

Ülesanded RSA murdmisest

Ülesanne 1. RSA moodul on $n = 1199021$. On teada, et $598963^2 \equiv 1 \pmod{n}$. Tegurda selle teadmise abil moodul n .

Ülesanne 2. Süsteemis on kolm kasutajat: A , B ja C . Kõigil neil on RSA salajased võtmed, kusjuures vastavad avalikud võtmed (st moodulid) on $n_A = 451$, $n_B = 391$ ja $n_C = 145$. Avalik astendaja on kõigil ühine: $e = 3$. Ründajale on teada, et kõigile kolmele kasutajale saadetakse üks ja sama salasõnum $x \in \{0, \dots, 144\}$, kusjuures vastavad krüptogrammid on:

$$\begin{aligned}y_A &= x^3 \pmod{451} = 133 \\y_B &= x^3 \pmod{391} = 213 \\y_C &= x^3 \pmod{145} = 80\end{aligned}$$

Kuidas saab ründaja leida sõnumi x ? Leia x ja põhjenda vastust!

Lahendused

Ülesanne 1. Mooduli $n = 1199021$ proovimise teel tegurdamine on ilmselt liiga töömahukas. Teisendame kongruentsi $598963^2 \equiv 1 \pmod{n}$ järgmisele kujule:

$$598963^2 - 1 \equiv (598963 - 1) \cdot (598963 + 1) \equiv 598962 \cdot 598964 \equiv 0 \pmod{n}.$$

Eeldades, et $n = pq$, kus p ja q on algarvud, saame et korrutis $598962 \cdot 598964$ jagub n -ga kuid kumbki teguritest n -ga jaguda ei saa sest nad on n -st rangelt väiksemad. Seega jagub üks tegureist arvuga p ja teine neist arvuga q . Seega saame otsitava teguri kätte, kui arvutame suurima ühisteguri:

$$(598962, 1199021) = 1097,$$

mis on algarv. Kontroll näitabki, et $1199021 = 1097 \cdot 1093$.

Ülesanne 2. Lahutades kolmanda mooduli teguriteks saame $n_C = 145 = 5 \cdot 29$. Tähistame $p = 5$ ja $q = 29$. Kongruentsist $x^3 \equiv 80 \pmod{145}$ saame võrrandisüsteemi:

$$\begin{cases} x^3 \pmod{5} = 0 \\ x^3 \pmod{29} = 22 \end{cases},$$

milles esimesest võrrandist järeldub kohe, et $x \equiv 0 \pmod{5}$. Teise võrrandi lahendamiseks leiame $\frac{1}{3} \pmod{q} - 1 = \frac{1}{3} \pmod{28} = 19$. Seega $x \equiv 22^{19} \pmod{40}$ ja selle arvutamiseks kasutame skeemi:

$$22^{19} \equiv 22^{2^4} \cdot 22^{2^1} \cdot 22^{2^0},$$

kus teguriteks olevad astmed arvutatakse skeemi $22^{2^{k+1}} \equiv (22^{2^k})^2$ järgi ja saame:

$$22^{2^0} \equiv 22, 22^{2^1} \equiv 484 \equiv 20, 22^{2^2} \equiv 400 \equiv 23, 22^{2^3} \equiv 7, 22^{2^4} \equiv 49.$$

Seega, $x \equiv 22^{19} \equiv 49 \cdot 20 \cdot 22 = 21560 \equiv 13 \pmod{29}$ ja x väärtuse saab leida võrrandisüsteemist

$$\begin{cases} x \pmod{5} = 0 \\ x \pmod{29} = 13 \end{cases}$$

Hiina jäägiteoreemi abil. Kasutades Eukleidese algoritmi saame, et $6 \cdot 5 + (-1) \cdot 29 = 1$ ja seega $p^{-1} \pmod{q} \equiv 6$ ja siit tuleneb, et ainus lahend vahemikus $[0 \dots 144]$ on

$$x = 6 \cdot 5 \cdot 13 + (-1) \cdot 29 \cdot 0 \pmod{145} = 100.$$