

Ülesanded

Ülesanne 1 (30 punkti). Arvuta (võimalikult lihtsalt) $7^{398} \pmod{451}$.

Ülesanne 2 (40 punkti). RSA krüptosüsteemis kasutatakse algarvudena $p = 113$ ja $q = 47$. Avalik astendaja $e = 19$. Leia salajane astendaja d . Kas samade algarvude korral oleks $e = 23$ 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 $n_A = 205$, $n_B = 391$ ja $n_C = 319$. Avalik astendaja on kõigil ühine: $e = 3$. Ründajale on teada, et kõigile kolmele kasutajale saadetakse üks ja sama salasõnum $x \in \{0, \dots, 204\}$, kusjuures vastavad krüptogrammid on:

$$\begin{aligned}y_A &= x^3 \pmod{205} = 10 \\y_B &= x^3 \pmod{391} = 213 \\y_C &= x^3 \pmod{319} = 254\end{aligned}$$

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

Lahendused

Ül.1. Avaldise $7^{398} \pmod{451}$ arvutamisel on esimene mõte tõenäoliselt Euleri teoreemi rakendamine, millest järeldub, et $7^{\varphi(451)} \pmod{451} = 7^{400} \pmod{451} = 1$, sest $(7, 451) = 1$. Antud ülesandes on aga astendaja väiksem kui 400, mistõttu astendaja taandamisest $\pmod{400}$ ei ole otseselt kasu. Siiski saab siin kasutada asjaolu, et 7 on pööratav element mooduli 451 järgi ja seega:

$$7^{398} \pmod{451} = 7^{398-400} \pmod{451} = 7^{-2} \pmod{451} = 49^{-1} \pmod{451} .$$

Pöördväärtuse 49^{-1} leidmiseks kasutame Eukleidese algoritmi ja saame vastuseks 405.

Ül.2. Et $\varphi(n) = (p-1)(q-1) = 112 \cdot 46 = 5152$, siis saame, et $d = \frac{1}{19} \pmod{5152}$, mis tuleb Eukleidese algoritmi järgi arvutatuna 1627. Astendaja $e = 23$ ei sobi antud algarvude valiku korral, sest $(23, 5152) = 23 \neq 1$ ja seega 23 ei ole pööratav mooduli $\varphi(n)$ järgi.

Ül.3. Lahutades esimese mooduli teguriteks saame $n_A = 205 = 5 \cdot 41$. Tähistame $p = 5$ ja $q = 41$. Kongruentsist $x^3 \equiv 10 \pmod{205}$ saame võrrandisüsteemi:

$$\begin{cases} x^3 \pmod{5} = 0 \\ x^3 \pmod{41} = 10 \end{cases},$$

milles esimesest võrrandist järeldub kohe, et $x \equiv 0 \pmod{5}$. Teise võrrandi lahendamiseks leiame $\frac{1}{3} \pmod{q-1} = \frac{1}{3} \pmod{40} = 27$. Seega $x \equiv 10^{27} \pmod{41}$ ja selle arvutamiseks kasutame skeemi:

$$10^{27} \equiv 10^{24} \cdot 10^{23} \cdot 10^{21} \cdot 10^{20},$$

kus teguriteks olevad astmed arvutatakse skeemi $10^{2^{k+1}} \equiv (10^{2^k})^2$ järgi ja saame:

$$10^{2^0} \equiv 10, 10^{2^1} \equiv 100 \equiv 18, 10^{2^2} \equiv 37, 10^{2^3} \equiv 16, 10^{2^4} \equiv 10.$$

Seega, $x \equiv 10^{27} \equiv 10 \cdot 16 \cdot 18 \cdot 10 = 28800 \equiv 18 \pmod{41}$ ja x väärtuse saab leida võrrandisüsteemist

$$\begin{cases} x \pmod{5} = 0 \\ x \pmod{41} = 18 \end{cases}$$

Hiina jäägiteoreemi abil. Kasutades Eukleidese algoritmi saame, et $(-8) \cdot 5 + 1 \cdot 41 = 1$ ja seega $p^{-1} \pmod{q} \equiv -8$ ja siit tuleneb, et ainus lahend vahemikus $[0 \dots 204]$ on

$$x = (-8) \cdot 5 \cdot 18 + 1 \cdot 41 \cdot 0 \pmod{205} = 100.$$