

Ülesanded

Ülesanne 1 (30 punkti). Arvuta (võimalikult lihtsalt) $7^{162} \pmod{205}$.

Ülesanne 2 (40 punkti). RSA krüptosüsteemis kasutatakse algarvudena $p = 101$ ja $q = 37$. Avalik astendaja $e = 17$. Leia salajane astendaja d . Kas samade algarvude korral oleks $e = 5$ sobilik avalik astendaja? Põhjenda!

Ülesanne 3 (60 punkti). 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 krüptogrammide 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

Ü1.1 Astme $7^{162} \pmod{205}$ arvutamiseks lahutame esmalt mooduli 205 algarvulisteks teguriteks ja saame, et $205 = 5 \cdot 41$. Arvutame Euleri funktsiooni $\varphi(205) = (5-1)(41-1) = 160$. Et $(7, 205) = 1$, siis saame rakendada Euleri teoreemi, mille kohaselt

$$7^{160} \pmod{205} = 1,$$

ja seega $7^{162} \pmod{205} = 7^2 \pmod{205} = 49$.

Ü1.2. Et $\varphi(n) = (p-1)(q-1) = 100 \cdot 36 = 3600$, siis saame, et $d = \frac{1}{17} \pmod{3600}$, mis tuleb Eukleidese algoritmi järgi arvatuna 2753. Astendaja $e = 5$ ei sobi antud algarvude valiku korral, sest $(5, 3600) = 5 \neq 1$ ja seega 5 ei ole pööratav mooduli $\varphi(n)$ järgi.

Ü1.3. 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:

$$\begin{cases} x^3 \pmod{5} = 0 \\ x^3 \pmod{29} = 20 \end{cases},$$

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

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