

# Nové možnosti pri hľadani hesiel

Moje poznatky s aplikácie

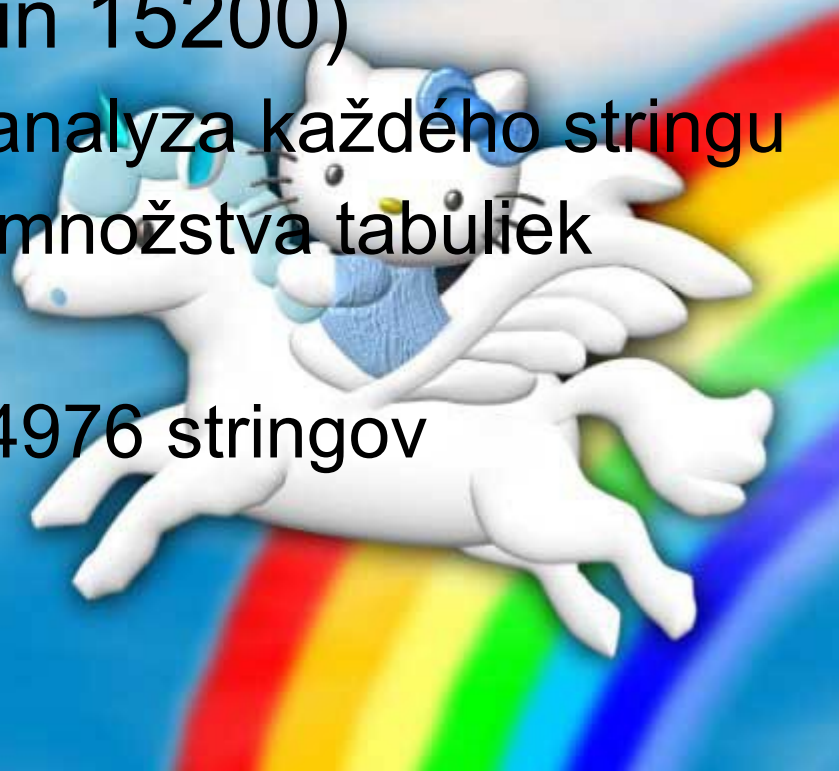
# Okruhy

- Efektivita RT útoku
- perfected rainbow tabulky
- markovove retazce
- generatore stringov klavesnice
- Pouzitie Nvidia CUDA

# Rainbow table attack efektivita

- LM BF 26 dní na jednom CPU
- LM RT attack (chain 15200)
  - 2.5 min pri cryptoanalyza každého stringu
  - Cca 30min podľa množstva tabuliek

Hranica efektivity 14976 stringov  
( $26 \times 24 \times 60 / 2.5$ )



# Optimalizácia RT

- Odstránenie zdvojených chainov

`rm_duplicate_chains.cc`

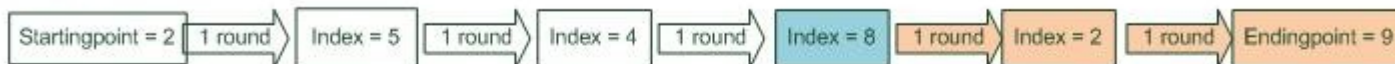
[http://www.sisecurite.fr/articles\\_et\\_actualites/Retirer-les-doublons-des-Rainbow.html](http://www.sisecurite.fr/articles_et_actualites/Retirer-les-doublons-des-Rainbow.html)

- Vytvorenie perfected tables  
`rtperfecter` (merging chains)

# Perfected tables

- Spájané sú chains s rovnakým Endingpointom a zhodným indexom na rovnakej pozícii

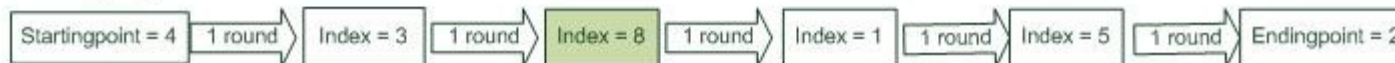
## Merging chain 1



## Merging chain 2



## Non merging chain



# Výsledok

- + Zredukovanie veľkosti tabuliek
- + Zrýchlenie vzhľadávania
- Na vstup treba  $x$  násobne viac tabuliek
- Náhodné prírastky

# Markovove reťazce

- Generovanie na základe pravdepodobnosti
- Použitá vzorka 80 tis. neznámich hesiel
- úspešnosť:
  - Dĺžka 6 - nájdených 153 (60 dní)
  - Dĺžka 7 - nájdených 138 (310 dní) ip 30
  - Dĺžka 8 - nájdených 2 (1500 dní) ip 4

<http://btb.banquise.net/bin/myjohn.tgz>

# Keyboard string

- Rovnaká vzorka 80 tis. Hesiel  
Úspešnosť 55 hesiel za 35 hodín
- + Efektívne kombinácie
- Neúplná implementácia

# Zoznam zdrojov

- <http://openwall.info/wiki/john/markov>
- <http://www.freerainbowtables.com/en/faq/>
- <http://bvernoux.free.fr/md5/index.php>
- [http://www.sisecurite.fr/articles\\_et\\_actualites/M](http://www.sisecurite.fr/articles_et_actualites/M)