Lúštenie historických šifier na GRIDe

Bc. Martin Eliáš

Ing. Eugen Antal, PhD.

Slovenská technická univerzita v Bratislave

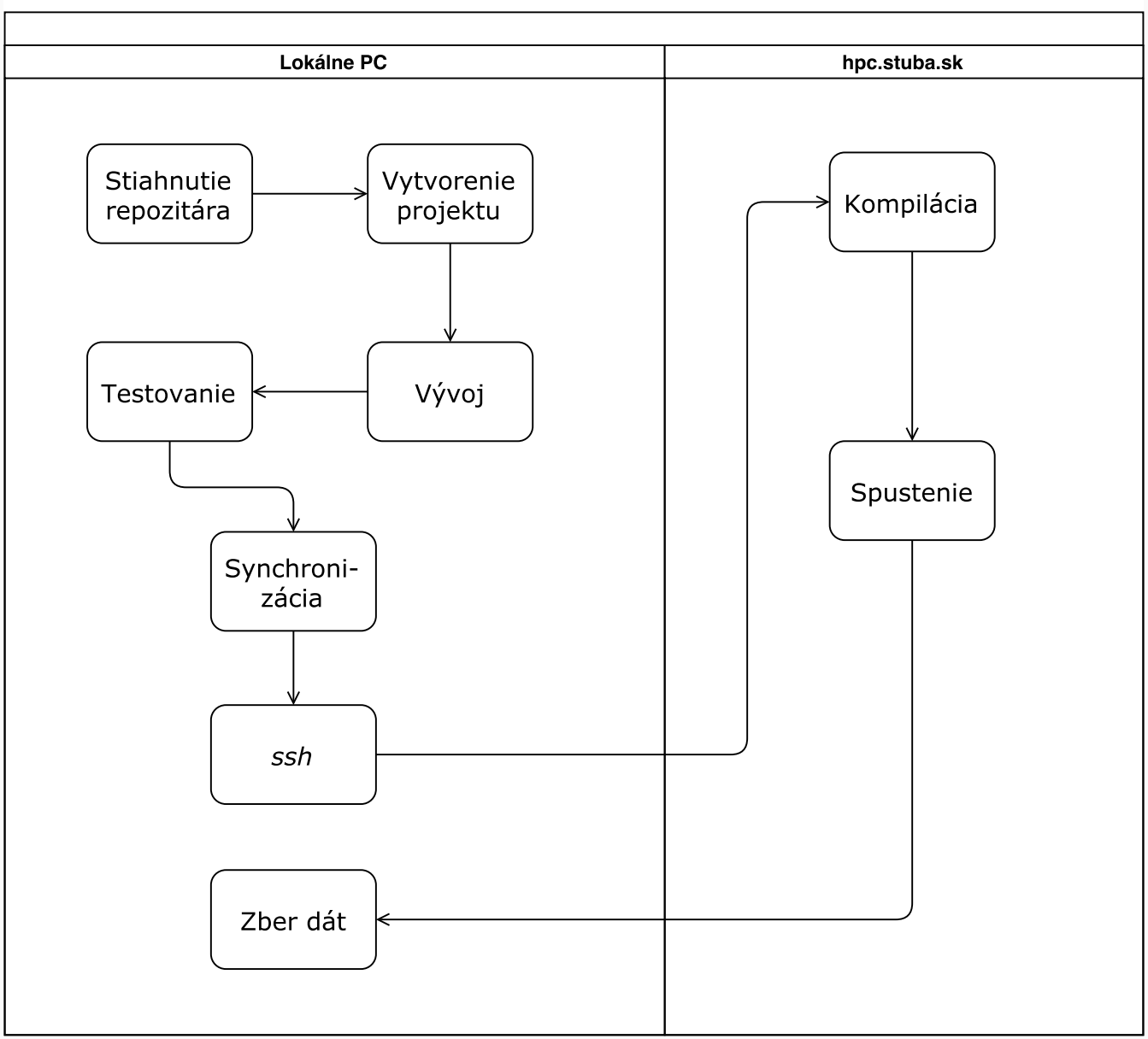
Úvod

- Historické šifry
- Grid vrámci STU
- Monoalfabetická substitúcia
- Paralelné genetické algoritmy

Požiadavky

- Automatické vytváranie projektov
- Lokálny vývoj a testovanie
- Zdieľanie modulov medzi projektami
- Automatické generovanie a úprava skriptov pre gridové prostredie
- Jednoduchá synchronizácia s gridom hpc.stuba.sk

Príklad použitia



Technológie

- C++
- CMake
- Boost
- MPI
- Git

build.sh

- Vytvorenie projektu
- Kompilácia
- Spúštanie projektov
- Synchronizácia s gridom

Genetické algoritmy

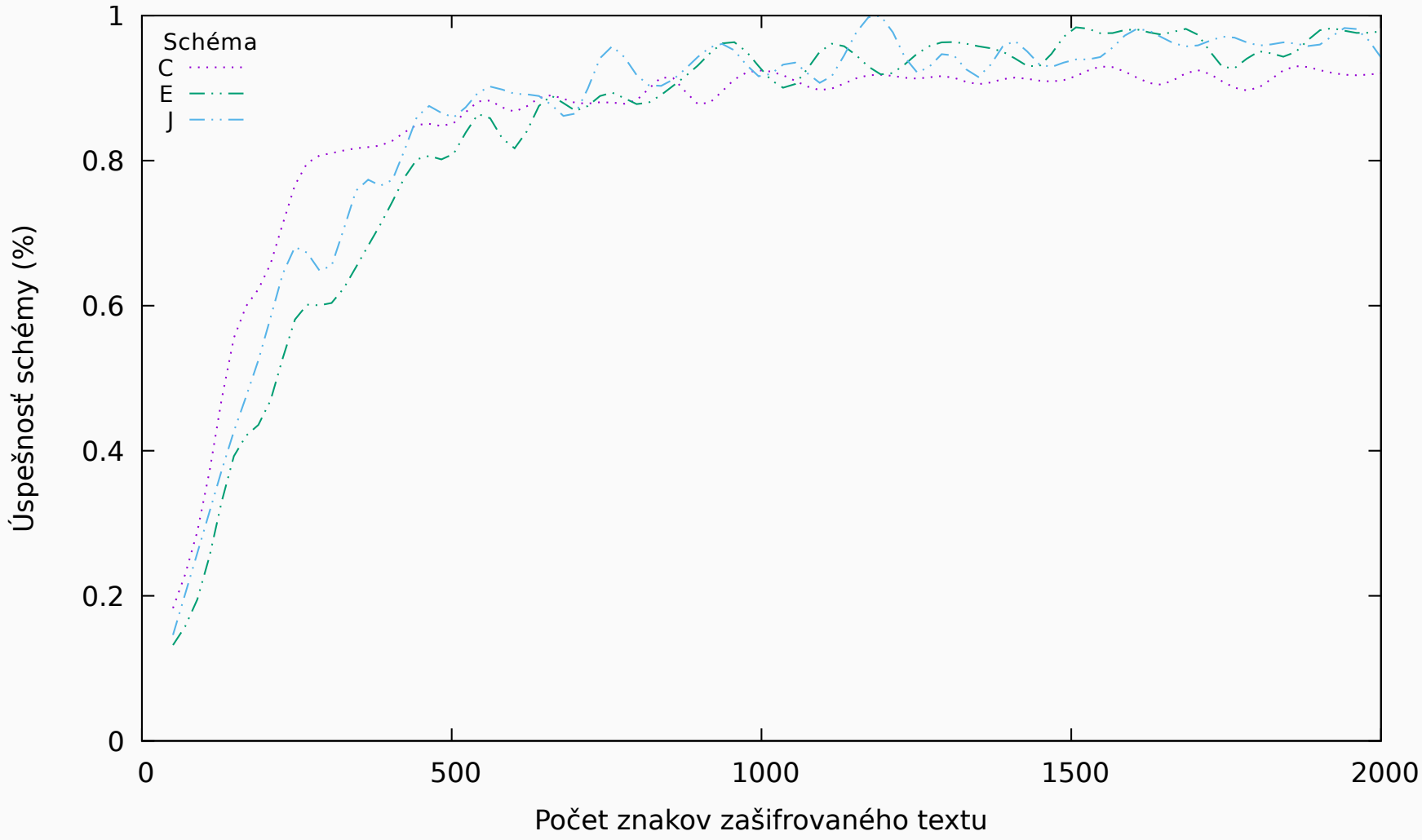
- Implementácia
- Vytváranie schém
- Distribúcia parametrov

Experiment s GA

- Veľkosť populácie: 10, 20, 50, 100
- Počet iterácií: 10000, 50000
- 10 rôznych schém
- Dĺžky textov od 50, 100, ..., 2000
- 34 hodín, 320 000 spustení GA

Výsledky GA 50000 iterácií 100 jedincov

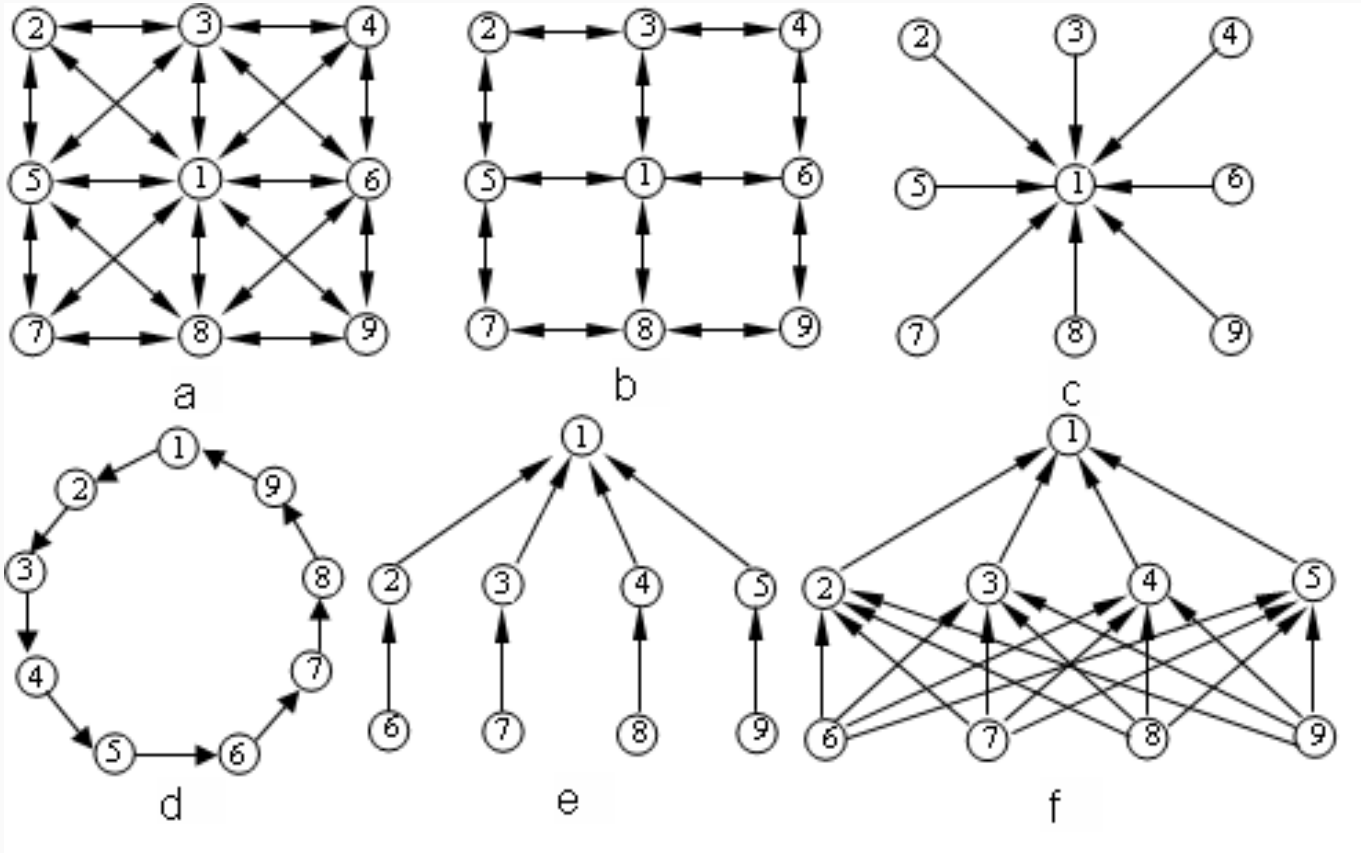
Výsledky GA 50000 iterácií 100 jedincov



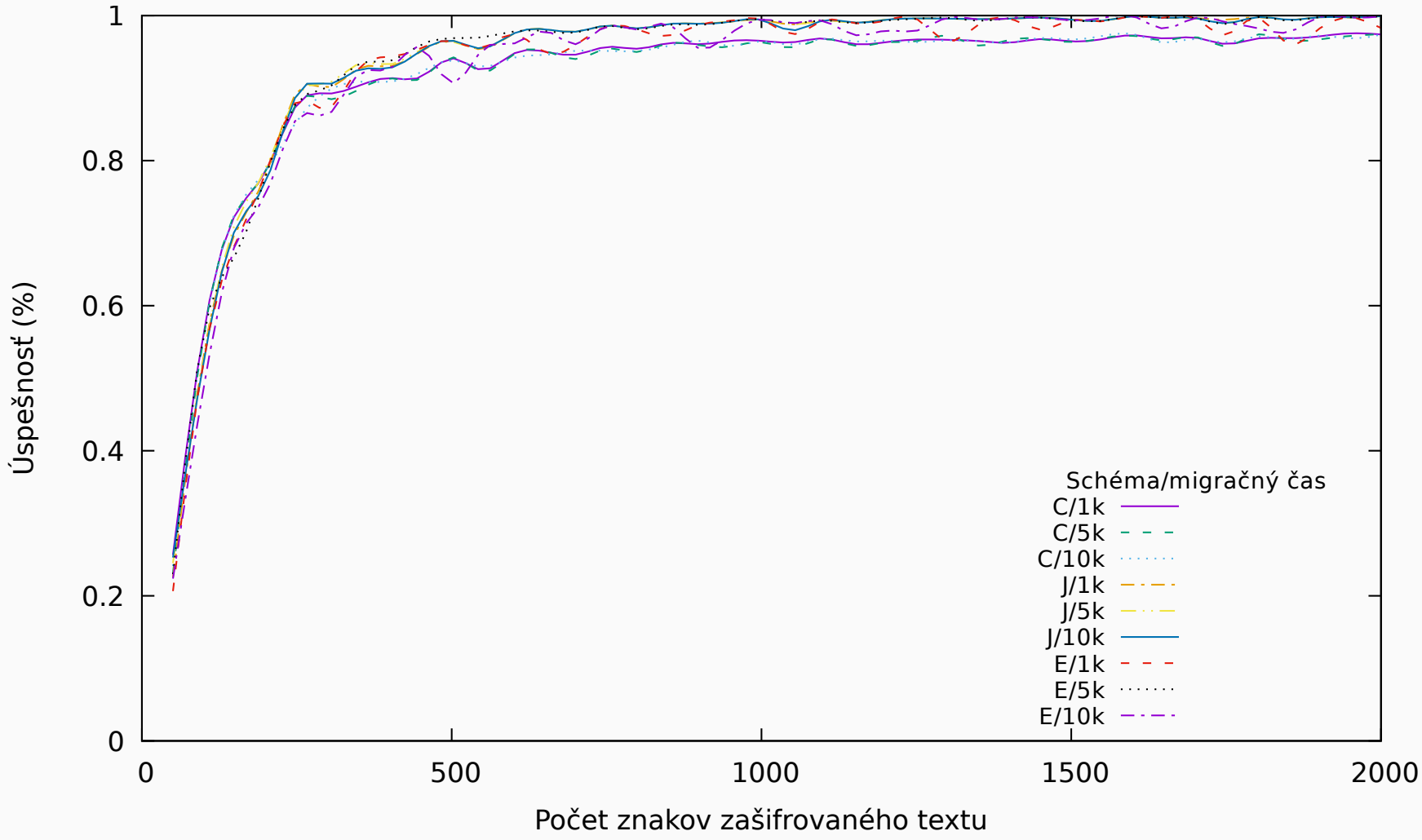
Experiment s PGA

- 3 schémy z predchádzajúceho exprimentu
- 4 rôzne topológie
- Veľkosti topológií: 3, 5, 11
- Migračný čas: 1000, 5000, 10000 iterácií
- 2,5 týždňa, viac ako 7 000 000 spustení GA

Toplógie PGA



Výsledky PGA



Zhrnutie

- Vytvorenie nástrojov na kryptoanalýzu
- Modul PGA
- Vplyv veľkosti populácie na úspešnosť
- Takmer 100% úspešnosť riešenia pri PGA
- Možné využitie pre ďalších riešiteľov

Ďakujem za pozornosť

Oponentská otázka

- Čo je to manhatanovská vzdialenosť?