Szivárványtáblák generálása griden

Kiss Viktória Dr. Érdi Gergő

ELTE IK, 2009. december 10.

Kriptográfiai hasítófüggvények

- A: Nyílt szövegek halmaza (praktikusan valamilyen T véges ábécé feletti T^*)
- B: Hasított értékek véges halmaza
- $\phi : A \rightarrow B$ nem injektív függvény

Kriptográfiai hasítófüggvények

- A: Nyílt szövegek halmaza (praktikusan valamilyen T véges ábécé feletti T^*)
- B: Hasított értékek véges halmaza
- $\phi : A \to B$ nem injektív függvény

- $a \in A$ jelszóhoz $\phi(a)$-t tároljuk el

Kriptográfiai hasítófüggvények

- A: Nyílt szövegek halmaza (praktikusan valamilyen T véges ábécé feletti T^*)
- B: Hasított értékek véges halmaza
- $\phi : A \to B$ nem injektív függvény

- $a \in A$ jelszóhoz $\phi(a)$-t tároljuk el
- Cél: adott $b \in B$-hez találni egy $a' \in A$-t úgy, hogy $\phi(a') = b$

Kriptográfiai hasítófüggvények

- A: Nyílt szövegek halmaza (praktikusan valamilyen T véges ábécé feletti T^*)
- B: Hasított értékek véges halmaza
- $\phi : A \to B$ nem injektív függvény

- $a \in A$ jelszóhoz $\phi(a)$-t tároljuk el
- Cél: adott $b \in B$-hez találni egy $a' \in A$-t úgy, hogy $\phi(a') = b$

- Adott $A_0 \subseteq A$ elemeihez akarunk táblázatot készíteni

Kriptográfiai hasítófüggvények

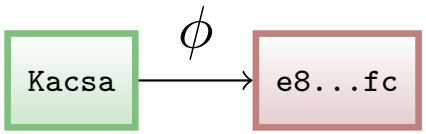
- A: Nyílt szövegek halmaza (praktikusan valamilyen T véges ábécé feletti T^*)
- B: Hasított értékek véges halmaza
- $\phi : A \to B$ nem injektív függvény

- $a \in A$ jelszóhoz $\phi(a)$-t tároljuk el
- Cél: adott $b \in B$-hez találni egy $a' \in A$-t úgy, hogy $\phi(a') = b$

- Adott $A_0 \subseteq A$ elemeihez akarunk táblázatot készíteni
- Helyigény csökkentése: szivárványtáblák

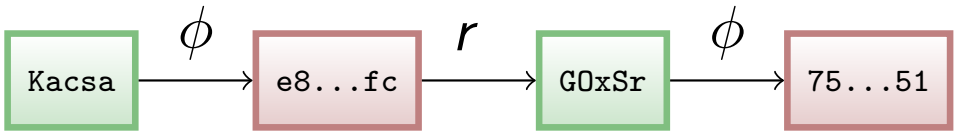
Szivárványtáblák

Szivárványtáblák



Szivárványtáblák

Szivárványtáblák



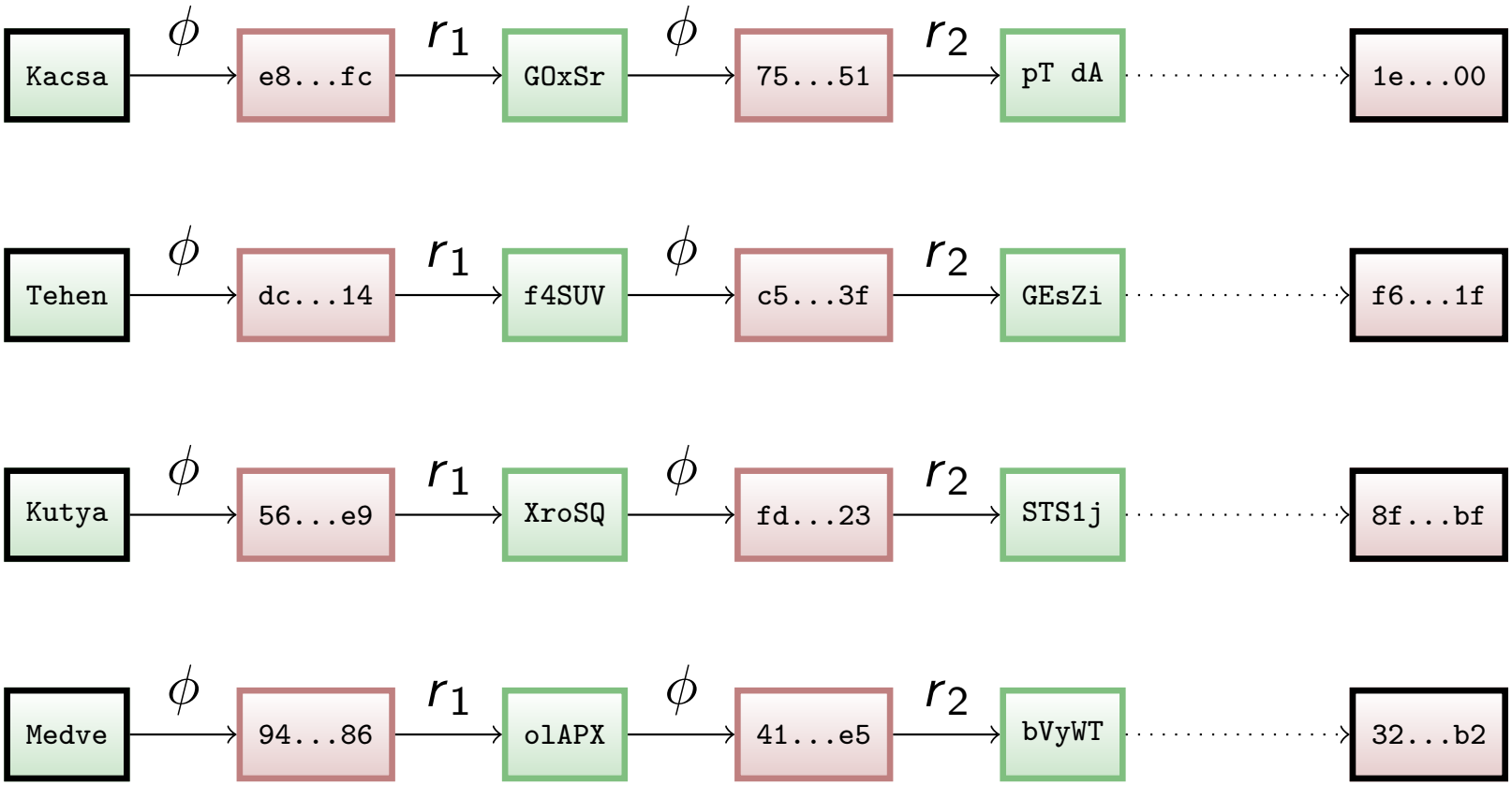
Szivárványtáblák

Szivárványtáblák

Szivárványtáblák

Szivárványtáblák

Szivárványtáblák



Szivárványtáblák

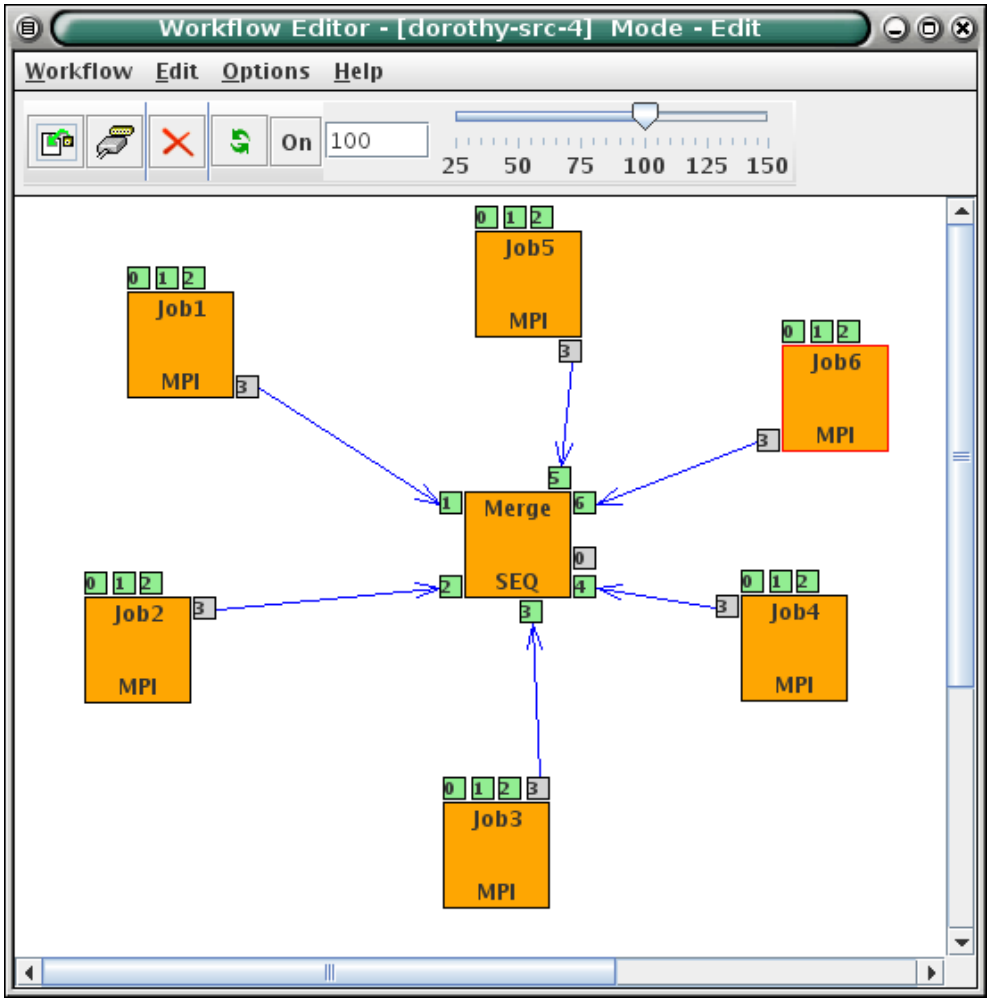
Implementáció: Platform

- A feladat könnyen párhuzamosítható: minden szál a szótár néhány láncát készíti el
- Implementációs platform: MPI, EGEE

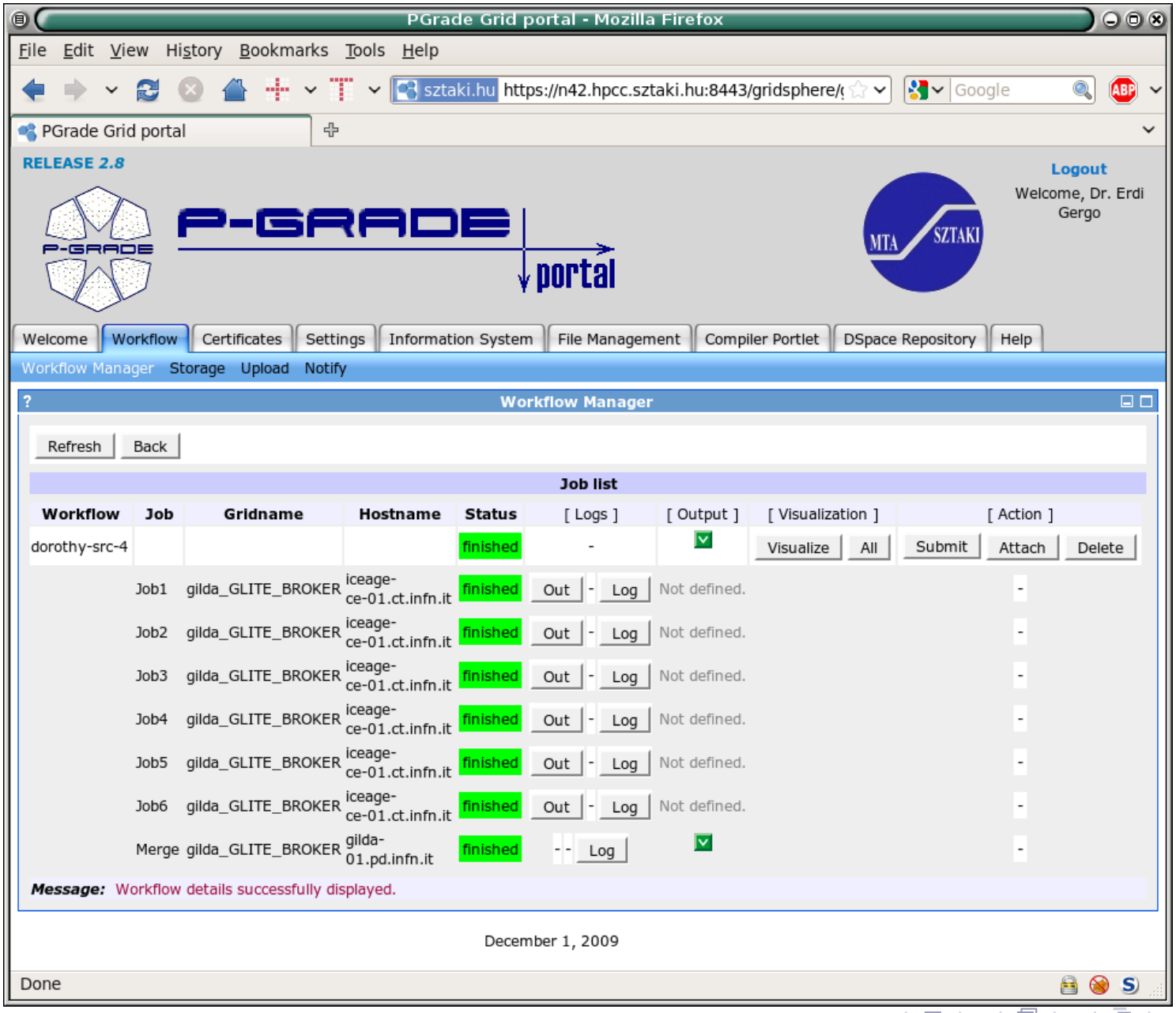
- 6+1 EGEE job, jobonként 20+1 MPI szál

Implementáció: Workflow

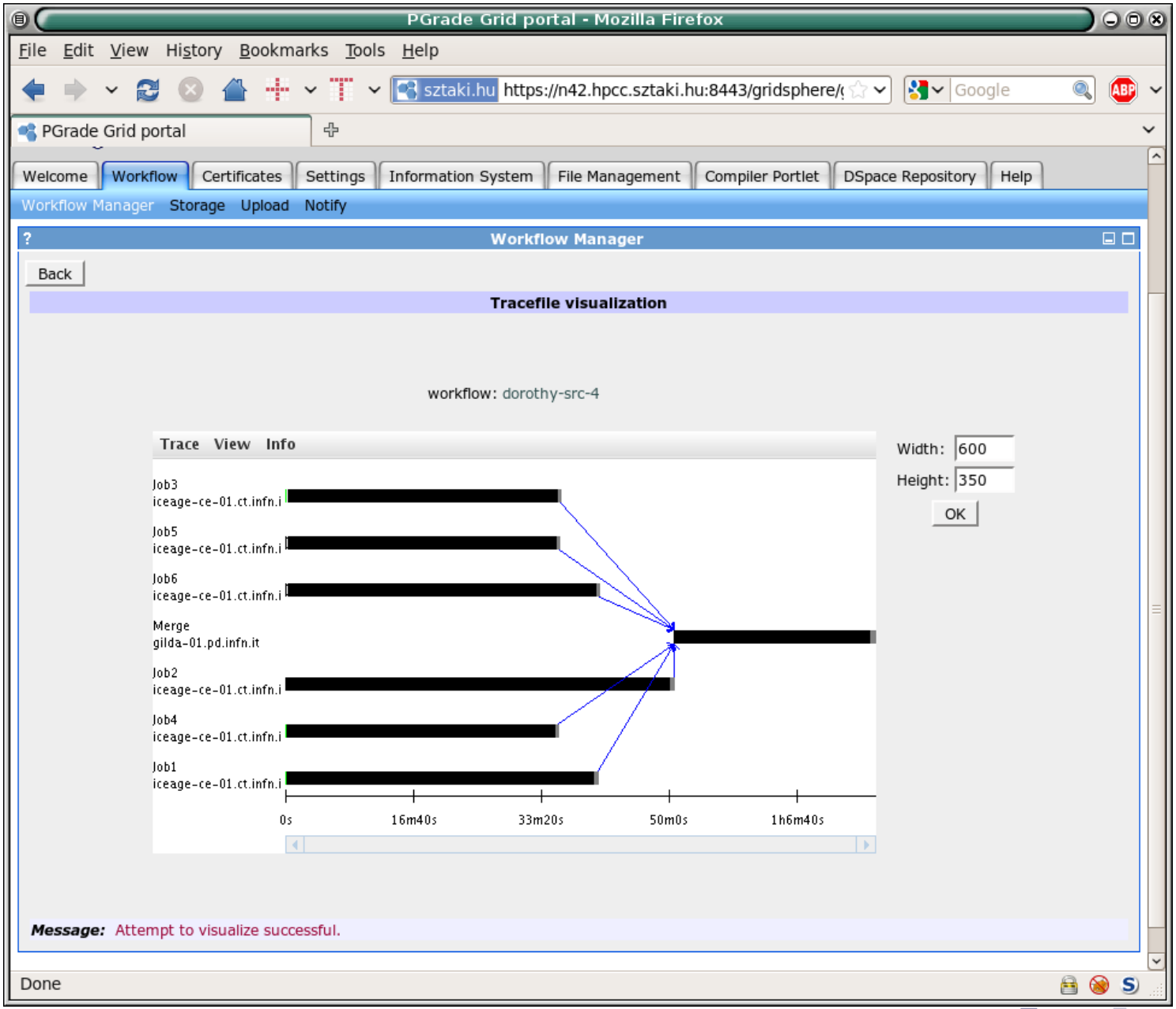
Tipikus ,,bag of tasks” alkalmazás:



Futtatási eredmény



Futtatási eredmény



A kész szótár

```
$ ls -l dorothy.out
-rw-r--r-- 1 cactus cactus 36288000 2009-11-25 20:15 dorothy.out
```

A kész szótár

```
$ ls -l dorothy.out
-rw-r--r-- 1 cactus cactus 36288000 2009-11-25 20:15 dorothy.out

$ ./dorothy-search dorothy.out 412993573ac5399904aa16173afb743b
```

A kész szótár

```
$ ls -l dorothy.out
-rw-r--r-- 1 cactus cactus 36288000 2009-11-25 20:15 dorothy.out

$ ./dorothy-search dorothy.out 412993573ac5399904aa16173afb743b
Searching for 412993573ac5399904aa16173afb743b
```

A kész szótár

```
$ ls -l dorothy.out
-rw-r--r-- 1 cactus cactus 36288000 2009-11-25 20:15 dorothy.out

$ ./dorothy-search dorothy.out 412993573ac5399904aa16173afb743b
Searching for 412993573ac5399904aa16173afb743b
Starting from RwyDU
```

A kész szótár

```
$ ls -l dorothy.out
-rw-r--r-- 1 cactus cactus 36288000 2009-11-25 20:15 dorothy.out

$ ./dorothy-search dorothy.out 412993573ac5399904aa16173afb743b
Searching for 412993573ac5399904aa16173afb743b
Starting from RwyDU
...
```

A kész szótár

```
$ ls -l dorothy.out
-rw-r--r-- 1 cactus cactus 36288000 2009-11-25 20:15 dorothy.out

$ ./dorothy-search dorothy.out 412993573ac5399904aa16173afb743b
Searching for 412993573ac5399904aa16173afb743b
Starting from RwyDU
...
Starting from 87lZI
Found "grid."
```

A kész szótár

```
$ ls -l dorothy.out
-rw-r--r-- 1 cactus cactus 36288000 2009-11-25 20:15 dorothy.out

$ ./dorothy-search dorothy.out 412993573ac5399904aa16173afb743b
Searching for 412993573ac5399904aa16173afb743b
Starting from RwyDU
...
Starting from 87lZI
Found "grid."

$ ./dorothy-search dorothy.out 7ddae137e45c954b1ac4ff33486fda7f
```

A kész szótár

```
$ ls -l dorothy.out
-rw-r--r-- 1 cactus cactus 36288000 2009-11-25 20:15 dorothy.out

$ ./dorothy-search dorothy.out 412993573ac5399904aa16173afb743b
Searching for 412993573ac5399904aa16173afb743b
Starting from RwyDU
...
Starting from 87lZI
Found "grid."

$ ./dorothy-search dorothy.out 7ddae137e45c954b1ac4ff33486fda7f
Searching for 7ddae137e45c954b1ac4ff33486fda7f
Starting from JvkO2
...
Starting from OIiT8
Found ".grid"
```