

SEMINARAS

2015 spalio 6 d. 8:45, SRA II 09

Raimondas Čiegis

Skaičiavimo matematika ir matematinis modeliavimas

Apie algoritmus, kurie keičia mūsų gyvenimą.
III paskaita. Kriptografija ir kriptografiniai pinigai.

Šios paskaitos tikslas – supažindinti su kriptografiniais algoritmais ir technologijomis, kurie esmingai panaudoti realizuojant populiariają kriptografinę valiutą – bitcoin.

Aptarsime šias svarbiausias duomenų struktūras ir kriptografinius algoritmus, bei jų taikymus:

- a) kriptografinės maišos funkcijos (hash functions), jų papildomos savybės;
- b) maišos rodyklės (hash pointers) ir duomenų struktūros;
- c) skaitmeninis parašas;
- d) viešasis raktas;
- e) paprasčiausias kriptografinės valiutos pavyzdys.

Kasdien sužinome, kad bitcoin valiuta vis plačiau naudojama net ir Lietuvos ekonomikoje – tai tampa prestižo reikalu ir ... taip atsiskaityti yra pigiau. Matyt verta pasidomėti, kaip veikia šis projektas, kiek saugu (ar saugu?) laikyti santaupas bitcoin valiuta, ar tai nebus dar vienas "dot" burbulas?

Kviečiame dalyvauti.
Seminaro sekretorius A. Bugajev