PB173 - Tématický vývoj aplikací v C/C++ (podzim 2014)

Skupina: Aplikovaná kryptografie a bezpečné programování

https://is.muni.cz/auth/el/1433/podzim2013/PB173/index.qwarp?fakulta=1433;obdobi=5983;predmet=734514;prejit=2957738;

Petr Švenda svenda@fi.muni.cz

Konzultace: A406, Monday 15-15:50

CROCS
Centre for Research on Cryptography and Security

Practical assignment – this week

- Finalize implementation of your project
  - Register and authenticate securely against server
  - Get list of online users securely (privacy, integrity…)
  - Secure and high-speed communication (multi-threaded CTR mode with pool of keys) between two clients (privacy, integrity, freshness…)
  - Easy to compile, setup and run example test cases (everything in GitHub repo and single zip in IS)
- Prepare slides about your implementations
  - 10 minutes talk, presented by you at 2.12.2014