Kryptológia (2) – úvod

Martin Stanek

2025

KI FMFI UK Bratislava

Úvod

- štvrtok @ 14:50, M-II
- hodnotenie
  - 50% test (na konci semestra)
  - 50% projekt: 20 min. prezentácia (OK, čiastočne, nesplnené)
- prednášky budú a témy projektov sú na web stránke
- kontakt
  - email: stanek@dcs.fmph.uniba.sk
  - miestnosť: M-214
  - web stránka: www.dcs.fmph.uniba.sk/~stanek

Náplň predmetu (orientačne)

1. Signal – kryptografia
2. Symbolická analýza kryptografických protokolov
3. Bezznalostné dôkazy
4. Dokázateľá bezpečnosť
   - Bezpečnosť asymetrického šifrovania
   - Bezpečnosť podpisových schém
5. Kryptoanalýza symetrických šifier
   - Algebraický a korelačný útok na prúdové šifry
   - Diferenčná a lineárna kryptoanalýza
   - Integrálna kryptoanalýza a cube útok
6. Crystals-Kyber
7. Mriežky v kryptológii
   - GGH a NTRU
   - Kryptoanalýza – vybrané útoky
8. Bezpečné výpočty viacerých účastníkov