

Lúštenie historických šifier na GRIDe

Bc. Martin Eliáš

Ing. Eugen Antal

Slovenská technická univerzita v Bratislave

- Grid vrámci STU
- Zjednodušenie práce pre výskumníkov
- Využitie dostupných prostriedkov
- Ušetrenie času a peňazí

IBM iDataPlex

- 52 výpočtových uzlov
- 624 CPU
- 2,5TB RAM
- 115TB HDD
- 6 TFlop/s (vs 93k Sunway TaihuLigth)



- Zoznámenie sa s gridom
- Štúdium paralelných problémov
- Technológie
- Prvé experimenty s bruteforce útokom

- Definícia
- Synchronizácia
- Komunikácia
- Návrh

- OpenMPI a C++
- Skript na generovanie projektov a ich spúšťanie
- Stavebné bloky (Runner, Communicator, ...)

Plán na letný semester

- Dokončenie frameworku
- Slovníkový útok
- Experiment s PGA

Ďakujem za pozornosť
