SEMINARAS

2020 spalio 20 d. 09:00, SRL-I 401

Raimondas Čiegis

Tikimybių teorijos ir statistikos metodai kriptografijoje

Slaptųjų dokumentų ir informacijos slėpimo poreikis yra toks pat senas, kaip ir mūsų istorija. Šis poreikis apima labai didelę dalį žmonių veiklos sričių (teisingiau, sunku įvardinti tokią sritį, kur informacijos slėpimas nebūtų naudojamas).

Tvari tik kova tarp informacijos slėpimo (šifravimo) ir jos "nulaužimo" algoritmų. Čia niekada nebuvo galutinio nugalėtojo, tik trumpalaikės pergalės.

Seminare apžvelgsime du klasikinius šifravimo algoritmus - jie puikūs, išradingi ir tikrai nelengvai iššifruojami. Daug vilčių turėta, kad jie absoliučiai saugūs (ypač antrojo algoritmo atveju). Tačiau baziniai tikimybių teorijos ir statistikos rezultatai, kuriuos pateikiame ir mūsų studentams matematikos studijų pirmuose semestruose, sugriovė šias viltis. Neblogas pavyzdys, galintis pareklamuoti šių kursų naudą VGTU studentų išsilavinime.

Teorinę dalį derinsime su praktika, pabandysime perskaityti vieną įdomų užšifruotą tekstą.

Kaip visada, šioje tematikoje nėra galutinio nugalėtojo. Tiems, kas norės pratęsti šią pažintį su kriptografiniais algoritmais, pateiksime naujų uždavinių rinkinėlį.

Kviečiame dalyvauti.
Seminaro sekretorius A. Bugajev