cdot y_r = 1.$$

Kongruenční rovnice a mocninné zbytky VI

Položme $e_i = \frac{m}{m_i} \cdot y_i$ pro $1 \leq i \leq r$.

Zřejmě platí

$$e_1 + e_2 + \cdots + e_r = 1 \pmod{m}, \tag{1.8}$$

$$e_i \cdot e_j = 0 \pmod{m} \text{ pro } i \neq j, \tag{1.9}$$

$$e_i \cdot e_i = e_i \pmod{m}, \tag{1.10}$$

$$e_j = \begin{cases} 0 \pmod{m_i} & \text{pro } i \neq j, \\ 1 \pmod{m_i} & \text{pro } i = j. \end{cases} \tag{1.11}$$

Totiž $e_i \cdot e_j = m \cdot c$, $e_i \cdot e_i = \sum_i^r e_j \cdot e_i = 1 \cdot e_i = e_i \pmod{m}$, $e_j = m_i \cdot c'$, $(e_i, m_i) = 1$.

Položme

$$x_0 = c_1 e_1 + c_2 e_2 + \cdots + c_r e_r.$$

Kongruenční rovnice a mocninné zbytky VII

Máme pak z 1.11, že

$$x_0 = c_i \pmod{m_i}$$

pro $1 \leq i \leq r$.

Je tedy x_0 společné řešení modulo m. Pro každé jiné řešení x_0' modulo m systému 1.7 máme

$$x_0 = x_0' \pmod{m_i}$$

pro $1 \leq i \leq r$ a tedy také $x_0 = x_0' \pmod{m}$.

Připomeňme, že pro všechna přirozená čísla m tvoří zbytkové třídy $[a]_m$ pro $(a, m) = 1$ multiplikativní abelovskou grupu modulo m.

Přitom počet prvků této grupy je právě $\varphi(m)$. Tuto grupu budeme v dalším označovat jako G_m.

Grupa G_m I

Věnujme se pro chvíli zkoumání její algebraické struktury. Nechť $m = m_1 m_2 \dots m_r$, kde čísla $m_1, m_2, \dots, m_r$ jsou navzájem nesoudělná.

Podle Věty 1.2 má systém kongruencí

$$x = a_i \pmod{m_i}$$

pro $1 \leq i \leq r$ právě jedno řešení a modulo m.

Přitom platí, že $(a, m_i) = (a_i, m_i)$ pro $1 \leq i \leq r$.

Zejména tedy $(a, m_i) = 1$ právě tehdy, když $(a_i, m_i) = 1$. Opět podle věty 1.2 máme jednoznačně určený rozklad na základě rovností 1.8, 1.9, 1.10, 1.11 tvaru

$$[a]_m = [a_1 e_1]_m + \dots + [a_r e_r]_m. \qquad (1.12)$$

Grupa G_m II

Označme jakožto $[a_i^*]_m$ zbytkovou třídu

$$[e_1 + \cdots + e_{i-1} + a_i e_i + e_{i+1} + \cdots + e_r]_m.$$

Pak pro pevné i tvoří množina $G_{m_i}^*$ zbytkových tříd $[a_i^*]_m$ podgrupu grupy G_m.

Z rovnosti 1.12 obdržíme jednoznačně určený rozklad

$$[a]_m = [a_1^*]_m \dots [a_r^*]_m. \tag{1.13}$$

Provedeme-li tento rozklad pro všechna $[a]_m \in G_m$, lze výše uvedené formulovat tak, že grupa G_m je přímý součin podgrup $G_{m_1}^*, \dots, G_{m_r}^*$.

Máme zejména izomorfismus mezi grupami G_{m_i} a $G_{m_i}^*$ pomocí zobrazení $[a_i^*]_m \longleftrightarrow [a_i]_{m_i}$.

Grupa G_m III

Řekneme, že ***a patří modulo m k exponentu d***, pokud

$$(a, m) = 1,\ a^d = 1 \pmod m,$$

$$\text{ale } a^n \neq 1 \pmod n \text{ pro } 1 \leq n < d.$$

To ale není nic jiného, než že a je prvek řádu d v multiplikativní grupě G_m.

Grupa G_m III

Lemma 1.3

Patří-li a modulo m k exponentu d, jsou čísla $1, a, a^2, \ldots, a^{d-1}$ modulo m nekongruentní. Je-li dále $a^t = 1 \pmod m$, pak $d|t$.

Důkaz. Nechť $a^k = a^h \pmod m$, $0 \leq h < k < d$. Protože $(a, m) = 1$, je $a^{k-h} = 1 \pmod m$.

To je však spor s $0 < k - h < d$ a minimalitou d.

Položíme-li $t = dq + r$, $0 \leq r < d$, máme

$$1 = a^t = a^{dq+r} = a^r \pmod m,$$

tj. musí platit $r = 0$.

Grupa G_m IV

Lemma 1.4

Patří-li a modulo m k exponentu d a n je přirozené číslo s $(n, d) = 1$, patří a^n rovněž modulo m k exponentu d.

Důkaz. Nechť a^n patří k exponentu t. Pak z 1.3 a $(a^n)^t = 1 \pmod m$, obdržíme $d|nt$. Protože $(n, d) = 1$, je nutně $d|t$ a tedy i $d \leq t$. Protože $(a^n)^d = (a^d)^n = 1 \pmod m$, je nutně i $t \leq d$. Celkem $t = d$. ∎

Poznamenejme, že číslo g, které modulo m patří k exponentu $\varphi(m)$, se nazývá ***primitivní kořen*** modulo m.

Lze dokázat, že pro každé prvočíslo p vždy existuje primitivní kořen g modulo p, tedy každé číslo od 1 do $p - 1$ lze vyjádřit jakožto mocninu g.

Grupa G_m V

Speciálně lze ověřit, že pokud $t|\varphi(p)$, má kongruenční rovnice

$$x^t = 1 \pmod{p}, \tag{1.14}$$

právě t navzájem nekongruentních řešení.

Tvrzení 1.5

K modulu m existuje buď žádný nebo $\varphi(\varphi(m))$ modulo m nekongruentních primitivních kořenů.

Grupa G_m VI - Důkaz Věty 1.5

Důkaz. Nechť g je primitivní kořen modulo m.

Podle Lemmatu 1.4 je rovněž g^n primitivní kořen modulo m v případě, že platí $(n, \varphi(m)) = 1$.

Takovýchto čísel $n \leq \varphi(m)$ je právě $\varphi(\varphi(m))$.

Máme tedy v každém případě alespoň $\varphi(\varphi(m))$ primitivních kořenů.

To, že nelze nalézt žádné další primitivní kořeny, plyne z Lemmatu 1.3. Totiž, probíhá-li ν čísla mezi 0 a $\varphi(m) - 1$, probíhá pak g^ν grupu G_m. Zvolíme-li ν tak, že $(\nu, \varphi(m)) = t > 1$, pak platí $1 < \frac{\varphi(m)}{t} < \varphi(m)$

$$(g^\nu)^{\frac{\varphi(m)}{t}} = (g^{\varphi(m)})^{\frac{\nu}{t}} = 1 \pmod{m}.$$

Pak ale nemůže být g^ν primitivní kořen modulo m. ∎

Grupa G_m VII

Tvrzení 1.6

Buď p prvočíslo. Pak G_p je cyklická. Zejména tedy existuje primitivní kořen modulo p.

Důkaz. Pro $p = 2$ je tvrzení věty triviální.

Nechť p je v dalším liché prvočíslo.

Pro $d|(p-1)$ označme $\chi(d)$ počet zbytkových tříd z G_p, které patří k exponentu d modulo p.

Máme ukázat, že $\chi(p-1) > 0$. Podle Tvrzení 1.5 je pak dokonce $\varphi(p-1) = \chi(p-1)$.

Nechť tedy existuje nějaké číslo a, které patří k exponentu d.

Pak dle lemmatu 1.3 jsou čísla tvaru $1, a, a^2, \ldots, a^{d-1}$ navzájem nekongruentní řešení rovnice $x^d - 1 = 0 \pmod p$.

Grupa G_m VIII - Pokračování důkazu Tvrzení 1.6

Toto lze přepsát pomocí polynomiální kongruence následovně

$$x^d - 1 = (x-1)(x-a)\cdots(x-a^{d-1}) \pmod p.$$

Zároveň jsou výše uvedená čísla také všechna řešení této kongruence. Podle Lemmatu 1.4 pak i a^k patří k exponentu d, pokud $(d,k) = 1$. To znamená, že mezi řešení přináleží $\varphi(d)$ čísel, která patří k exponentu d. Nutně pak buď $\chi(d) = 0$ nebo $\chi(d) = \varphi(d)$.
Provedeme-li výčet všech prvků z G_p podle toho, ke kterému exponentu patří, je

$$\sum_{d|(p-1)} \chi(d) = p - 1.$$

Grupa G_m IX - Pokračování důkazu Tvrzení 1.6

Je ale dobře známo, že pro Eulerovu funkci φ platí

$$\sum_{d|(p-1)} \varphi(d) = p - 1.$$

Nutně pak $\chi(d) = \varphi(d)$. ■

FI Buď g primitivní kořen modulo m, $(a, m) = 1$ a μ buď jednoznačně určené číslo mezi 0 a $\varphi(m) - 1$ z kongruenční rovnice

$$g^{\mu} = a \pmod{m}.$$

Pak říkáme, že μ je ***index (diskrétní logaritmus)*** čísla a vzhledem k bázi g.
Píšeme pak $\mu = \log_g a \bmod \varphi(m)$. Přitom platí pravidla pro logaritmování součinu, mocniny atd.

Grupa G_m X

Tvrzení 1.7

Pro diskrétní logaritmování platí následující zákony:

1. $\log_g ab = \log_g a + \log_g b \pmod{\varphi(m)}$,
2. $\log_g a^n = n \log_g a \pmod{\varphi(m)}$,
3. $\log_g 1 = 0 \pmod{\varphi(m)}$,
4. $\log_g g = 1 \pmod{\varphi(m)}$,
5. $\log_g(-1) = \frac{1}{2}\varphi(m) \pmod{\varphi(m)}, m > 2$.

Důkaz. **MA** Z $a = g^{\log_g a} \pmod{m}$ a $b = g^{\log_g b} \pmod{m}$ obdržíme $ab = g^{\log_g a + \log_g b} \pmod{m}$. Porovnáme-li toto s $ab = g^{\log_g ab} \pmod{m}$, obdržíme první vlastnost. Vlastnosti 2 a 3 plynou bezprostředně z vlastnosti 1. Z $g = g^{\log_g g} \pmod{m}$ obdržíme 4.

Grupa G_m XI

Pátá vlastnost je založena na Fermat-Eulerově větě:

$$g^{\varphi(m)} - 1 = \left(g^{\frac{\varphi(m)}{2}} - 1\right)\left(g^{\frac{\varphi(m)}{2}} + 1\right) = 0 (\mathrm{mod}\, m).$$

■

Tvrzení 1.8

Buď p liché prvočíslo tak, že číslo a není dělitelné p. Kongruenční rovnice

$$x^n = a \,(\mathrm{mod}\, p^r)$$

má právě $d = (n, p^{r-1}(p-1))$ nekongruentních řešení, pokud d dělí $\log_g a$. Jinak je tato kongruence neřešitelná.

Důkaz. Tvrzení věty se logaritmováním převede na lineární kongruenční rovnici

$$n \log_g x = \log_g a \,(\mathrm{mod}\, p^{r-1}(p-1)).$$

Grupa G_m XII

Tvrzení 1.9

Buď p liché prvočíslo tak, že číslo a není dělitelné p, $d = (n, p^{r-1}(p-1))$. Kongruenční rovnice

$$x^n = a \,(\mathrm{mod}\, p^r)$$

má právě řešení právě tehdy, když platí kongruenční rovnice

$$a^{\frac{1}{d}p^{r-1}(p-1)} = 1 \,(\mathrm{mod}\, p^r). \qquad (1.15)$$

Důkaz. Buď g primitivní kořen modulo p^r. Podle Věty 1.8 je výše uvedená kongruence řešitelná právě tehdy, když existuje číslo h tak, že $\log_g a = h \cdot d$. Pak platí $a = g^{\log_g a} = g^{h \cdot d} \,(\mathrm{mod}\, p^r)$. Tedy

$$a^{\frac{1}{d}p^{r-1}(p-1)} = g^{h \cdot p^{r-1}(p-1)} = 1 \,(\mathrm{mod}\, p^r).$$

Grupa G_m XIII

Nechť obráceně platí kongruenční rovnice (1.15). Položme $\mu = \log_g a$.

Protože $a = g^\mu \pmod{p^r}$, máme $g^{\frac{\mu}{d} \cdot p^{r-1}(p-1)} = 1 \pmod{p^r}$.

Protože g je primitivní kořen modulo p^r, je $\frac{\mu}{d}$ celé číslo, tj. d dělí μ.

Tedy dle Tvrzení 1.8 je kongruenční rovnice řešitelná.

Grupa G_m XIV

Věta 1.10

Buď $f(x)$ polynom v proměnné x s celočíselnými koeficienty. Pak počet řešení kongruenční rovnice

$$f(x) = 0 \pmod{m}, m = \Pi_{i=1}^{r} p_i^{s_i} \tag{1.16}$$

je číslo $N = n_1 n_2 \cdot \cdots \cdot n_r$, přičemž n_i je počet řešení rovnice

$$f(x) = 0 \pmod{p_i^{s_i}} \tag{1.17}$$

pro $1 \leq i \leq r$.

Důkaz. Řešitelnost kongruenční rovnice (1.16) nastává právě tehdy, když je systém kongruečních rovnic (1.17) řešitelný. V případě řešitelnosti každé jednotlivé kongruenční rovnice označme $x = c_i \pmod{p_i^{s_i}}$ řešení i-té kongrunční rovnice.

Grupa G_m XV - Důkaz Věty 1.10

Obdržíme pak lineární systém kongruencí, který má dle Věty 1.2 jednoznačně určené řešení (mod m).

Probíhají-li c_i všechna nekongruentní řešení (těch je n_i), získáme celkem N řešení (mod m). ■

Důsledek 1.11

Počet řešení kongruenční rovnice

$$x^s = x \ (mod\, m), m = \Pi_{i=1}^{r} p_i^{s_i} \tag{1.18}$$

je číslo $N = n_1 n_2 \cdot \cdots \cdot n_r$, *přičemž* n_i *je počet řešení rovnice*

$$x^s = x \ (\mathrm{mod}\, p_i^{s_i}) \tag{1.19}$$

pro $1 \leq i \leq r$.

Grupa G_m XVI

Tvrzení 1.12

Počet řešení kongruenční rovnice

$$x^s = x \ (mod\, p), \tag{1.20}$$

kde p *je prvočíslo, je roven* $1 + (p-1, s-1)$.

Důkaz. Uvažme dva případy. Nechť x je číslo soudělné s p tj. $x = p \ (\mathrm{mod}\, p)$ - takové x je pouze jedno (p) a je řešením.

Nechť x je nesoudělné s p. Množina všech nesoudělných čísel s p tvoří cyklickou grupu stupně $p-1$ a z předchozího víme, že existuje právě $(p-1, s-1)$ prvků této grupy splňujících (1.20).

■

Grupa G_m XVII

Důsledek 1.13

Počet řešení kongruenční rovnice

$$x^s = x \ (mod\, m), m = \Pi_{i=1}^{r} p_i \tag{1.21}$$

je číslo $N = \Pi_{i=1}^{r}(1 + (p_i - 1, s - 1))$.

Kvadratické kongruence I

Uvažme pro celá čísla a, b, c, m ($m > 1, a \neq 0 \ (\mathrm{mod}\, m)$) kvadratickou kongruenci

$$ax^2 + b \cdot x + c = 0 \ (\mathrm{mod}\, m). \tag{1.22}$$

Vynásobením $4a$ převedeme rovnici na tvar

$$(2ax + b)^2 = b^2 - 4ac \ (\mathrm{mod}\, m). \tag{1.23}$$

To znamená, že jsme schopni plně vyřešit kvadratickou kongruenci (1.22), jestliže umíme vyřešit speciální případ

$$x^2 = a \ (\mathrm{mod}\, m). \tag{1.24}$$

Kvadratické kongruence II

Tím se celá problematika převede na problém ***kvadratických zbytků***.
Z důkazu Věty 1.10 víme, že se lze dále omezit na řešení rovnice

$$x^2 = a \pmod{p^s}, \tag{1.25}$$

kde p je prvočíslo. Zároveň lze předpokládat, že $(a, p) = 1$.
Totiž v případě, že p dělí a máme

1. $x = 0 \pmod{p}$, pokud je $s = 1$,
2. v případě $s > 1$ by muselo být $x = py$ tj.
   $py^2 = a' \pmod{p^{s-1}}, a = pa'$.
   Nutně pak $a' = pa''$ tj. získáme kongruenční rovnici
   $y^2 = a \pmod{p^{s-2}}$.

Kvadratické kongruence III

Uvažme nyní kongruenční rovnici tvaru

$$x^2 = a \pmod{p^s}, (a, p) = 1. \tag{1.26}$$

Snadným ověřením získáme řešení pro $p = 2$.

1. $s = 1$: Existuje právě jedno řešení a to $x = 1$.
2. $s = 2$:
   a. $a = 1 \pmod{4}$: Existují právě dvě řešení.
   b. $a = -1 \pmod{4}$: Neexistuje žádné řešení.
3. $s \geq 3$:
   a. $a = 1 \pmod{8}$: Existují právě čtyři řešení.
   b. $a \neq 1 \pmod{8}$: Neexistuje žádné řešení.

Kvadratické kongruence IV

MA

Theorem 1.14

Je-li p liché prvočíslo, pak má kongruence (1.26) buď žádné nebo právě dvě řešení. Je-li a kvadratický zbytek modulo p, je také kvadratický zbytek modulo p^s a obráceně.

Důkaz. Víme, že $(2, p^{s-1}(p-1) = 2$. Podle Věty 1.8 má pak kongruenční rovnice (1.26) právě dvě řešení, pokud $\log a = 0 \pmod 2$ a žádné řešení, pokud $\log a = 1 \pmod 2$. Musíme ještě ukázat, že $\log a$ je nezávisle na s dělitelné 2 nebo ne. Buď g primitivní kořen modulo p^s pro libovolné $s \geq 1$ a $\mu_s = \log_g a$ vzhledem k modulu p^s. Ze vztahu

$$a = g^{\mu_s} \pmod{p^s}, a = g^{\mu_s} = g^{\mu_1} \pmod p,$$

plyne $\mu_s = \mu_1 \pmod{p-1}$ a proto $\mu_s = \mu_1 \pmod 2$. ■

Kvadratické kongruence V

Stačí se tedy zřejmě omezit na případ, že $s = 1$.

Věta 1.15

Je-li p liché prvočíslo, pak máme právě tolik kvadratických zbytků jako nezbytků. Kvadratické zbytky modulo p jsou určeny $a = 1^2, 2^2, \ldots, \frac{p-1}{2}^2 \ mod\, p.$

Důkaz. Uvedená čísla jsou zřejmě modulo p nekongruentní. Totiž je-li $b^2 = c^2 \pmod p$, kde $1 \leq b, c \leq \frac{p-1}{2}$, máme $(b-c)(b+c) = 0 \pmod p$.

Protože $1 < b + c < p$, máme $b - c = 0 \pmod p$, tj. $b = c$.

Protože dále $(p-k)^2 = k^2 \pmod p$, musí být každý kvadratický zbytek kongruentní s jedním z výše uvedených čísel.
Tímto je tvrzení dokázáno. ■

Kvadratické kongruence VI

Lemma 1.16

Řešení rovnice **FI** $x^2 + B \cdot x = C \pmod{p \cdot q}$ (1.27)
lze obdržet jako kombinaci řešení u, v rovnic

$$x^2 + B \cdot x = C \pmod{p} \tag{1.28}$$

$$x^2 + B \cdot x = C \pmod{q} \tag{1.29}$$

a přirozených čísel a, b splňujících

$$\begin{array}{llll} a = 1 \pmod{p}, & a = 0 \pmod{q}, \\ b = 0 \pmod{p} & b = 1 \pmod{q}, \end{array} \tag{1.30}$$

a pak $x = a \cdot u + b \cdot v$
splňuje (1.27).

Důkaz. **MA** Plyne bezprostředně z předchozích tvrzení.

Kvadratické kongruence VII

Buď p liché prvočíslo, p nedělí číslo a. ***Legendrův symbol*** $\left(\frac{a}{p}\right)$ definujeme jako

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{pokud je } a \text{ kvadratický zbytek modulo } p, \\ -1 & \text{pokud je } a \text{ kvadratický nezbytek modulo } p. \end{cases}$$

Mimo jiné je vhodné vytvořit pravidla pro výpočet Legendrova symbolu. Evidentní jsou následující vlastnosti

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \quad \text{pro } b = a \pmod{p}$$

$$\left(\frac{a^2}{p}\right) = 1$$

Kvadratické kongruence VIII

MA Z Fermat-Eulerovy věty víme, že $a^{p-1} = 1 \pmod p$ a proto platí $a^{\frac{p-1}{2}} = \pm 1 \pmod p$.

Podle Věty 1.9 je podmínka $a^{\frac{p-1}{2}} = 1 \pmod p$ dostatečná a nutná pro řešitelnost kongruenční rovnice $x^2 = a \pmod p, (a, p) = 1$.

FI
Máme tedy tzv. ***Eulerovo kritérium***:

Věta 1.17

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p.$$

Z tohoto kritéria lze odvodit řadu důležitých faktů:**MA**

Kvadratické kongruence IX

Tvrzení 1.18

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Důkaz. Z Eulerova kritéria máme, že

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p.$$

Kvadratické kongruence X

Tvrzení 1.19

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Důkaz. První vztah plyne bezprostředně z Eulerova kritéria. Abychom dokázali druhý vztah, uvažme součin

$$\prod_{k=1}^{\frac{p-1}{2}} (-1)^k k = (\frac{p-1}{2})!(-1)^{\frac{p^2-1}{8}}.$$

Je-li v součinu číslo k liché, zaměníme $(-k)$ modulo p číslem $(p-k)$ o obdržíme rovnost

$$\prod_{k=1}^{\frac{p-1}{2}} (-1)^k k = 2 \cdot 4 \cdot 6 \cdot \cdots \cdot (p-1) = (\frac{p-1}{2})! 2^{\frac{p-1}{2}} \bmod p.$$

Kvadratické kongruence X - Pokračování důkazu Tvrzení 1.19

Protože ale p nedělí $(\frac{p-1}{2})!$, máme po vykrácení a z Eulerova kritéria

$$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}}.$$

Lemma 1.20

Je-li p prvočíslo tvaru $4k-1$ a d kvadratický zbytek modulo p, řešení kongruenční rovnice tvaru

$$y^2 = d \pmod p \tag{1.31}$$

je dáno předpisem

$$y = d^k \pmod p. \tag{1.32}$$

Kvadratické kongruence XI

Důkaz. Z Eulerova kritéria máme, že

$$\left(\frac{d}{p}\right) = 1 = d^{\frac{p-1}{2}} \bmod p.$$

Protože $k = \frac{1}{4}(p+1)$, máme

$$d^{\frac{1}{4}(p+1)} d^{\frac{1}{4}(p+1)} = d^{\frac{1}{2}(p+1)} = d^{\frac{1}{2}(p-1)} d = d \bmod p.$$

■

Kvadratické kongruence XII

Zkombinujeme-li předchozí úvahy, dostaneme následují tvrzení

Tvrzení 1.21

Za předpokladu, že jak p tak q jsou kongruentní s 3 modulo 4, lze dešifrovací proceduru provést v polynomiálním čase.

Důkaz. Příjemci, který zná faktory p a q a ví, že kryptogram je kvadratický zbytek, stačí jenom aplikovat předchozí lemmata. ■

Kvadratické kongruence XIII

FI Rabin ve skutečnosti dokázal víc než Tvrzení 1.21.

Totiž dokázal, že i v případě, že prvočísla p a q nejsou v tomto speciálním tvaru, kongruenční rovnice modulo p a modulo q lze řešit náhodným algoritmem v polynomiálním čase.

Poznamenejme, že praktickou nevýhodou Rabinova schématu je, že příjemce obdrží čtyři možné zprávy, z nichž má vybrat tu správnou. Obvykle to lze provést tím, že má nějakou dodatečnou informaci - např. že po převedení z binárního do textového tvaru je zpráva psaná v angličtině.

Mr. X však nezná faktory p a q čísla N a musí se zabývat mnohonásobně obtížnějším problémem. Že je tomu skutečně tak, plyne z níže uvedené druhé Rabinovy věty.

Kvadratické kongruence XIV

Věta 1.22

Označme D_N množinu všech takových d, $0 \leq d < N$, že existuje řešení kongruenční rovnice

$$y^2 = d \pmod{N}. \tag{1.33}$$

Jestliže pro alespoň $\lceil \frac{|D_N|}{\log N} \rceil$ takovýchto d jsme schopni najít takové y, pak jsme schopni najít faktor N v náhodné polynomiální době.

Kvadratické kongruence XV

Lemma 1.23

Jsou-li $x, y \in \mathbf{Z}_N$ celá čísla modulo N taková, že

$$x^2 = y^2 \pmod N, \qquad x \neq \pm y \pmod N, \tag{1.34}$$

jsou pak $(x + y, N)$ a $(x - y, N)$ dělitelé N.

Zejména pro $N = p \cdot q$, p a q prvočísla je $(x + y, N)$ prvočíselný dělitel N.

Důkaz. $x^2 = y^2 \pmod N$ implikuje $x^2 = y^2 + rN$, kde $r \in \mathbf{Z}$. Tudíž $(x - y)(x + y) = rN$. ∎

Větu 1.22 lze neformálně přepsat do tvaru

Kvadratické kongruence XVI

Věta 1.24

Rozšifrování Rabinova systému s veřejným klíčem je ekvivalentní nalezení efektivního algoritmu pro faktorizaci.

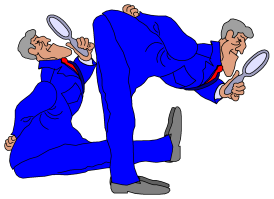
Důkaz. Předpokládejme, že máme algoritmus $\mathcal{A}$, který pro dané (q, N) a pro $\lceil \frac{|D_N|}{\log N} \rceil$ takovýchto q dává na výstupu odmocninu z q modulo N.

Pak můžeme faktorizovat N iterováním následujících kroků: Vyberme náhodně z ze $\mathbf{Z}_N$ tak, že $(z, N) = 1$ a vypočtěme $q = z^2 \pmod N$.

Vložme na vstup algoritmu $\mathcal{A}$ dvojici (q, N). Pokud $\mathcal{A}$ má za výstup druhou odmocninu z q různou od z nebo $-z$ modulo N, pak Lemma 1.23 nám dává, že jsme schopni faktorizovat N.

Očekávaný počet iterací algoritmu bude malý, protože je $\frac{1}{2 \log N}$-ní šance na faktorizaci N v každé iteraci.

O čem to bude



1. Systém s veřejným klíčem se složitostí stejnou jako faktorizace
2. Jak se napadá RSA-algoritmus?
   - Narušení RSA-algoritmu prostřednictvím faktorizace modulu
     - Pollardova rho-metoda
     - Fermatova faktorizace
     - Důsledky nových faktorizačních algoritmů
     - Další možné útoky
     - Speciální přístupy k dešifrování
3. Algebraické vlastnosti a iterovaný útok

Narušení RSA faktorizací modulu $N = p \cdot q$ I

Faktorizace modulu N je nepoměrně obtížnější než jeho konstrukce, tj. nalezení prvočísel p a q.

V době vzniku RSA-algoritmu (1978) byla 50-místná prvočísla bezpečná, což dnes už není pravda.

Proto se v současné době pracuje se 100-místnými prvočísly.

Přitom není vyloučené, že bude možno najít algoritmus na faktorizaci, který pracuje v polynomiálmím čase.

Zároveň se nepodařilo dokázat, že by faktorizace šifrovacího modulu byla ekvivalentní s bezpečností RSA-systému. Mohla by se totiž najít metoda, jak tento systém narušit bez faktorizace N.

Zatím jsou však pokusy o narušení bezpečnosti RSA-systému založeny hlavně na faktorizaci. Lze například dokázat, že výpočet dešifrovacího exponentu t je ekvivalentní faktorizaci šifrovacího modulu N.

Narušení RSA faktorizací modulu $N = p \cdot q$ II

Prvním algoritmem, který nás napadne, je tzv. ***pokusné dělení*** (Trial Division) čísly $2, 3, \ldots, \lceil\sqrt{N}\rceil$. Postup lze urychlit tak, že dělíme jen čísly 2, 3 a pak čísly tvaru $6k - 1, 6k + 1$ pro $k = 1, 2, \ldots$.

Další používanou metodou je ***Pollardova*** $p - 1$ *a* $p + 1$ metoda. Základem metody je následující tvrzení:

Theorem 2.1

Buď $n = p \cdot q$, p, q, r prvočísla, $r - 1 | b$, $r | n$ a n nedělí a. Pak $r | (n, a^b - 1)$.

Důkaz. Podle Fermatovy věty platí $a^{r-1} = 1 \bmod r$ a tedy i $a^b = 1 \bmod r$ tj. $r | (a^b - 1)$. Zároveň však $r | n$. ■

Narušení RSA faktorizací modulu $N = p \cdot q$ III

Aby se výše uvedená věta dala využít, je nutno najít vhodná čísla a, b. Nalezení a je snadné. Stačí zvolit nějaké malé prvočíslo a přesvědčit, zda je či není dělitelem n - pokud by bylo dělitelem, našli bychom faktorizaci čísla n a tím byli hotovi.

Volba b je obtížnější, je třeba ho najít postupným zkoušením. Přitom se obvykle za b volí čísla tvaru

$$b_j = nsn(1, 2, \ldots, j).$$

Tato čísla je vhodné volit z toho důvodu, že mají mnoho vlastních dělitelů a je tedy velká šance na splnění podmínky $r - 1 | b$.

Algoritmus se hodí na nalezení menších prvočíselných dělitelů čísla n. Touto metodou bylo např. faktorizované číslo $2^{257} - 1$ jako součin tří různých prvočísel.

Pollardova rho-metoda I

Další známou metodou je ***Pollardova rho-metoda*** (Monte Carlo), kterou se obvykle najdou malé prvočíselné dělitele modulu N asi po $\sqrt{p}$ cyklech programu.

Metoda začíná výběrem libovolné ***nelineární funkce*** f ***s celočíselnými koeficienty***, nejčastěji $f(x) = x^2 + c$, $c \neq 0, -2$ a volbou počáteční hodnoty x_0, kterou lze zvolit náhodně. V dalších krocích se rekurentně počítají hodnoty posloupnosti $x_{j+1} = f(x_j) \bmod N$, $j = 0, 1, 2, \ldots$.

Pomocí pravděpodobnostních úvah lze dokázat, že výsledná posloupnost bude ***skoroperiodická***. To znamená, že po jisté době lze očekávat výskyt dvou hodnot x_j, x_k, pro které platí

$$x_j \neq x_k \bmod N, \qquad N = p \cdot q$$

$$x_j = x_k \bmod p.$$

Pollardova rho-metoda II

To ale znamená, že $(x_j - x_k, N) = p$. Hledání největšího společného dělitele lze však provést Euklidovým algoritmem s malou složitostí.

Algoritmus se ještě trochu upraví: kdyby se tímto způsobem porovnávaly všechny rozdíly $x_k - x_j$ pro všechna $j < k$, počet operací by neúměrně narůstal. Proto postupujeme následovně:

Předpokládejme, že máme už spočítané x_k, přičemž k je $h+1$-bitové číslo, $2^h \leq k < 2^{h+1}$. Označme $j = 2^h - 1$. Pak najdeme $(x_k - x_j, N)$. Pokud prvočíslo p nenalezneme, postup zopakujeme pro $k + 1$. Nevýhodou takovéhoto postupu je, že pravděpodobně nenajdeme "první dvojici" x_k, x_j.

Fermatova faktorizace aj. I

Věnujme se pro okamžik tzv. ***Fermatově faktorizaci***, která je založena na Tvrzení 1.23 tj., že $x - y$ je pravděpodobně netriviální dělitel čísla N.

Je-li navíc $N = p \cdot q$, je pak i

$$N = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2. \qquad (2.1)$$

Protože p a q jsou různá prvočísla, nemusíme se bát toho, že by N bylo úplným čtvercem nějakého prvočísla. Pokud jsou prvočísla p a q blízko, resp. rozdíl $|p - q|$ je malý, je číslo $\frac{p+q}{2}$ jen o málo větší než $\sqrt{N}$.

Pak ale stačí pro $x = 1 + \lceil\sqrt{N}\rceil, 2 + \lceil\sqrt{N}\rceil, \ldots$ počítat $x^2 - N = u$. Je-li $u = y^2$ úplný čtverec, bude $p = x - y$ hledané prvočíslo.

Fermatova faktorizace aj. II

Další z možných metod je metoda tzv. ***řetězových zlomků***. Na základě této metody lze navrhnout procesor v ceně asi 1000000 $, který rozloží 100-místné dekadické číslo asi za 1 měsíc. Pro 200-místné dekadické číslo je ale odhad 3.8 miliónů let, což garantuje postačující bezpečnost celého systému.

Připomeňme si, že tvůrci RSA vsadili 100 USD na to, že nikdo nerozluští jejich anglický text zašifrovaný algoritmem RSA s veřejným modulem $e = 9007$ a známým modulem N, který je součinem dvou 64- a 65-ciferných prvočísel.

Rivest v roce 1977 spočítal, že na faktorizaci uvedeného modulu N by bylo nejlepší faktorizační metodou potřeba 40 000 000 000 000 000 let. Proto se nebáli "investovat" 100 USD do sázky.

Fermatova faktorizace aj. III

V dubnu 1994 bylo však oznámeno, že se toto 129-ciferné číslo N podařilo rozložit. Zároveň tak byl odhalen otevřený text zašifrované zprávy, která neměla nikdy spatřit světlo světa: "The magic words are squemish ossifrage".

Poznamenejme k výše uvedenému, že v roce 1873 se zdálo nemožné faktorizovat deseticiferné číslo. V roce 1977 byla však už známá Pollardova rho metoda faktorizace. S její výkonností také Rivest počítal při odhadu uvedeného času na faktorizaci našeho čísla N.

Od té doby se však objevily další metody faktorizace: ECM (elliptic curve method), QS (quadratic sieve factoring) a NFS (number field sieve factoring algorithm).

Fermatova faktorizace aj. IV

Pollardova rho metoda na nalezení 64-ciferného součinitele potřebovala odhadem 4×10^{32} modulárního násobení, tj. asi 1.3×10^{16} let – Rivest uvažoval, že by jedno modulární násobení mohlo trvat jednu nanosekundu.

ECM však už dnes potřebuje už jen 5×10^{15} modulárního násobení, tj. asi 2 měsíce.

Ve skutečnosti se takovéto rychlosti modulárního násobení nedosahuje a reálný odhad by byl cca 15 000 let, což je však obrovský pokrok oproti 10^{16} letům.

Na rozdíl od ECM a Pollardovy rho metody metoda QS, použitá k nalezení 64-ciferného součinitele u našeho čísla N, závisí mnohem více na přístupu do paměti než na výkonu procesoru.

Frematova faktorizace aj. V

Na základě analýzy reálně použitých typů počítačů a jimi spotřebovaného času na faktorizaci bylo spočítáno, že k nalezení 64-ciferného součinitele se spotřebovalo celkem 4000 až 6000 tzv. MIPS roků.

Přitom jeden MIPS rok je množství operací, které za jeden rok vykoná počítač s výkonem jeden milion operací za vteřinu. Je to tedy $365,25 \times 24 \times 3600 \times 1000000$ =cca. $3.16 \cdot 10^{13}$ operací.

Počítáme-li průměrný výkon jednoho počítače v experimentu 10 MIPS s tím, že na experimentu pracoval jen polovinu dne tj. s reálným výkonem pouze 5 MIPS, bylo k faktorizaci použito cca. 1000 let práce.

Zároveň je z výše uvedeného vidět úžasný nárůst výkonnosti faktorizačních metod v posledních letech.

Frematova faktorizace aj. VI

Faktorizaci 154-místného čísla (512 bitů) pak bude trvat cca 500000 MIPS let.

Tento výkon by mohli zajistit všichni účastníci sítě INTERNET. Dostáváme pak výpočetní kapacitu 20 miliónů MIPS - tj. faktorizace by proběhla během devíti dní.

Důsledky nových faktorizačních algoritmů I

Nejspolehlivější cesta, jak narušit veřejnou síť využívající RSA-kryptosystém, je nalezení dešifrovacího exponentu, označme si ho třeba t.

Jednou z takovýchto možností je poznání čísel $p-1$ a $q-1$, tj. faktorizace šifrového modulu $N = pq$. Slabým místem Pollardovy $p-1$ a $p+1$ metody je nalezení vhodného čísla b.

Abychom úlohu faktorizace čísla N pro nekompetentní osobu zkomplikovali, musíme zvolit prvočísla p a q tak, aby $p-1$ ($q-1$) mělo velký prvočíselného dělitel r a $p+1$ ($q+1$) velký prvočíselný dělitel d.

Zároveň je vhodné požadovat, aby číslo $r-1$ mělo rovněž velký prvočíselný dělitel e.

Důsledky nových faktorizačních algoritmů II

Proto prvočísla splňující kongruenční rovnice

$$\begin{aligned} p &= 1 \bmod r \\ p &= d-1 \bmod d \\ r &= 1 \bmod e. \end{aligned} \tag{2.2}$$

(kde r, d a e jsou velká náhodná prvočísla) se nazývají ***silná prvočísla***.

Abychom se zabezpečili i proti metodám založeným na Fermatově faktorizaci, musíme zvolit silná náhodná prvočísla p a q tak, aby rozdíl $|p-q|$ byl několik řádů.

Pokud budeme mít efektivní metodu na nalezení silných náhodných prvočísel, pak splnění poslední podmínky nám nezpůsobí žádné komplikace. Takováto metoda byla poprvé navržená Gordonem v roce 1985.

Další možné útoky na RSA-šifrovací systém I

Ukážeme, že dva účastníci RSA-šifrovacího systému nemohou mít stejný šifrovací modul N. Uvažujme účastníky A a B, $N_A = N_B = N$. Pak musí platit

$$(s_A, \varphi(N)) = 1 \quad \text{a} \quad s_B \cdot t_B - 1 = k \cdot \varphi(N) \tag{2.3}$$

pro nějaké celé číslo k.

Uvidíme, že účastník B je schopen díky společnému N číst každou zprávu určenou účastníkovi A a také podpisovat účastníka A.

Totiž účastník B je schopen použitím Euklidova algoritmu vypočíst $f = (s_B \cdot t_B - 1, s_A)$. Označme

$$n = \frac{s_B \cdot t_B - 1}{f}. \tag{2.4}$$

Další možné útoky na RSA-šifrovací systém II

Pak $(n, s_A) = 1$ a $(f, \varphi(N)) = 1$, protože šifrovací exponent s_A je nesoudělný s N. Odtud pak

$$n = \frac{k}{f}\varphi(N) \tag{2.5}$$

a přitom číslo f dělí číslo k.

Proto je n násobek $\varphi(N)$. Z nesoudělnosti čísel n a s_A plyne existence čísel u, v tak, že

$$u \cdot n + v \cdot s_A = 1. \tag{2.6}$$

Další možné útoky na RSA-šifrovací systém III

Bez újmy na obecnosti lze předpokládat, že $v > 0$. Pak

$$v \cdot s_A = 1 - u \cdot n = 1 \bmod \varphi(N) \tag{2.7}$$

a

$$t_A \cdot s_A = 1 \bmod \varphi(N). \tag{2.8}$$

Zejména tedy

$$(v - t_A) \cdot s_A = 0 \bmod \varphi(N). \tag{2.9}$$

a

$$v = t_A \bmod \varphi(N). \tag{2.10}$$

Další možné útoky na RSA-šifrovací systém IV

Takovéto v je dešifrovacím exponentem zpráv, které jsou zasílány účastníkovi A. Totiž, je-li

$$y = x^{s_A} \bmod (N), \tag{2.11}$$

zpráva určená pro A, pak platí

$$y^v = x^{s_A \cdot v} = x^{s_A \cdot v + s_A \cdot l \cdot \varphi(N)} = x \bmod (N), \tag{2.12}$$

pro vhodné $l \in \mathbf{Z}$.

Pokud chce B odeslat zprávu jinému účastníkovi C, stačí podepsat zprávu místo dešifrovacím exponentem účastníka A exponentem v.

Další možné útoky na RSA-šifrovací systém V

Jinou z možných příčin narušení RSA-šifrovacího systému by mohla být skutečnost, že tatáž zpráva je odeslána více účastníkům šifrovacího systému tak, že je zašifrovaná různými šiframi tohoto systému. RSA-algoritmus nemůže používat stejné šifrovací exponenty.

Z důvodu jednoduchosti uvažujme tři účastníky šifrovacího systému, kteří mají šifrovací klíče (s, N_i), $i = 1, 2, 3$. Můžeme bez újmy na obecnosti předpokládat, že moduly jsou navzájem nesoudělné. Pokud by tomu tak nebylo, našli bychom faktorizaci a tím byli hotovi.

Zašleme-li těmto třem účastníkům stejnou zprávu x, $x < \min N_i$, pak $\mathrm{Mr.\ X}$, který zachytí její zašifrované varianty y_i, $i = 1, 2, 3$, může zprávu x lehce dešifrovat.

Faktorizace Napadání RSA Algebraické vlastnosti Faktorizace Pollard Fermat Důsledky Další možné útoky Speciální přístupy

Další možné útoky na RSA-šifrovací systém VI

Postup $\mathrm{Mr.\ X}$ bude následovný. Z kongruenčních rovnic

$$y_1 = x^s \bmod N_1 \tag{2.13}$$
$$y_2 = x^s \bmod N_2 \tag{2.14}$$
$$y_3 = x^s \bmod N_3 \tag{2.15}$$

dostaneme pro $N = N_1 N_2 N_3$

$$y_1 N_2 N_3 = x^s N_2 N_3 \bmod N \tag{2.16}$$
$$y_2 N_1 N_3 = x^s N_1 N_3 \bmod N \tag{2.17}$$
$$y_3 N_1 N_2 = x^s N_1 N_2 \bmod N. \tag{2.18}$$

Po jejich sečtení obdržíme

$$y_1 N_2 N_3 + y_2 N_1 N_3 + y_3 N_1 N_2 = x^s \cdot (N_2 N_3 + N_1 N_3 + N_1 N_2) \bmod N. \tag{2.19}$$

Další možné útoky na RSA-šifrovací systém VII

Je-li $s = 3$, pak $x^s < N$ a Mr. X může z poslední kongruence přímo vypočítat zprávu x - vynásobením prvkem inverzním k prvku $(N_2N_3 + N_1N_3 + N_1N_2)$ a standardním odmocněním. Výsledek lze zobecnit na d účastníků šifrovacího systému.

Faktorizace Napadání RSA Algebraické vlastnosti
Faktorizace Důsledky
Pollard Další možné útoky
Fermat Speciální přístupy

Speciální přístupy k dešifrování RSA I

Můžeme-li počítat s jistou neopatrností účastníka sítě, zašle Mr. X účastníkovi A zprávu $x^s \cdot a^s$, kde x^s je zašifrovaná zpráva, kterou Mr. X zachytil a pozměnil ji pronásobením číslem a^s.

Veřejný šifrovací klíč je dvojice (s, N). Tedy účastník A obdrží zprávu

$$y' = a^s \cdot x^s \bmod N \qquad (2.20)$$

a po dešifrování $x' = (y')^t = xa \bmod N$.

Pokud bude A neopatrný a umožní přístup k číslu x', pak můžeme jednoduše spočítat

$$x = a^{-1} \cdot x' \bmod N. \qquad (2.21)$$

Speciální přístupy k dešifrování RSA II

Další možný přístup souvisí s ***protokolem*** při vytváření spojení mezi účastníky, kdy se A i B navzájem identifikují.

Pokud chce účastník B navázat spojení s účastníkem A, zvolí libovolnou zprávu x a vyšle pomocí dešifrovacího exponentu t_B šifru $y = x^{t_B} \bmod N_B$.

Účastník A zná šifrovací exponent účastníka B a proto si může zkontrolovat $y^{s_B} = x^{t_B \cdot s_B} = x \bmod N_B$.

Nyní použije účastník A svůj dešifrovací exponent t_A a výše uvedený postup zopakuje. Zřejmě je $x < \min\{N_A, N_B\}$.

Jak bude probíhat vlastní útok?

Faktorizace Napadání RSA Algebraické vlastnosti
Faktorizace Pollard Fermat
Důsledky Další možné útoky Speciální přístupy

Speciální přístupy k dešifrování RSA III

Pokud účastník B získá dva takovéto podpisy od účastníka A

$$y_1 = x_1^{t_A} \bmod N_A, \tag{2.22}$$

$$y_2 = x_2^{t_A} \bmod N_A, \tag{2.23}$$

je pak schopný vytvořit třetí hodnověrný podpis účastníka A bez znalosti jeho dešifrovacího exponentu t_A

$$y = (x_1 x_2)^{t_A} \bmod N_A, \tag{2.24}$$

a ten zneužít při podpisu nějaké zprávy (B zná jak x_1 tak x_2). Proto je vhodné doplnit při podpisování zprávu x nějakou aktuální redundantní a nepředvídanou informací.

Speciální přístupy k dešifrování RSA IV

Třetí z možných přístupů je následující.

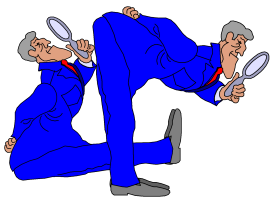
Nechť šifrovací modul $N = p \cdot q$ má n-bitovou reprezentaci a prvočísla p a q mají $\frac{n}{2}$-bitovou reprezentaci.

Předpokládejme, že $\mathrm{Mr.\ X}$ má možnost získat nějakým způsobem $\frac{n}{2}$-bitovou informaci o modulu N. Potom ho samozřejmě může faktorizovat - přímo se zeptá na jedno z prvočísel p a q.

Dá se ukázat, že šifrovací modul N je možno faktorizovat polynomiálním algoritmem, pokud má $\mathrm{Mr.\ X}$ možnost získat jen $\frac{n}{3}$ bitů.

Na poslední z přístupů k rozšifrování RSA-šifry poukázali jako první G.J. Simmons a M.J. Norris. Tento přístup využívá algebraické vlastnosti RSA-kryptosystému.

O čem to bude



Algebraický popis RSA I

Uvažujme množinu zpráv rozšířenou o nulový prvek, tj. $M = \{0, 1, 2, \ldots, N-1\}$.

Pro každé s, $(s, \phi(N)) = 1$ je zobrazení

$$T(s, x) = x^s \bmod N \tag{3.1}$$

permutací množiny M, která nechává nulový prvek na místě.

Permutace $T(s, -)$ tvoří konečnou komutativní grupu s neutrálním prvkem $T(1, -)$, kterým je identické zobrazení.

Platí $T(s, -) \circ T(t, -) = T(s \cdot t, -) = T(t, -) \circ T(s, -)$ a $T(s, -)^{-1} = T(t, -)$, kde $t \cdot s = 1 \bmod \phi(N)$.

Algebraický popis RSA II

Lze tedy množinu M s násobením považovat za konečnou komutativní pologrupu s nulovým prvkem,

$T(s, -) : M \to M$ je homomorfismus pologrup zachovávající nulový prvek.

Iterovaný útok na RSA I

Ukažme si možnost narušení systému iterovaným šifrováním.

Příklad 3.1

Zvolme $N = 3 \cdot 59 = 177$, $s = 17$. *Pak* $M = \{0, 1, 2, \ldots, 176\}$. *Uvažujme zprávu* $x = 5$. *Postupně iterováním dostaneme*

$$\begin{aligned} T(17,5) &= 5^{17} \; mod \, 177 = 95, \\ T(17, T(17,5)) &= T(17,95) = 95^{17} \; mod \, 177 = 71, \\ T(17, T(17, T(17,5))) &= T(17,71) = 71^{17} \; mod \, 177 = 41, \\ T(17,-)^4(5) &= 41^{17} \; mod \, 177 = 5, \\ T(17,-)^5(5) &= 5^{17} \; mod \, 177 = 95, \end{aligned}$$

Protože jak N tak s známe, takovéto iterované šifrování může provést každý.

Iterovaný útok na RSA II

Z konečnosti množiny M víme, že existuje číslo h tak, že

$$T(s,-)^{h+1} = T(s,-) \qquad (3.2)$$

a tedy pro každé zprávu x platí $T(s,x)^h = x$.

Navíc lze pro konkrétní zprávu najít takové minimální h - tj. délku cyklu, který obsahuje zprávu x.

Tento postup je však prakticky realizovatelný jen v případě, když h bude relativně malé číslo, např. menší než milión.

Je přitom dokázáno, že při vhodném výběru prvočísel p a q je pravděpodobnost nalezení takovéhoto malého h menší než 10^{-90}.

Iterovaný útok na RSA III

Vzhledem k tomu, že počet elementárních částic v námi známém vesmíru je řádově 10^{80}, lze každou pravděpodobnost menší než 10^{-80} považovat za nulovou.

Popišme si nyní pologrupu M. Ta je sjednocením čtyř disjunktních grup a obsahuje přesně čtyři idempotenty - $0, 1, e_1, e_2$. Poslední dva idempotenty dostaneme jako řešení rovnic

$$a_1 \cdot p = 1 \bmod q, \qquad \text{resp.} \qquad a_2 \cdot q = 1 \bmod p, \quad (3.3)$$

kde $a_1 \cdot p = e_1$ a $a_2 \cdot q = e_2$ leží v M, $1 \leq a_1 < q$ a $1 \leq a_2 < p$.

Iterovaný útok na RSA IV

Příslušné grupy jsou tedy

$$G(0) = \{0\}, \; G(1) = \{x : (x, p \cdot q) = 1\},$$
$$G(e_1) = \{x : x = p \cdot a \bmod q, a = 1, 2, \ldots, q-1\},$$
$$G(e_2) = \{x : x = q \cdot b \bmod p, b = 1, 2, \ldots, p-1\}.$$

To znamená, že počet prvků v jednotlivých grupách je $1, (p-1)(q-1), q-1$ a $p-1$.

Nejprve určeme počet těch zpráv $x \in M$, které zůstanou při permutaci $T(s, -) = T_s$ na místě. Ptáme se tedy na počet řešení rovnice

$$T(s, x) = x^s = x \bmod N. \quad (3.4)$$

Iterovaný útok na RSA V

Lze dokázat, že všechna takováto řešení tvoří podpologrupu Z_1 pologrupy M, která obsahuje přesně

$$|Z_1| = [1 + (s-1, p-1)][1 + (s-1, q-1)] \qquad (3.5)$$

prvků.

V případě, že zvolíme parametry s, p, q tak, že

$$s = 2r + 1,\ p = 2p_1 + 1,\ q = 2q_1 + 1, \qquad (3.6)$$

kde p_1, q_1 a r jsou navzájem různá prvočísla, je $|Z_1| = 9$ a to je zřejmě nejmenší možný počet zpráv, které se nezašifrují.

Iterovaný útok na RSA VI

Příklad 3.2

Nechť $p = 5$, $q = 7$. *Potom* $a_1 * 5 = 1 \ mod\, 7$, *tj.* $a_1 = 3$, $e_1 = 15$. *Dále* $a_2 * 7 = 1 \ mod\, 5$, *tj.* $a_2 = 3$, $e_2 = 21$. *Odtud*

$$G(0) = \{0\}, \quad G(1) = \{x \mid 1 \leq x \leq 34, (x, 35) = 1\},$$
$$G(15) = \{5, 10, 15, 20, 25, 30\} \quad ,$$
$$G(21) = \{7, 14, 21, 28\}.$$

Iterovaný útok na RSA VII

Podívejme se nyní, jak to vypadá při iterovaném šifrování. Chceme vědět, kolik různých zašifrovaných zpráv můžeme tímto způsobem přečíst, zopakujeme-li šifrování $h+1$-krát.

Rovnost (3.2) přepíšeme na tvar

$$x^{s^{h+1}} = x^s \bmod N, \text{ resp. } x^{s^h} = x \bmod N. \qquad (3.7)$$

Všechna takováto řešení opět tvoří podpologrupu Z_h pologrupy M, která obsahuje přesně

$$|Z_h| = [1 + (s^h - 1, p - 1)][1 + (s^h - 1, q - 1)] \qquad (3.8)$$

prvků.

Iterovaný útok na RSA VIII

Lemma 3.3

a) $Z_l \cap Z_h = Z_d$, *kde* $d = (l, h)$,

b) *Dělí-li číslo* l *číslo* h, *je* $Z_l \subseteq Z_h$.

Důkaz. a) Nechť $x \in G(f)$, kde $f \neq 0$ je jeden z idempotentů pologrupy M. Rovnice

$$x^{s^l - 1} = f \bmod N \quad \text{a} \quad x^{s^h - 1} = f \bmod N, \qquad (3.9)$$

které získáme vydělením vztahu (3.7) v příslušné grupě $G(f)$, mají společné řešení právě tehdy, když
$(s^l - 1, s^h - 1) = s^d - 1$, kde $d = (l, h)$.
Tvrzení b) je speciálním případem pro $l = (l, h)$.

Iterovaný útok na RSA IX

Lemma 3.4

Označme $Z_h^* = \{x : x = x^{s^h}, x^{s^l} \neq x \text{ pro všechna } l < h\}$, $D_h = \{d : d/h, d \neq h\}$. *Pak*

a) $Z_h^* = Z_h - \bigcup\{Z_d : d/h, d \neq h\}$,

b)
$$\begin{aligned} |Z_h^*| &= |Z_h| - [\sum\{|Z_d| : d \in D_h\} \\ &\quad - \sum\{|Z_{d_1} \cap Z_{d_2}| : d_1, d_2 \in D_h, d_1 \neq d_2\} + \dots \\ &\quad + (-1)^{|D_h|} |\bigcap\{Z_d : d \in D_h\}|] , \end{aligned}$$

c) *Pokud je* $h = p^\alpha$, p *prvočíslo, je* $Z_h^* = Z_h - Z_{\frac{h}{p}}$.

Iterovaný útok na RSA X - Důkaz Lemmatu 3.4

a) Nechť $x \in Z_h^*$, pak $x \notin Z_l$ pro libovolné $l < h$, $(l, h) \neq 1$. Tedy

$$Z_h^* \subseteq Z_h - \bigcup\{Z_l : l < h, (l, h) \neq 1\}, \text{ tj.}$$
$$Z_h^* \subseteq Z_h - \bigcup\{Z_d : d/h, d \neq h\}.$$

Opačná implikace je zřejmá.

Zároveň, protože $Z_h \supseteq \bigcup\{Z_d : d/h, d \neq h\}$, máme

$$|Z_h^*| = |Z_h - \bigcup\{Z_d : d/h, d \neq h\}|.$$

b) Plyne z principu exkluze a inkluze.

c) Plyne z inkluzí

$$Z_1 \subseteq Z_p \subseteq Z_{p^2} \subseteq \cdots \subseteq Z_{p^{\alpha-1}}$$

a z rovnosti $Z_{\frac{h}{p}} = \bigcup\{Z_d : d/h, d \neq h\}$. ■

Iterovaný útok na RSA XI

Příklad 3.5

Pokud zvolíme parametry tak jako v Příkladu 3.1, máme $p = 3$, $q = 59$ *a* $s = 17$. *Pak*

$$
\begin{aligned}
&|Z_1^*| = |Z_1| = [1 + (16, 2)] \cdot [1 + (16, 58)] = 3 \cdot 3 = 9,\\
&|Z_2| = [1 + (17^2 - 1, 2)] \cdot [1 + (288, 58)] = 3 \cdot 3 = 9,\\
&|Z_3| = [1 + (17^3 - 1, 2)] \cdot [1 + (4912, 58)] = 3 \cdot 3 = 9,\\
&|Z_4| = [1 + (17^4 - 1, 2)] \cdot [1 + (83520, 58)] = 3 \cdot 59 = 177,\\
&|Z_2^*| = |Z_2| - |Z_1| = 0, |Z_3^*| = |Z_3| - |Z_1| = 0,\\
&|Z_4^*| = |Z_4| - |Z_{\frac{4}{2}}| = |Z_4| - |Z_2| = 168.
\end{aligned}
$$

Jestliže vypočteme $|Z_1^*| + |Z_2^*| + |Z_3^*| + |Z_4^*| = 9 + 0 + 0 + 168 = 177$ *a* $|M| = 3 \cdot 59 = 177$, *vidíme, že jsme tímto vyčerpali celou množinu zpráv a tedy jsme zprávy dešifrovali.*

Faktorizace Napadání RSA Algebraické vlastnosti Algebraický popis Iterovaný útok

Iterovaný útok na RSA XII

Pologrupu M můžeme tedy napsat jako disjunktní sjednocení množin Z_h^*. Úloha navrhovatele šifrovacího systému je, aby $|Z_h^*| = 0$ pro malá h. Množinu Z_h^* můžeme pomocí zobrazení T_s popsat následovně

$$Z_h^* = \{x : T_s^h(x) = x \text{ a } T_s^l(x) = x \text{ pro } l < h\}.$$

Lze ukázat, že univerzálním dešifrovacím exponentem je $h_0 = \lambda(\lambda(N))$.

Zejména tedy pro každou zprávu $x \in M$ a pro každé $1 \leq s \leq N - 1$, $(s, N) = 1$ platí

$$T_s^{h_0}(x) = x. \tag{3.10}$$

Iterovaný útok na RSA XIII

Přitom λ je tzv. Carmichaelova funkce, která číslu $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdot p_r^{\alpha_r}$ přiřadí číslo

$$\lambda(n) = \begin{cases} 1 & \text{jestliže } n = 1, \\ 2^{\alpha-2} & \text{jestliže } n = 2^{\alpha}, \alpha > 2, \\ \varphi(n) & \text{jestliže } n = 2, 4, p^{\alpha}, \\ & p \text{ – liché prvočíslo,} \\ nsn\{\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_r^{\alpha_r})\} & \text{jinak.} \end{cases}$$

Zároveň lze dokázat, že tento univerzální dešifrovací exponent h_0 nelze nahradit menším číslem.

Iterovaný útok na RSA XIV

Je zřejmé, že permutace T_s tvoří grupu.

Lze dokázat, že počet prvků této grupy je $h_1 = \varphi(\lambda(N))$.

Každá z permutací T_s generuje v této grupě nějakou konečnou cyklickou podgrupu $\{T_s, T_s^2, \ldots\}$.

Její exponent (exponentem grupy G nazýváme takové celé číslo h tak, že $a^h = 1$ pro všechny prvky a grupy G) musí dělit exponent h_0 celé grupy.

Proto nutná podmínka neprázdnosti množiny Z_h^* je, aby h dělilo h_0.

Iterovaný útok na RSA XV

Příklad 3.6

Pokud opět zvolíme parametry tak jako v Příkladu 3.1, máme $p = 3$, $q = 59$ *a* $s = 17$. *Pak*

$$\begin{aligned}\lambda(p \cdot q) &= nsn\{\lambda(3), \lambda(59)\} = nsn\{\varphi(3), \varphi(59)\} \\ &= nsn\{2, 58\} = 58,\end{aligned}$$

$$\begin{aligned}\lambda(58) &= nsn\{\lambda(2), \lambda(29)\} = nsn\{\varphi(2), \varphi(29)\} \\ &= 1 \cdot 28 = 28.\end{aligned}$$

Tedy každé h, *pro které je* Z_h^* *neprázdné, musí být dělitelem čísla 28. Ve skutečnosti je to jen pro* $h = 1$ *a* $h = 4$. *Totiž pologrupa* M *má následující idempotenty: 0, 1, 118 a 60. Je sjednocením čtyř grup* $G(0) = \{0\}$, $G(1) = \{x \mid (x, 177) = 1\}$, $G(118) = \{59, 118\}$ *a* $G(60) = \{3, 6, 9, \ldots, 58 \cdot 3\}$.

Faktorizace Napadání RSA Algebraické vlastnosti Algebraický popis Iterovaný útok

Iterovaný útok na RSA XVI

Nyní se budeme zajímat o výběr vhodných parametrů s, p a q. Po analýze, kterou jsme provedli, lze psát

$$M = \bigcup\{Z_h^* : h \text{ dělí } h_0\}, \quad |M| = \sum\{|Z_h^*| : h \text{ dělí } h_0\}, \tag{3.11}$$

kde některé sčítance $|Z_h^*|$ mohou být nulové.

Naším úkolem je zvolit s a N tak, aby $|Z_h^*| \neq 0$ pro velká h, tj. aby pravděpodobnost úspěchu při pokusu o narušení RSA-algoritmu iterovaným útokem byla co nejmenší.

Iterovaný útok na RSA XVII

Protože víme, že

$$h_0 = \lambda(\lambda(N)) = \lambda(\text{nsn}\{p-1, q-1\}),$$

takovouto nutnou podmínkou je, aby číslo h_0 mělo velké prvočíselné dělitele.

Vezmeme-li do úvahy podmínku (3.6), pak dostaneme

$$h_0 = \lambda(\text{nsn}\{a_1 p_1, b_1 q_1\}) = \lambda(p_1 q_1 \text{nsn}\{a_1, b_1\}), \quad (3.12)$$

kde a_1, b_1 jsou libovolná náhodně zvolená malá čísla, $p-1 = a_1 p_1$, $q-1 = b_1 q_1$. Podle definice Carmichaelovy funkce λ je pak h_0 násobek čísla $\text{nsn}\{p-1, q-1\}$.

Iterovaný útok na RSA XVIII

Aby toto číslo bylo co největší, můžeme zvolit

$$p_1 = a_2 p_2 + 1 \quad \text{a} \quad q_1 = b_2 q_2 + 1,$$

kde a_2, b_2 jsou libovolná náhodně zvolená malá čísla a p_2 a q_2 jsou přibližně 90-ti ciferná prvočísla. Pak bude $h_0 = p_2 \cdot q_2 \cdot a$, pro vhodné celé číslo a.

Dále dokážeme, že toto h_0 je pro většinu transformací T_s nejmenším exponentem v příslušné grupě.

Zabývejme se nyní exponentem zpráv $x \in M$. Zpráva x nebude z grupy $G(1) \subseteq M$ právě tehdy, když bude násobkem prvočísla p nebo q.

Iterovaný útok na RSA XIX

Pravděpodobnost takovéto situace, že $(x, N) = (x, pq) \neq 1$ pro náhodně zvolené x bude

$$\frac{|G(e_1)| + |G(e_2)| + 1}{N} = \frac{p + q - 1}{N} \leq \frac{1}{p} + \frac{1}{q} \leq 10^{-90}, \tag{3.13}$$

což je možno považovat za nulovou pravděpodobnost.

Tento výsledek podtrhuje spolehlivost RSA-systému při vhodné volbě klíče. Tvrdí, že pro odesilatele zprávy nemá praktický význam, aby počítal číslo (x, N), které může být rovné 1, p nebo q.

Iterovaný útok na RSA XX

Předpokládejme tedy, že $(x, N) = 1$ a prvočísla jsou vybraná výše uvedeným způsobem

$$\begin{aligned} p &= a_1 \cdot p_1 + 1, & q &= b_1 \cdot q_1 + 1 \\ p_1 &= a_2 \cdot p_2 + 1, & q_1 &= b_2 \cdot q_2 + 1 \end{aligned} \tag{3.14}$$

kde a_i, b_j jsou libovolná náhodně zvolená malá čísla, p, q, p_1, q_1, p_2, q_2 jsou náhodně zvolená prvočísla, $p_2, q_2 \geq 10^{90}$.

Ukážeme, že pro většinu zpráv x je jejich exponent násobkem čísla $p_1 q_1$.

Iterovaný útok na RSA XXI

Připomeňme si následující známou větu z obecné algebry.

Věta 3.7

(L. Sylow) *Nechť G je abelovská grupa, $|G| = n$. Nechť dále p^α je největší mocnina prvočísla p, která dělí n. Pak grupa G obsahuje jedinou podgrupu, která má přesně p^α prvků. Tato podgrupa se nazývá* **Sylowovská**.

Důsledek 3.8

Nechť G je abelovská grupa a $|G| = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}$ je kanonický rozklad čísla $n = |G|$. Pak G je izomorfní s kartézským součinem všech svých Sylowovských podgrup G_{p_i}.

Aplikujeme-li předchozí důsledek na naši situaci, dostáváme, že pro podgrupu $G(1)$ platí $|G(1)| = t_1^{\alpha_1} \cdot t_2^{\alpha_2} \cdot \cdots \cdot t_k^{\alpha_k} \cdot p_1 \cdot q_1$.

Iterovaný útok na RSA XXII

Je tedy grupa $G(1)$ izomorfní s kartézským součinem grup $G' \times G_{p_1} \times G_{p_2}$, kde $G' = G_{t_1^{\alpha_1}} \times G_{t_2^{\alpha_2}} \times \cdots \times G_{t_k^{\alpha_k}}$.

Počet prvků $x \in G(1)$, jejichž exponent nebude soudělný se součinem $p_1 q_1$ je

$$|G'| \cdot (p_1 + q_1) - |G'|.$$

Proto pravděpodobnost, že náhodně zvolené $x \in G(1)$ nebude mít exponent h, který je násobek $p_1 \cdot q_1$, bude rovna

$$\frac{|G'| \cdot (p_1 + q_1) - |G'|}{|G'| \cdot p_1 \cdot q_1} = \frac{p_1 + q_1 - 1}{p_1 \cdot q_1} \leq 10^{-90}. \quad (3.15)$$

Iterovaný útok na RSA XXII

Naprostá většina prvků pologrupy M má tedy exponent, který je násobkem prvočísel p_1 a q_1, tj. $h = a \cdot p_1 \cdot q_1$.

Aplikujeme-li tedy tento postup na grupu τ různých transformací T_s pro pevně zvolený modul N, víme, že se jedná o komutativní grupu, která má přesně $\varphi(\lambda(N))$ prvků a její exponent je $h_0 = \lambda(\lambda(N))$.

Zvolíme-li parametry p a q v souladu s (3.14), dostaneme

$$\begin{aligned} \varphi(\lambda(N)) &= \varphi(p_1 q_1 \cdot \mathrm{nsn}\{a_1, b_1\}) = \\ &= (p_1 - 1) \cdot (q_1 - 1) \cdot \varphi(\mathrm{nsn}\{a_1, b_1\}) = \\ &= a_2 \cdot b_2 \cdot \varphi(\mathrm{nsn}\{a_1, b_1\}) \cdot p_2 \cdot q_2. \end{aligned}$$

Iterovaný útok na RSA XXIII

Snadno lze spočítat prvky $x \in G(1)$, jejichž exponent není dělitelný součinem $p_2 q_2$.

Pak pravděpodobnost, že při iterovaném šifrování budeme úspěšní, je

$$\frac{a \cdot (p_2 + q_2) - |G'|}{|G'| \cdot p_2 \cdot q_2} = \frac{p_2 + q_2 - 1}{p_2 \cdot q_2} \leq 10^{-90}. \qquad (3.16)$$

Navíc exponent h pro většinu transformací T_s je řádově 10^{180}.

Iterovaný útok na RSA XXIV

Poznámka. Poznamenejme, že existuje ještě další zřejmá možnost, jak úspěšně narušit RSA-algoritmus a to za předpokladu, že známe $\varphi(N)$. Pak je snadné najít tajný dešifrovací klíč t.

Ale jak je snadno vidět, znalost $\varphi(N)$ vede k faktorizaci N. Platí totiž identity

$$p+q = N-\varphi(N)+1,\ (p-q)^2 = (p+q)^2 - 4N,$$
$$q = \tfrac{1}{2}[(p+q)-(p-q)], \quad p = N-\varphi(N)-q+1. \tag{3.17}$$