Automatické dešifrovanie starých šifier

Kristína Komanová

Univerzita Komenského v Bratislave
FMFI

RNDR. Michal Forišek, phd.

13. júna 2019

Tradičné šifrovacie systémy

- **substitučné** - znaky otvoreného textu sa nahradia znakom/skupinou znakov šifrového textu
  - monoalfabetické
  - polygramové
  - polyalfabetické
  - homofónne
- **transpozičné** - šifrový text vzniká preusporiadaním znakov otvoreného textu

Ciele práce

- spraviť prehľad techník používaných pri dešifrovaní starých šifier, s dôrazom na moderné automatické techniky
- navrhnúť a **implementovať automatické dešifrátory**, s dôrazom na techniky založené na pravdepodobnostných modeloch
- skúmať **otázku minimálnej dĺžky šifrového textu** potrebnej na úspešné dešifrovanie, pokúsiť sa o teoretické a/alebo experimentálne zistenie dolných a horných odhadov

Podobné problémy

- konverzia textu do štandardizovaného formátu
- fonetický preklad jazyka
- neznámy jazykový systém
- strojový preklad

Automatické dešifrovanie

- **Heuristická metóda** - definuje, akým spôsobom budeme prehľadávať stavový priestor
- **Skórovacia funkcia** - ohodnocuje kvalitu dešifrovaného textu

Heuristické metódy

- Hill climbing
- Simulované žíhanie
- Vitterbiho algoritmus [Kevin Knight2006],[Sujith Ravi2011]
- Celočíselné programovanie [Ravi and Knight2008]
- Beam search [Malte Nuhn2013], [Bradley Hauer2013]
- Slovníkový útok [Bradley Hauer2013]
- RNN [Mikolov et al.2010]

Skórovacia funkcia

- **znakové n-gramy** - vierohodnosť, že text je generovaný Markovovským zdrojom

$$\frac{\sum_{i=0}^{t-n+1} log_2(f_i)}{t-n+1}$$

- **slovníkové ohodnotenie**
- **kompresia** - veľkosť skomprimovaného dešifrovaného textu [Noor R Al-Kazaz2018]

Entropia a Redundancia

- **Entropia jazyka** - množstvo informácie na 1 znak
  - angličtina 1.41, 1.19
  - slovenčina 1.64, 1.45
- **Redundancia jazyka** - rozdiel medzi počtom bitov na uloženie znaku a entropiou jazyka
  - angličtina 3.29, 3.565
  - slovenčina 3.819, 4.042

UNICITY DISTANCE

Vzdialenosť jednoznačnosti [Shannon1948]

- minimálne množstvo šifrového textu potrebné k jednoznačnému určeniu kľúča
- RXQQL $\in$ (HELLO, SILLY)
- $\min(n \in N | D_n \geq H(K))$
  - Jednoduchá substitúcia $= log_2(26!)/(4.7 - 1.41) \approx 27$
  - Playfair $= log_2(25!)/(4.7 - 1.41) \approx 26$
  - Stĺpcová $= log_2(10!)/(4.7 - 1.41) \approx 7$

Hranica lepšieho textu

- dobre znejúci text = text generovaný Markovovským zdrojom s dostatočne nenulovou pravdepodobnosťou
- dobre znejúcich textov dĺžky N: $2^{E_n \cdot N + O(\sqrt{N})}$
- existuje k kľúčov, najhorší prípad je, ak zodpovedajúce otvorené texty nekorelujú
- pravdepodobnosť, že 1 kľúč generuje dobrý text: $p = good/all$
- pravdepodobnosť, že v priestore generovanom kľúčmi sa nebude nachádzať dobrý text: $(1-p)^k$

Porovnanie odhadov hranice lepšieho textu a vzdialenosti jednoznačnosti

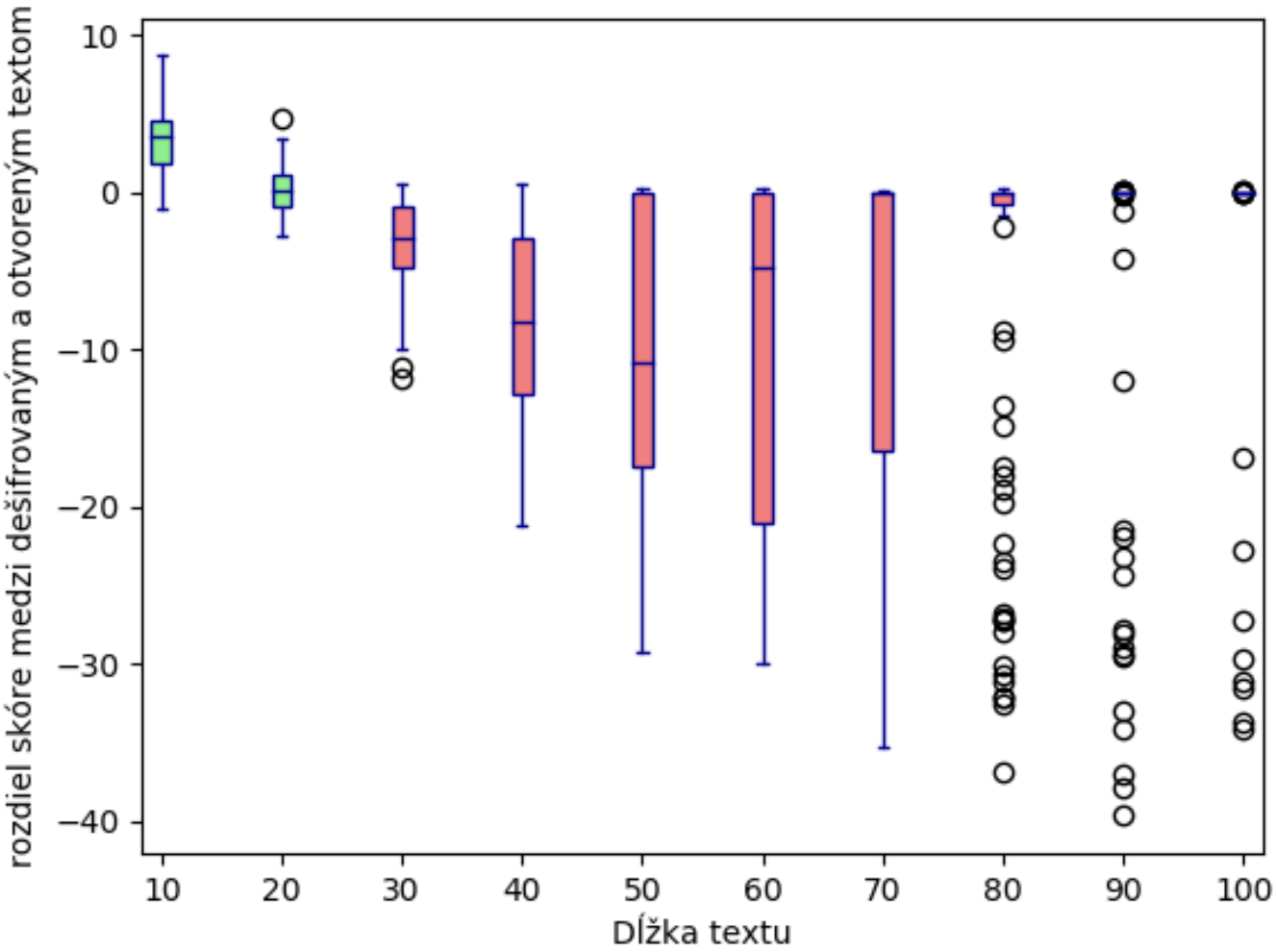
	UD	hran. lepšieho textu		
n-gram =		3	4	5
EN bez medzier	27	90	70	55
EN s medzerami	26	75	60	50
SK bez medzier	47	135	115	95
SK s medzerami	46	115	100	90

Praktické testy

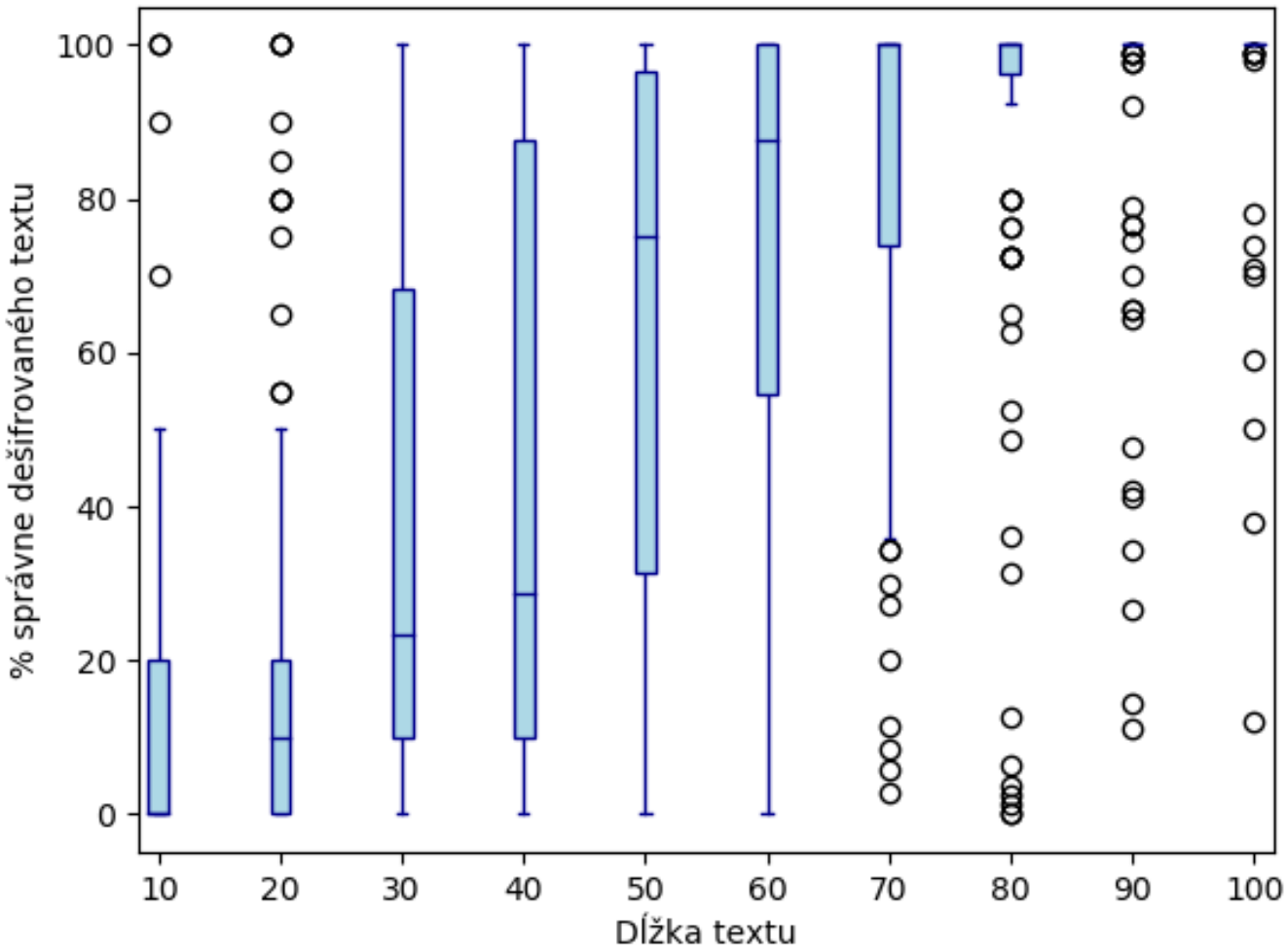
Dataset je očistený korpus wikipédie

- **Jazykový model** - abeceda, n-gramy (n, medzery, znaky/slová)
- **Typ šifry**
- **Heuristika a parametre pre ňu**
- **Dĺžka šifrového textu**

Rozdiel skóre dešifrovaného a otvoreného textu



Úspešnosť dešifrovania



Porovnanie teoretických a experimentálnych odhadov

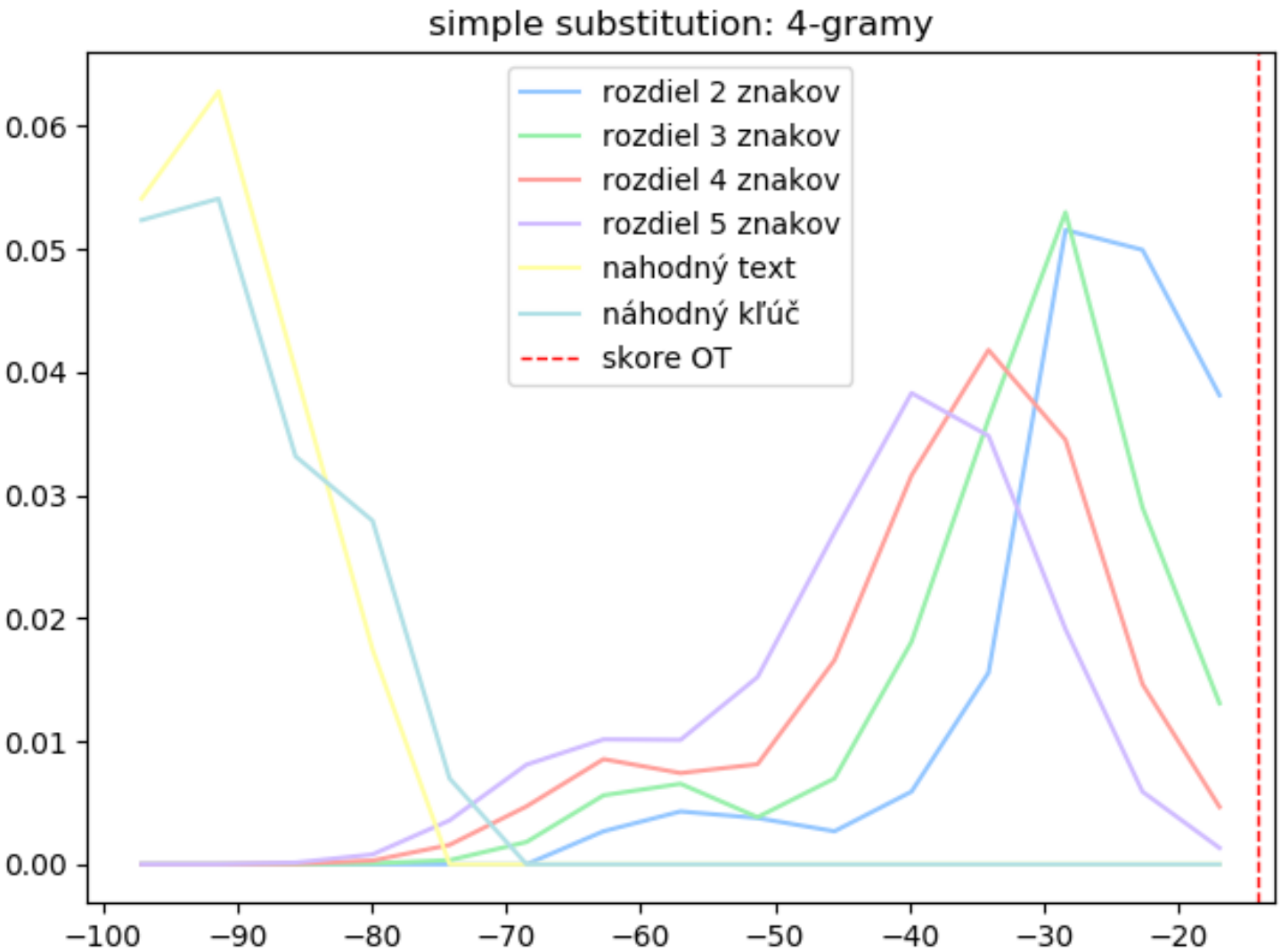
- Jednoduchá substitučná šifra
- EN bez medzier

n-gramy	Teória	medián úspešnosti pre rôzne dĺžky textov			
3	90	50 = 50%	60 = 70%	80 = 80%	100 = 90%
4	70	60 = 35%	70 = 50%	80 = 55%	90 = 65%
5	55	40 = 50%	50 = 70%	60 = 90%	70 = 100%

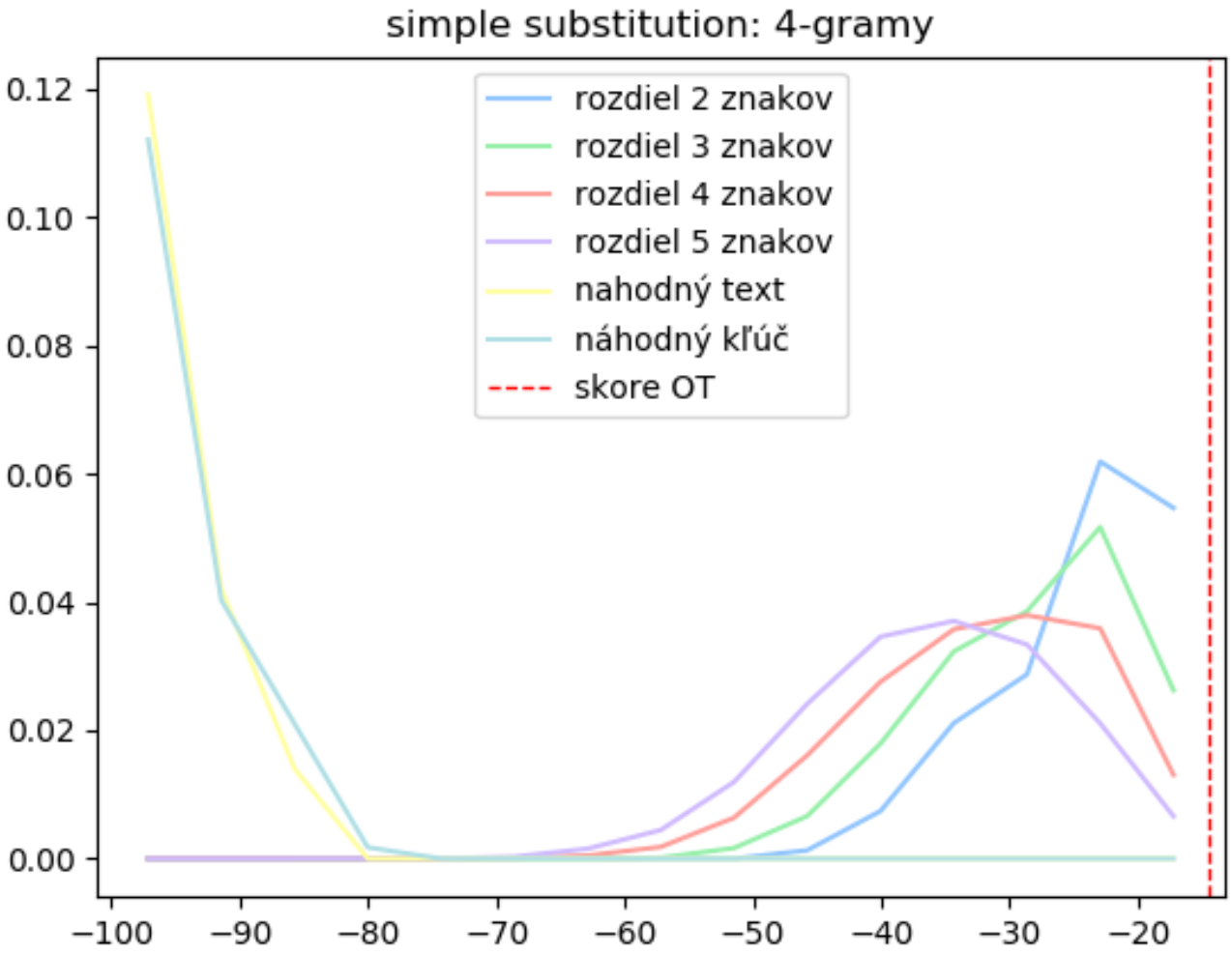
Analýza výsledkov

- rôzne stupne n-gramov
- typy šifier:
  - substitučná šifra
  - stĺpcová šifra
  - Playfair
- typy heuristík:
  - hill climbing
  - simulované žíhanie
  - brute force
- typy jazykových modelov:
  - anglický
  - slovenský

Spojitosť priestoru kľúčov



Spojitosť priestoru kľúčov



References I


Bradley Hauer, Ryan Hayward, G. K. (2013).
Solving substitution ciphers with combined language models.


Kevin Knight, Anish Nair, N. R. (2006).
Unsupervised analysis for decipherment problems.


Malte Nuhn, Julian Schamper, H. N. (2013).
Beam search for solving substitution ciphers.


Mikolov, T., Karafiát, M., Burget, L., Cernocký, J., and Khudanpur, S. (2010).
Recurrent neural network based language model.
volume 2, pages 1045–1048.


Noor R Al-Kazaz, Sean A Irvine, W. T. W. J. T. (2018).
An automatic cryptanalysis of playfair ciphers using compression.
dostupné z http://www.ep.liu.se/ecp/149/021/ecp18149021.pdf.

References II


Ravi, S. and Knight, K. (2008).
Attacking decipherment problems optimally with low-order n-gram models.


Shannon, C. E. (1948).
A mathematical theory of communication.
Nokia Bell Labs.


Sujith Ravi, K. K. (2011).
Bayesian inference for zodiac and other homophonic ciphers.

Ďakujem za pozornosť!