SEMINARAS

2018 gegužės 15 d. 9:00, SRL-I-519

Eugenijus Paliokas

Dviejų pirminių skaičių sandaugos dekompozicija

Šitokios priežastys „privertė“ pasidomėti dviejų pirminių skaičių dekompozicijos problema:

- Tai – lyg koks mentalinis „tabu“, nesgi šis uždavinys vadinamas labai sunkiu:
  Duotajam n surasti p ir q, kad n=pq, laikoma labai sunkia užduotimi. Visas RSA sistemos saugumas remiasi šiuo faktu (Vikipedija).

- RSA Laboratories paskelbė konkursą, kurio esmė yra surasti p ir q duotajam n. Nuo 2007 m. RSA Laboratories šių konkursų neberengia (Vikipedija).

- Ėmė atrodyti, kad mes savo studentus mokome (mentalinio) „paklusnumo“, o ne minties laisvės, juolab ne „įžūlumo“.

Kviečiame dalyvauti.
Seminaro sekretorius A. Bugajev