PĀRBAUDES DARBS

1. Kurš apgalvojums ir patiess?

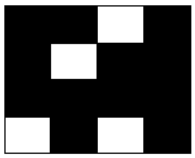
A Abas tabulas ir „Kardano siets”.

B Abas tabulas nav „Kardano siets”.

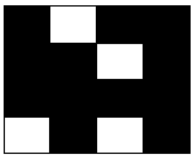
C Tikai tabula **A** ir „Kardano siets”.

D Tikai tabula **B** ir „Kardano siets”.

A



B



2. Kurš apgalvojums ir patiess?

A $\varphi(35) = 3$ B $\varphi(35) = 5$ C $\varphi(35) = 24$ D $\varphi(35) = 35$

3. Paroli no 8 mazajiem burtiem kriptoanalītiķis spēj atklāt

A apmēram 2 stundās

B apmēram 1 minūtē

C apmēram 17 stundās

D apmēram 29 000 gados

4. Vai skaitļi a un b ir kongruenti pēc moduļa n? Kāpēc?

1) $a = 2015,\ b = 3535353,\ n = 5$
2) $a = 2016,\ b = 3535353,\ n = 9.$

Risinājums

1) Nē, jo a, dalot ar 5, dod atlikumu 0, bet b, dalot ar 5, dod atlikumu 3.
2) Jā, jo gan a, gan b, dalot ar 9, dod atlikumu 0 (abi skaitļi dalās ar 9, jo to ciparu summas dalās ar 9).

5. Aprēķināt, kādu atlikumu dod skaitlis 2^{36}, dalot to ar 14!

Risinājums. Virkne $2^m\ (mod\ 14)$, $m = 1,2,3,..$, ir periodiska ar perioda garumu 3, t.i., $2^4 \equiv 2\ (\text{mod } 14)$. Tāpēc $2^{36} = (2^4)^9 \equiv 2^9 \equiv (2^4)^2 \cdot 2 \equiv 2^2 \cdot 2 \equiv 8\ (\text{mod } 14)$. Tātad skaitlis 2^{36}, dalot to ar 14, dod atlikumu 8.