

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
- ▶ $\phi : A \rightarrow B$ 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
- ▶ $\phi : A \rightarrow B$ 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
- ▶ $\phi : A \rightarrow B$ 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

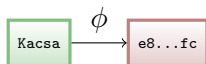
Kriptográfiai hasítófüggvények

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

Kacsa

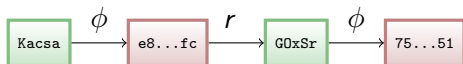
Szivárványtáblák



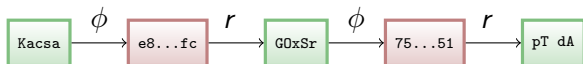
Szivárványtáblák



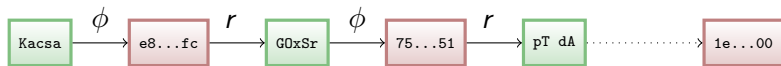
Szivárványtáblák



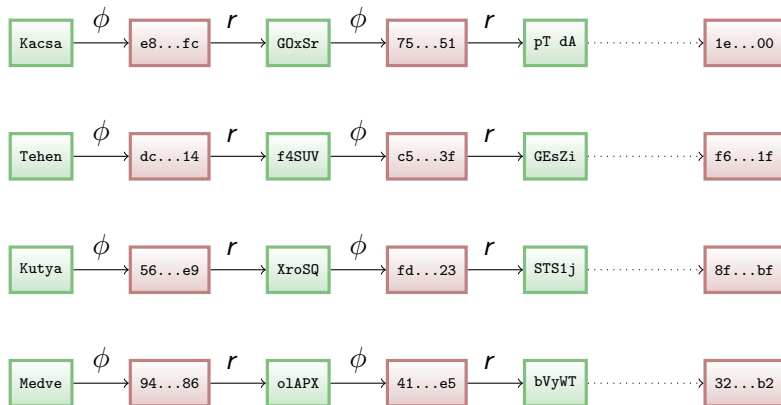
Szivárványtáblák



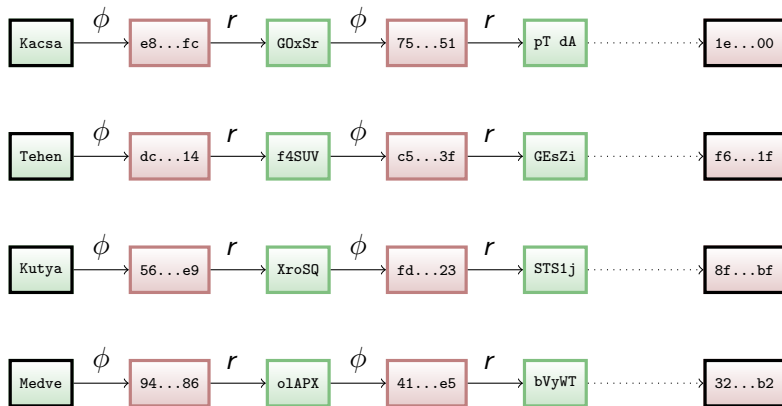
Szivárványtáblák



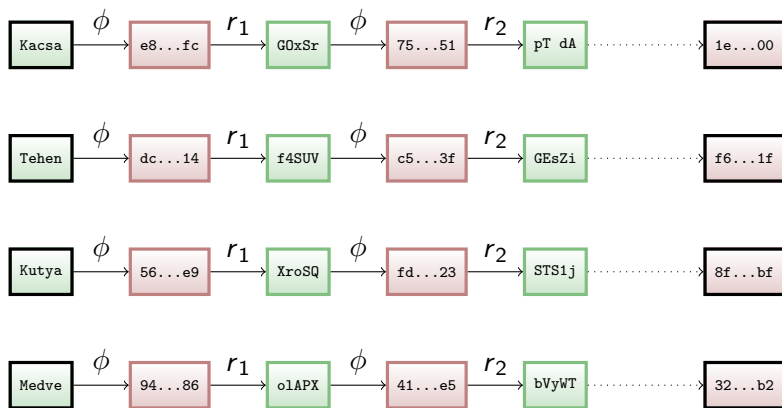
Szivárványtáblák



Szivárványtáblák



Szivárványtáblák



Szivárványtáblák

Kacsa

1e...00

Tehen

f6...1f

Kutya

8f...bf

Medve

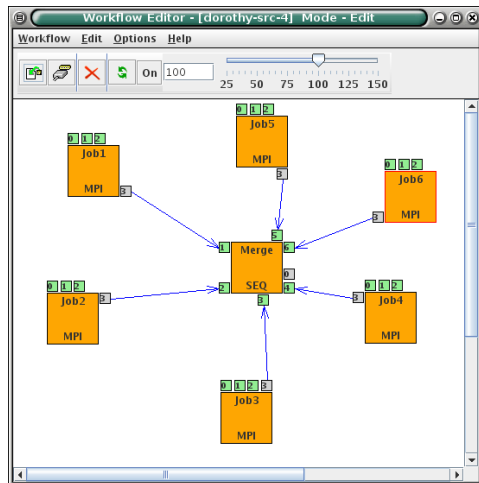
32...b2

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

PGrade Grid portal - Mozilla Firefox

File Edit View History Bookmarks Tools Help

sztaki.hu https://n42.hpcc.sztaki.hu:8443/gridsphere/

PGrade Grid portal

Welcome Workflow Certificates Settings Information System File Management Compiler Portlet DSpace Repository Help

Workflow Manager Storage Upload Notify

Workflow Manager

Back

Tracefile visualization

workflow: dorothy-src-4

Trace View Info

Job3
iceage-ce-01.ct.infn.i

Job5
iceage-ce-01.ct.infn.i

Job6
iceage-ce-01.ct.infn.i

Merge
gilda-01.pd.infn.it

Job2
iceage-ce-01.ct.infn.i

Job4
iceage-ce-01.ct.infn.i

Job1
iceage-ce-01.ct.infn.i

Width: 600
Height: 350
OK

0s 16m40s 33m20s 50m0s 1h6m40s

Message: Attempt to visualize successful.

Done

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 Jvk02
...
Starting from 0IiT8
Found ".grid"
```