SEMINARAS

2024 kovo 19 d. 09:00 SRL-I 420

Raimondas Čiegis

Matematiniai rezultatai ir eksperimentai apie vieną 'nenulaužiamą" šifrą

Seminaruose jau nagrinėjome pagrindinius klasikinius ir naujausius šifrus. Jų atsparumas dešifravimui kinta nuo silpnų, pakankamai patikimų iki stiprių. Pastaruosius naudojame kasdien ir miegame ramiai, nes žinome jų stiprumo garantijas: juos galima nulaužti, bet mūsų duomenys tampa atviri dažniausiai dėl žmogiškų klaidų (ar noro neteisėtai uždirbti), o ne dėl to, kad matematinių įverčių garantuojamas patikimumas staiga pasikeičia, nes sukuriami nauji dešifravimo algoritmai.

Dažniausiai kriptografiniai algoritmai remiasi gerai žinomų matematinių uždavinių sprendimo sudėtingumu, juos sprendė talentingi ir net dar stipresni matematikai. Neigiamas rezultatas yra geriausias patikimumo garantas.

Trumpai prisiminsime DES, AES, RSA algoritmus. Tada atliksime netikėtą viražą ir panagrinėsime Cezario, Vigenerė ('the indecipherable cipher') šifrus. Keista bus išvada, bet jie tikrai yra 'the indecipherable ciphers'.

Būtent taip: aptarsime jų ryšį su One Time Pad (OTP) šifru, kuris yra absoliučiai patikimas (su teorema gi negalima ginčytis, o tokį įrodymą pateikė Claude Shannon 1949 metais). Įdomu, kad galima pateikti ir ne tokį griežtą, bet paprastesnį paaiškinimą, kodėl OTP šifras yra nenulaužiamas.

Seminaro svarbiausia dalis bus eksperimentinė. Patikrinsite (pažaisite) ar tikrai dešifravimo užduotis tampa paprasta, jeigu aš "netyčia" padariau klaidą ir du kartus panaudojau tą patį raktą.

Kviečiame dalyvauti.
Seminaro sekretorius A. Bugajev