RSA, stručný popis algoritmu

Princip

Podstatou RSA je vztah, kdy

$$(x^a)^b \,\%m \quad = \quad (x^a \%m)^b \,\%m = x, \tag{1}$$

kde

$$m = p \cdot q,$$

a prvočísla p, q, dostatečně velká, splňují podmínku

$$(ab) \,\%\, (\varphi(p \cdot q)) = 1.$$

kde $\varphi(p \cdot q) = (p-1)(q-1)$ je Eulerova funkce. Pozor, rovnost (1) neplatí obecně, ale pouze pro výše uvedenou volbu p, q, a, b! Operace šifrování je definována takto:

$$y = x^a \%m.$$

Inverzní operace, dešifrování, je definována jako

$$x = y^b \%m.$$

Postup šifrování. Zvolíme prvočísla p, q, která budou dostatečně veliká (alespoň 100 cifer) a spočteme

$$m = pq.$$

a určíme hodnotu Eulerovy funkce

$$\varphi(p \cdot q) = (p-1)(q-1).$$

Zvolíme přirozená čísla a, b, aby platilo

$$(ab) \,\%\, (\varphi(p \cdot q)) = 1. \tag{2}$$

Tento krok je netriviální. Zveřejníme $\langle a, m \rangle$, tvořící veřejný klíč. Soukromý klíč tvoří $\langle b \rangle$, které se nesmí zveřejnit.

Výpočet a, b. Myšlenka nalezení čísel a, b je poměrně zajímavá. Pokud výsledkem (2) má být hodnota 1, jakou výchozí iteraci můžeme zvolit řešení

$$ab = \varphi(p \cdot q) + 1.$$

Pak platí, že $(ab) \,\%\, (\varphi(p \cdot q)) = 1$. Jak taková čísla najít? Předpokládejme a takové, že

$$\varphi(p \cdot q) \% a = 0.$$

Hodnota $a = a + 1$ nebude dělitelem $\varphi(p, q)$, pakliže p, q jsou prvočísla. Mohla by však být dělitelem $\varphi(p, q) + 1$. Známe -li a, můžeme b určit jako

$$b = \frac{\varphi(p \cdot q) + 1}{a}, \qquad (\varphi(p \cdot q) + 1) \,\%a = 0.$$

Takto definované číslo b nemusí existovat (funguje pro $p = 5$, $q = 7$, nefunguje pro $p = 7$ a $q = 11$). Pokud má být splněno $(ab) \,\%\, (\varphi(p \cdot q)) = 1$, bude platit obecnější podmínka

$$ab = k\varphi(p \cdot q) + 1.$$

Hodnotu b určíme ze vztahu

$$b = \frac{(k\varphi(p \cdot q) + 1)}{a}, \qquad (k\varphi(p \cdot q) + 1) \,\%a = 0, \tag{3}$$

pro neznámé k=1,2,... Algoritmus pro nalezení a provádí postupné dělení $\varphi(p \cdot q)$ hodnotami $2, 3, 4...$ Hodnotu a dostaneme jako první číslo, které nedělí φ

$$\begin{aligned} while \quad d > \quad & 1 \\ a \quad = \quad & a + 1; \\ d \quad = \quad & NSD(\varphi(p \cdot q), a). \end{aligned}$$

Následně b určíme tak, aby splňovalo podmínku (3). Tato faktorizace je výpočetně drahá, nelze ji provádět dostatečně rychle pro velké hodnoty prvočísel (odolnost proti dekódování hrubou silou).

Výpočet NSD. Pro výpočet a, b použijeme Eukleidův algoritmus pro nalezení největšího společného dělitele, využívající faktu

$$NSD(a,b) = NSD(a-b,b),$$

který lze přepsat do tvaru,

$$NSD(a,b) = NSD(a-kb,b),$$

kde $a - kb = r_1 = a\%b$. Potom lze vztah upravit tak, že pracujeme pouze se zbytky po dělení

$$NSD(r_1,b) = NSD(r_1, b-lr_1) = NSD(r_1,r_2),$$

kde $r_2 = b\%r_1 = b - lr_1$. V rámci algoritmu opakujeme, dokud $r_2 \neq 0$.

$$\begin{aligned} r_1 &= a\%b, \\ r_2 &= b\%r_1, \\ a &= r_1, \\ b &= r_2. \end{aligned}$$

Algoritmus lze zjednodušit tak, že oba kroky počítáme každý v jiné iteraci cyklu (t.j. ve dvou iteracích následujících), dokud $r \neq 0$.

$$\begin{aligned} r &= a\%b, \\ a &= b, \\ b &= r \end{aligned}$$

Výsledek bude uložen v proměnné a.

Výpočet $y = x^a\%m$**.** Tento výpočet nelze pro velké hodnoty a, m realizovat přímo, snadno dojde k přetečení. Vyjdeme ze vztahů

$$\begin{aligned} (ab)\%m &= ((a\%m)(b\%m))\,\%m. \\ [(ab)(cd)]\,\%m &= [(ab)\%m(cd)\%m]\,\%m = [(a\%m \cdot b\%m)\,\%m \cdot (c\%m \cdot d\%m)\,\%m]\,\%m. \end{aligned}$$

Přepíšeme -li x^a do tvaru

$$x^a = x \cdot x \cdot ... \cdot x \cdot (1 \cdot x) = \prod_{i=1}^{a} x,$$

a položíme -li $r = x\%m$, pak

$$\begin{aligned} (x^a)\,\%m &= \left(x\%m \cdot x^{a-1}\%m\right)\%m, \\ &= \left(x\%m \cdot \left[x \cdot x^{a-2}\right]\%m\right)\%m = \left(x\%m \cdot \left[x\%m \cdot x^{a-2}\%m\right]\%m\right)\%m, \\ &= \left(x\%m \cdot \left[x\%m \cdot \left\{x \cdot x^{a-3}\right\}\%m\right]\%m\right)\%m = \left(x\%m \cdot \left[x\%m \cdot \left\{x\%m \cdot x^{a-3}\%m\right\}\%m\right]\%m\right)\%m, \\ &= \left(x\%m \cdot \left[x\%m \cdot \left\{x\%m \cdot ... \left\langle x \cdot x^0\right\rangle\%m...\right\}\%m\right]\%m\right)\%m, \\ &= (x\%m \cdot [x\%m \cdot \{x\%m \cdot ... \langle x\%m \cdot 1\rangle\%m...\}\%m]\%m)\%m, \\ &= (r \cdot [r \cdot \{r \cdot ... \langle r \cdot 1\rangle\%m...\}\%m]\%m)\%m, \end{aligned}$$

Vztah vyhodnocujeme "od vnitřku". Položíme -li $r = x^0\%m = 1$, lze vztah vyjádřit rekurentně ve tvaru

$$\begin{aligned} r &= r \cdot x\%m, \\ r &= r\%m. \end{aligned}$$

Při útoku na klíč metodou hrubé síly nutno dávat pozor na fakt, že $m = pq$, lze pro malá čísla snadno faktorizovat. Pro dostatečně malá m lze tedy provést zpětný rozklad na součin prvočísel. Tím je šifra prolomena, protože můžeme při znalosti p, q, m, a určit b a zprávu dekódovat. Pro velká prvočísla tato úloha není hrubou silou řešitelná v "historicky krátkém čase" na žádném HW. Útok hrubou silou je primitivní, v praxi se však používají metody sofistikovanější.