SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY
A INFORMATIKY

**Ing. Eugen Antal**

**Autoreferát dizertačnej práce**

# Moderná kryptoanalýza klasických šifier

na získanie vedecko-akademickej hodnosti
*philosophiae doctor, PhD.*

| | |
|---|---|
| **v doktorandskom študijnom programe:** | Aplikovaná informatika |
| **v študijnom odbore:** | 9.2.9 aplikovaná informatika |

**Bratislava 2017**

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

---

**Ing. Eugen Antal**

**Autoreferát dizertačnej práce**

# Moderná kryptoanalýza klasických šifier

na získanie vedecko-akademickej hodnosti
*philosophiae doctor, PhD.*

| | |
|---|---|
| **v doktorandskom študijnom programe:** | Aplikovaná informatika |
| **v študijnom odbore:** | 9.2.9 aplikovaná informatika |

**Bratislava 2017**

**Dizertačná práca bola vypracovaná:** v dennej forme doktorandského štúdia na Ústave informatiky a matematiky FEI STU v Bratislave.


**Predkladateľ:** Ing. Eugen Antal
FEI STU v Bratislave
Ilkovičova 3, 812 19 Bratislava

**Školiteľ:** prof. RNDr. Otokar Grošek, PhD.
FEI STU v Bratislave
Ilkovičova 3, 812 19 Bratislava

**Konzultant:** Mgr. Marek Sýs, PhD.
Masarykova univerzita
Katedra počítačových systémů a komunikací
Botanická 554/68a, 602 00 Brno

**Oponenti:** prof. RNDr. Jiří Pospíchal, DrSc.
Univerzita sv. Cyrila a Metoda
Katedra aplikovanej informatiky a matematiky
Nám. J. Herdu 2, 917 01 Trnava

doc. RNDr. Karol Macák, CSc.
Ministerstvo obrany SR


**Autoreferát bol rozoslaný dňa:** .....

**Obhajoba dizertačnej práce sa koná:** ..... o ..... hod.

**Na:** Fakulte elektrotechniky a informatiky STU,
Ilkovičova 3, 812 19 Bratislava
v .....

prof. Dr. Ing. Miloš Oravec
dekan FEI STU v Bratislave

# Obsah

# Úvod

Rýchly vývin výpočtových technológií umožnil v mnohých prípadoch modernú a rýchlu kryptoanalýzu klasických šifier. Napriek tomu, že väčšina klasických šifier neodolá moderným technikám počítačového lúštenia, existujú isté triedy klasických šifier, ktoré úspešne odolávajú aj najmodernejším postupom. Príkladom takýchto šifier sú homofónne substitučné šifry, ktoré v prípade dobrej konštrukcie odolávajú doposiaľ známym metódam počítačového lúštenia.

Optimalizačné algoritmy - nazývané aj ako meta-heuristiky - patria do skupiny moderných spôsobov riešenia zložitých problémov. V zjednodušenom chápaní sa jedná o prehľadávanie možných parametrov tzv. účelovej funkcie, ktoré predstavujú možné riešenia stanoveného problému. Cieľom prehľadávania je nájdenie tých parametrov funkcie, ktoré reprezentujú najlepšie riešenie - globálny extrém účelovej funkcie. Pod pojmom optimalizácia chápeme hľadanie extrému účelovej funkcie. Napriek tomu, že tieto metódy sa používajú väčšinou len na aproximáciu správneho riešenia (čiže nie na nájdenie najlepšieho konkrétneho riešenia, ale na nájdenie dostatočne dobrého), našli si svoje uplatnenie v širokom spektre rôznych tried ťažkých problémov. Vo väčšine prípadov sú tieto algoritmy založené na inteligentnom prehľadávaní veľkého priestoru riešení, alebo na aplikovaní rôznych prírodou inšpirovaných techník.

Principiálne sa jedná o transformáciu kryptoanalýzy na optimalizačný problém. Účelová funkcia v prípade lúštenia klasických šifier musí byť skonštruovaná tak, aby vyjadrovala mieru zmysluplnosti textu. Túto problematiku môžeme zaradiť do oblasti analýzy textu. Napriek tomu, že v súčastnosti sa považuje táto metodika za pomerne dobre preskúmanú, klasické šifry patria do triedy problémov, kde ostáva otvorených veľa otázok. Takéto otázky sú napr. ako správne skonštruovať účelovú funkciu, alebo ako správne transformovať lúštenie šifier na optimalizačný problém. V doterajších prácach absentuje aj hlbšia analýza kľúčových častí lúštenia ako aj popis ucelenej metodiky. V praktickej časti našej práce predkladáme preto nový ucelený prístup, ktorý by prispel k rozšíreniu súčasných možností počítačového lúštenia klasických šifier.

Výzvou doposiaľ zostávajú tie typy klasických šifier, v prípade ktorých lúštenie pomocou meta-heuristík nedáva dostatočne dobré výsledky. Jedným z nich je homofónna substitúcia, na ktorú v tomto kontexte nazeráme ako na vylepšenú verziu monoalfabetickej.

# 1 Ciele dizertačnej práce

Teoretická časť predkladanej práce obsahuje zhrnutie aktuálnych poznatkov z troch kľúčových oblastí:

- Kryptoanalýza klasických šifier (kapitola 1 dizertačnej práce).
- Analýza textu (kapitola 2 dizertačnej práce).
- Meta-heuristiky (kapitola 3 dizertačnej práce).

Na základe zistených nedostatkov súčasného stavu problematiky sme si stanovili nasledovné ciele dizertačnej práce:

- Vytvorenie ucelenej metodiky kryptoanalýzy klasických šifier pomocou meta-heuristík.
- Zhodnotenie možnosti efektívneho využitia meta-heuristík pri lúštení monoalfabetickej substitúcie.
- Vytvorenie nových postupov lúštenia homofónnej substitúcie.

# 2 Teória a metódy

Novým prístupom pri *kryptoanalýze* klasických šifier je prehľadávanie priestoru kľúčov daného kryptosystému pomocou meta-heuristík. Základným krokom tohto procesu je transformácia prehľadávania na optimalizačný problém. K tomu je potrebné, aby kryptoanalýza a prvky kryptosystému boli prevedené na prvky optimalizačného problému, ktorého najdôležitejšie časti sú reprezentácie kandidáta na riešenie $\theta$ a účelová funkcia $\mathcal{F}$. Po transformácií základných prvkov nasleduje voľba meta-heuristiky, ktorou chceme daný optimalizačný problém riešiť. Cieľom kryptoanalýzy je nájdenie tajného kľúča $k$ z $\mathcal{K}$. Kandidátom riešenia $\theta^c$ je teda kľúč, alebo množina kľúčov z $\mathcal{K}$. Priestor riešení $\Theta$ ($\mathcal{K}$) závisí od známeho šifrovacieho algoritmu. Pri kryptoanalýze vychádzame z niekoľkých faktov:

- Vstupom je známy zašifrovaný text $Y$.
- Šifrovací a dešifrovací algoritmus $e_k$ resp. $d_k$ sú tiež známe.

Dôležitou časťou je vyhodnotenie úspešnosti kandidátov pomocou účelovej funkcie $\mathcal{F}(\theta^c)$. Keďže samotný kľúč nie je možné priamo ohodnotiť, vhodnosť sa overí na základe dešifrovaného textu $X^c = d_k(Y, \theta^c)$ [5].

Na matematický popis vlastností prirodzených jazykov sa využívajú tzv. modely jazyka, v ktorých sú obsiahnuté (pre lúštenie) dôležité charakteristiky, tzv. referenčné hodnoty. Nami zvolené účelové funkcie $\mathcal{F}(\theta)$ porovnávajú podobnosť, resp. vzdialenosť zvolených kvantitatívnych charakteristík textu od stanovených referenčných hodnôt jazyka. Od voľby modelu jazyka závisí, aké charakteristiky budeme porovnávať. Zvolený model môže zvýšiť úspešnosť lúštenia, ale prináša aj obmedzenia. Najčastejšie použité modely jazyka pri kryptoanalýze klasických šifier sú Markovské modely [2, 11, 4, 7, 3] rádov $1, 2$ a $3$.

Účelové funkcie je potrebné skonštruovať tak, aby ohodnotili text z prirodzeného jazyka. Ohodnotenie textu spočíva v jeho porovnaní so štatistickými (kvantitatívnymi) charakteristikami jazyka [8] na základe stanoveného modelu. Vyhodnotenie úspešnosti kandidátov pomocou $\mathcal{F}(\theta)$ pri lúštení klasických šifier pozostáva z porovnania kvantitatívnych charakteristík kandidáta s referenčnými hodnotami. Porovnanie spočíva vo vyjadrení ich vzdialenosti alebo podobnosti. Zvolili sme nasledovnú množinu účelových funkcií $\mathbb{F} = \{\chi^2$, kosínusová podobnosť, Manhattanská vzdialenosť, Euklidovská vzdialenosť, Jensen-Shannonova divergencia$\}$.

Na ohodnotenie kvality účelových funkcií sme si stanovili nasledovné kritériá:

- Funkcia má priradiť najlepšie skóre správnemu riešeniu.
- Funkcia má vyjadrovať mieru vhodnosti, čo môžeme interpretovať ako percentuálna zhoda grafém a otvoreného textu.

Prvé kritérium sa vzťahuje k základnému predpokladu úspešného využitia meta-heuristík, t.j. dosiahnutie globálneho extrému účelovej funkcie. Druhé kritérium sa týka priebehu prehľadávania priestoru riešení a umožní zoradenie kandidátov podľa úspešnosti, v našom prípade zmysluplnosti textu. Vytvorenie účelovej funkcie na porovnanie kvality kandidátov je možné na základe dôležitej vlastnosti klasických šifier, ktorá sa nazýva *Utility of partial solution* [6, 5] (neplatí vo všeobecnosti). Táto vlastnosť spočíva v tom, že čiastočne správny kľúč produkuje čiastočne správny text, čo umožňuje aj samotné využitie optimalizačných algoritmov na lúštenie.

# 3 Dosiahnuté výsledky dizertačnej práce

Prvému a druhému cieľu dizertačnej práce sme sa venovali v kapitole 4. Najprv sme vytvorili ucelenú metodiku kryptoanalýzy s využitím meta-heuristík, ktorú sme demonštrovali pomocou lúštenia monoalfabetickej susbtitúcie. Na základe analýzy vybraných parametrov lúštenia (voľba modelu jazyka, voľba meta-heuristiky

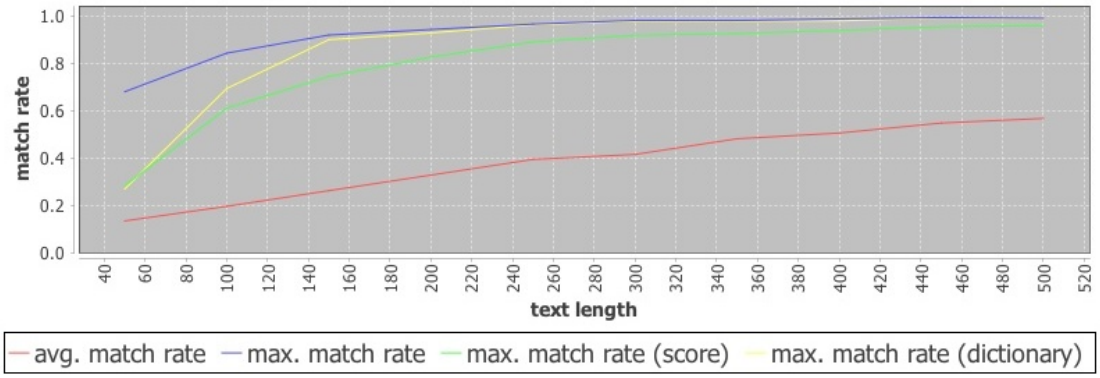
a voľba účelovej funkcie) a skúmania charakteru globálnej geometrie účelových funkcií, sme vytvorili odporúčania na dosiahnutie čo najlepších výsledkov a to aj v prípade lúštenia problematických krátkych textov. Najdôležitejšie zistenia a odporúčania sú nasledovné:

- Úspešnosť lúštenia monoalfabetickej substitúcie závisí hlavne od voľby modelu jazyka a od voľby účelovej funckie. Najvhodnejšia voľba je model jazyka založený na frekvencii 2-gramov (model $M_2$), a funkcie Manhatanská vzdialenosť (Manhattan) alebo Jensen-Shannonova divergencia (JSD).

- V prípade odporúčaného modelu $M_2$ globálny extrém účelových funkcií síce nepredstavuje správne riešenie, avšak nachádza sa v jeho blízkosti.

- V prípade modelu $M_2$ účelové funkcie Manhattan a JSD neobsahujú veľké neutrálne úseky (viacero možných riešení s rovnakým ohodnotením), obsahujú však väčší počet lokálnych extrémov v prípade kratších správ (do dĺžky 1000 znakov). Na riešenie tohto problému odporúčame využiť prírodou inšpirované meta-heuristiky DPSO, FFA alebo SAHC s reinicializáciou. Dôležité je pri tom dodatočné ohodnotenie výsledkov pomocou slovníka.

Najlepšie výsledky lúštenia sa nám podarilo dosiahnuť pomocou SAHC s reinicializáciou (Obr. 1). Priemernú zhodu grafém výsledku lúštenia so správnym riešením sme zvýšili už v prípade textov dĺžky 200 znakov na viac ako 90%, oproti doterajšiemu najlepšiemu výsledku 74% z [12]. V porovnaní s výsledkami z [12] to znamená dosiahnutie plne čitateľného textu.



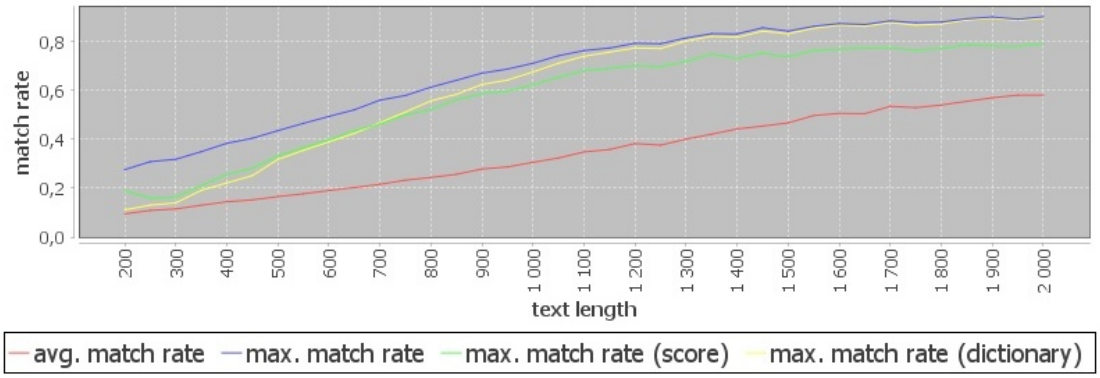

Obr. 1: Priemerná zhoda grafém výsledku lúštenia so správnym riešením pri reinicializácií (funkcia JSD)

Lúšteniu homofónnej substitúcie - čo bolo našim tretím cieľom - sme sa venovali v kapitole 5, v ktorej sme bližšie popísali vlastnosti homofónnej substitúcie. Ďalej sme skúmali možnosti vytvorenia jej reprezentácie (súčasť transformácie

kryptoanalýzy na optimalizačný problém) s využitím aj bez využitia poznatkov vyplývajúcich z konštrukcie šifry.

Pomocou odhadu štruktúry kľúča šifry sme vytvorili reprezentáciu (permutačný problém), vďaka ktorej sme boli schopní lúštiť homofónnu substitúciu až do počtu homofónov $n = |\mathcal{A}_c| = 50$, vrátane. Pri najmenšom skúmanom počte homofónov $n = 30$ sme dosiahli 80%-nú zhodu grafém so správnym výsledkom už od dĺžky textu 500 znakov. Pri $n = 40$ homofónov sme dosiahli rovnakú zhodu grafém so správnym výsledkom od dĺžky textu 1200 znakov a pri $n = 50$ od dĺžky textu 2000 znakov. Pre $n = 60$ homofónov sme neboli schopní dosiahnuť čitateľný text. V prípade menšieho počtu homofónov ($n = 30, 40$) sme našimi novými metódami dosiahli výsledky porovnateľné s doteraz najlepšími dosiahnutými výsledkami z fundamentálnej práce [3]. V prípade použitia väčšieho počtu homofónov ($n = 50, 60$) však už dosahujeme horšie výsledky.

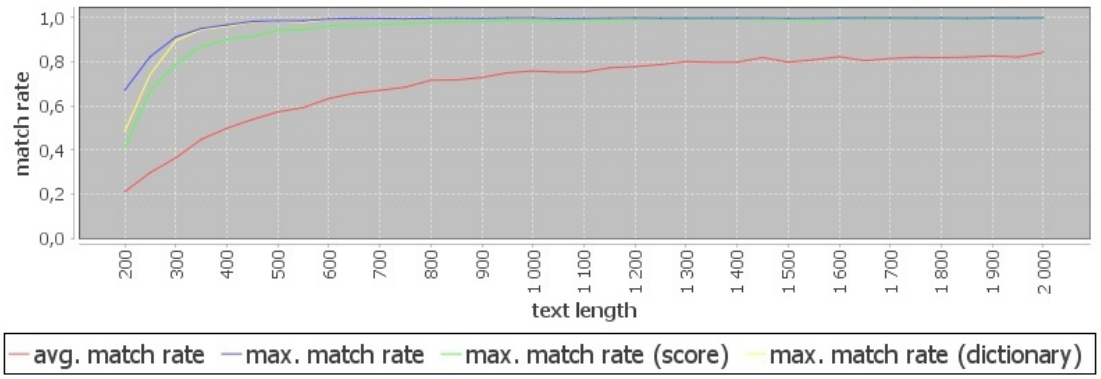
Ďalej sme ukázali, že v prípade rovnakej početnosti symbolov z príslušnej skupiny homofónov je možné rozšíriť metodiku o dodatočné ohodnotenie. Pomocou tohto ohodnotenia sa dá lúštiť aj homofónna substitúcia so zložitosťou $n = 60$ homofónov (s 80%-nou zhodou grafém so správnym výsledkom už pri textoch dĺžky 1200 znakov, Obr. 2). Dosiahnuté výsledky boli porovnateľne lepšie ako v [3] a to aj v prípade najväčšej skúmanej zložitosti.




Obr. 2: Priemerná zhoda grafém výsledku lúštenia so správnym riešením pri reinicializácií ($n = 60$, funkcia Manhattan)

V prípade špeciálnej konštrukcie šifry (keď sa všetky symboly cyklicky striedajú z príslušnej skupiny homofónov) sme vytvorili postup, pomocou ktorého je možné homofónnu substitúciu redukovať na monoalfabetickú a následne využiť metodiku a odporúčania z kapitoly 4. Hľadanie homofónov s cyklickou štruktúrou sme transformovali na problém hľadania klík v grafe, využili sme pri tom Bron–Kerboschov algoritmus. V tomto prípade sme dosiahli 90%-nú zhodu grafém so správnym výsledkom už aj v prípade veľmi krátkych textov, t.j. textov dĺžky 300 znakov pri zložitosti $n = 60$ homofónov (Obr. 3). Podobnú úspešnosť v [3] dosiahli len

pri textoch dlhších ako 3000 znakov v prípade nižšej zložitosti $n = 55$ homofónov (nevyužívali analýzu cyklickej štruktúry homofónov). V prípade textov dĺžky 300 znakov dosiahli len okolo 10%-nú zhodu grafém so správnym výsledkom.




Obr. 3: Priemerná zhoda grafém výsledku lúštenia so správnym riešením pri reinicializácií (po redukcii z $n = 60$; funkcia Manhattan)

Správne fungovanie nami vytvorenej metodiky sme overili lúštením reálnych šifier získaných z archívov a z rôznych publikácií, konkrétne: Gentlemen's cipher, dve šifrované správy z amerických prezidentských volieb z roku 1876, jedna šifrovaná správa z tridsaťročnej vojny a Zodiac-ova šifra Z408. Úspešnosť lúštenia monoalfabetických substitúcií v prípade textov dĺžky aspoň 200 znakov, kde sme mali možnosť overiť správnosť lúštenia bola viac ako 90%-ná. Pri správe, kde sme nemali k dispozícii otvorený text, sme dosiahli plne čitateľný text. Úspešnosť lúštenia homofónnej substitúcie (šifry Z408) bola porovnateľná s očakávaným výsledkom danej zložitosti ($n = 54$, dĺžka textu 408 znakov). Zhodu grafém výsledku lúštenia so správnym riešením sa nám podarilo zvýšiť na 48.2% využitím cyklickej štruktúry homofónov.

V uvedených výsledkoch sme ukázali, akým postupom je možné dosiahnuť priaznivé výsledky pri lúštení monoalfabetickej a homofónnej substitúcie. Problémom však ostáva lúštenie homofónnej substitúcie, v ktorej nie je možné využiť cyklickú štruktúru homofónov. V takomto prípade je lúštenie krátkych správ (do dĺžky 1000 znakov) problémové a to hlavne v prípade väčšieho počtu homofónov ($n = 40, 50, 60$). Za hlavný prínos práce považujeme nami vytvorenú ucelenú metodiku lúštenia klasických šifier pomocou optimalizačných algoritmov. Táto metodika, spoločne s vykonanými experimentmi, je zdrojom nových informácií potrebných pre vhodné použitie meta-heuristík pri lúštení. Zistené poznatky nám umožnili zvýšenie úspešnosti lúštenia problematických krátkych textov oproti doterajším prácam a sú perspektívnym podkladom aj pre ďalší rozvoj výskumu.

# 4 Literatúra


[1] Banks, M. J.: *A Search-Based Tool for the Automated Cryptanalysis of Classical Ciphers. The University of York Department of Computer Science*, 2008.

[2] Clark, A. J.: *Optimisation Heuristics for Cryptology.* PhD. thesis, Queensland University of Technology, 1998.

[3] Dhavare, A.; Low, R. M.; Stamp, M.: Efficient Cryptanalysis of Homophonic Substitution Ciphers. *Cryptologia*, ročník 37, č. 3, 2013: s. 250–281.

[4] Forsyth, W. S.; Safavi-Naini, R.: *Automated Cryptanalysis of Substitution Ciphers. Cryptologia*, volume 17, n. 4, 1993: pp. 407–418.

[5] Ganesan, R.; Sherman, A.: Statistical Techniques for Language Recognition: An Introduction and Guide for Cryptanalysts. 1993, [cit: 2015-08-07], Dostupné na internete: `http://web.cecs.pdx.edu/~bart/decrypter/gs93.pdf`.

[6] Hilton, R.: Automated Cryptanalysis of Monoalphabetic Substitution Ciphers Using Stochastic Optimization Algorithms. 2012, [cit: 2015-08-08], Dostupné na internete: `http://cse.ucdenver.edu/~rhilton/docs/Cryptanalysis-Against-Monosub-Ciphers.pdf`.

[7] Jakobsen, T.: *A Fast Method for the Cryptanalysis of Substitution Ciphers. Cryptologia*, volume 19, n. 3, 1995: pp. 265–274.

[8] Kullback, S.: *Statistical Methods in Cryptanalysis. Aegean Park Press*, 1976: pp. 206.

[9] Matthews, R. A. J.: *The Use of Genetic Algorithms in Cryptanalysis. Cryptologia*, volume 17, n. 2, 1993: pp. 187–201.

[10] Russell, M. D.; Clark, J. A.; Stepney, S.: *Making the Most of Two Heuristics: Breaking Transposition Ciphers with Ants. CEC 03*, volume 4, 2003: pp. 2653 – 2658.

[11] Spillman, R.; Janssen, M.; Nelson, B.: *Use of a Genetic Algorithm in the Cryptanalysis of Simple Substitution Cihers. Cryptologia*, volume 17, n. 1, 1993: pp. 31–44.

[12] Vobbilisetty, R.; Troia, F. D.; Low, R. M.; aj.: Classic cryptanalysis using hidden Markov models. *to appear Cryptologia*: s. 1–28.

# 5 Zoznam prác dizertanta

**Vedecké práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS**

ANTAL, Eugen - ZAJAC, Pavol. Key Space and Period of Fialka M-125 Cipher Machine. In Cryptologia. Vol. 39, No. 2 (2015), s. 126-144. ISSN 0161-1194. V databáze: WOS; SCOPUS.

ANTAL, Eugen - GROŠEK, Otokar - HORAK, Peter. On a Mnemonic Construction of Permutations. In Journal of Mathematical Cryptology. Prijaté 25.01.2017. V databáze: SCOPUS.

**Vedecké práce v domácich časopisoch registrovaných v databázach Web of Science alebo SCOPUS**

ANTAL, Eugen - HROMADA, Viliam . A New Stream Cipher Based on Fialka M-125. In Tatra Mountains Mathematical Publications. Vol. 57, Iss. 4 (2013), s.101-118. ISSN 1210-3195. V databáze: SCOPUS.

ANTAL, Eugen - HROMADA, Viliam . A micro-controller implementation of a FIALKA M-125 based stream cipher. In Tatra Mountains Mathematical Publications. Vol. 60, (2014), Issue: 1, s. 101-116. ISSN 1210-3195. V databáze: SCOPUS.

**Ostatné publikácie**

ANTAL, Eugen - VARGA, Juraj . Zodiac. In Mikulášská kryptobesídka 2010 : Sborník příspěvků. Praha, 2.-3.12.2010. Praha : Trusted Network Solutions, 2010, s.89-90. ISBN 978-80-904257-1-2.

ANTAL, Eugen. Fialka M-125. In Mikulášská kryptobesídka 2010 : Sborník příspěvků. Praha, 2.-3.12.2010. Praha : Trusted Network Solutions, 2010, , s.87-88. ISBN 978-80-904257-1-2.

ANTAL, Eugen. Nature-inspired heuristic methods in classical cipher cryptanalysis. In Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 25-33. ISBN 978-80-227-4541-3.

ANTAL, Eugen - GROŠEK, Otokar. Fialka M-125. In ŠVOČ 2009 : Študentská vedecká a odborná činnosť. Zborník víťazných prác. Bratislava, Slovak Republic, 29.4.2009. Bratislava : STU v Bratislave FEI, 2009, s.CD-Rom. ISBN 978-80-227-3094-5.

ANTAL, Eugen. Computer Processing of the Rohonczi Codex. In ELITECH' 12 [elektronický zdroj] : 14th Conference of Doctoral Students. Bratislava, Slovak Republic, 22 May 2012. Bratislava : Nakladateľstvo STU, 2012, s.CD-ROM, [5] s. ISBN 978-80-227-3705-0.

ANTAL, Eugen - SÝS, Marek - VARGA, Juraj. Evaluation Functions in the Cryptoanalysis of Homophonic Substitution. In ISCAMI 2012 : Book of abstracts. Malenovice, Czech Republic, 10.-13.5.2012. Ostrava : University of Ostrava, 2012, s.12.

ANTAL, Eugen - JÓKAY, Matúš. Rotorový šifrátor Fialka M-125. Diel 1. Popis šifrátora. In Crypto-World. Roč. 13, č. 4 (2011), s.18-27. ISSN 1801-2140.

ANTAL, Eugen - JÓKAY, Matúš. Rotorový šifrátor Fialka M-125. Úvod k seriálu. In Crypto-World. Roč. 13, č. 4 (2011), s.17. ISSN 1801-2140.

ANTAL, Eugen - JÓKAY, Matúš. Rotorový šifrátor Fialka M-125. Diel 2. Porovnanie s viacerými rotorovými šifrátormi. In Crypto-World. Roč. 13, č. 5 (2011), s.15-23. ISSN 1801-2140.

ANTAL, Eugen - JÓKAY, Matúš. Rotorový šifrátor Fialka M-125. Diel 4: Implementácia a možnosti využitia. In Crypto-World. Roč. 13, č. 9 (2011), s.9-15. ISSN 1801-2140.

ANTAL, Eugen - JÓKAY, Matúš. Rotorový šifrátor Fialka M-125. Diel 3. Vybrané vlastnosti šifry. In Crypto-World. Roč. 13, č. 6 (2011), s.23-32. ISSN 1801-2140.

ANTAL, Eugen. Záhada kódexu Rohonczi. In Crypto-World. Roč. 14, č. 9-10 (2012), s.21-28. ISSN 1801-2140.

ANTAL, Eugen - ZAJAC, Pavol. Analýza Rabenhauptovho zašifrovaného dopisu. In Crypto-World. Roč. 15, č. 11-12 (2013), s.9-17. ISSN 1801-2140.

ANTAL, Eugen. Modern cryptanalysis of classical ciphers. In CECC 2016 : The 16th central european conference on cryptology. Piestany, Slovakia. June 22 - 24, 2016. Bratislava : STU, 2016, S. 29-33.

ANTAL, Eugen - SÝS, Marek. Solving Homophonic Cipher Using Heuristic Methods. In ISCAMI 2013 : Book of abstracts. Malenovice, Czech Republic, May 2-5, 2013. Ostrava : University of Ostrava, 2013, s.9.

ANTAL, Eugen - SÝS, Marek. Nature-inspired heuristic methods in classical cipher cryptanalysis. In ISCAMI 2014 : book of abstracts. Malenovice, ČR, 27. - 30. 3. 2014. 1. vyd. Ostrava : Ostravská univerzita, 2014, s. 9.

ANTAL, Eugen. Lightweight Cipher Based on FIALKA M-125 Design. In Central European Conference on Cryptology 2013 : Telč, Czech Republic, June 26-28, 2013. Brno : Masaryk University, 2013, s.1.

**Rôzne publikácie v spoluatorstve so študentmi**

ANTAL, Eugen - BARANEC, František. Techniky získavania citlivých údajov z Apple iOS zariadení. In 43. konference EurOpen.CZ : Vranov, Czech Republik; 29. 9.-2.10.2013. Plzeň : EurOpen.CZ, 2013, s.21-32. ISBN 978-80-86583-26-6.

SOVIČ, Tomáš - ANTAL, Eugen . Comparison of selected rotor ciphers. In Mikulášská kryptobesídka 2016 : sborník příspěvků. Praha, ČR, 1. - 2. 12. 2016. 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2016, S. 41-42. ISBN 978-80-904257-8-1.

BARANEC, František - ANTAL, Eugen. Forenzná analýza iOS. In ŠVOČ 2013 [elektronický zdroj] : Zborník vybraných prác, Bratislava, 23. apríl 2013. 1. vyd. Bratislava : FEI STU, 2013, s.CD ROM, s. 19-21. ISBN 978-80-227-3909-2.

JACKULIAK, Daniel - ANTAL, Eugen. Lúštenie vybraných substitučných šifier pomocou SWARM intelligence. In ŠVOČ 2014 [elektronický zdroj] : Zborník vybraných prác 2014, Bratislava, 29. apríl 2014. 1.vyd. Bratislava : FEI STU, 2014, CD-ROM, s. 15-20. ISBN 978-80-227-5154-5.

KANIČÁR, Martin - ANTAL, Eugen. Lúštenie homofónnej substitúcie pomocou genetických algoritmov. In ŠVOČ 2013 [elektronický zdroj] : Zborník vybraných prác, Bratislava, 23. apríl 2013. 1. vyd. Bratislava : FEI STU, 2013, s.CD ROM, s. 6-9. ISBN 978-80-227-3909-2.

## 5.1 Ohlasy a citácie (bez autocitácií)

Stephen Budiansky v knihe *Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union* cituje článok *Key Space and Period of Fialka M-125 Cipher Machine*.

Pavol Zajac v článku *On insecurity of 4-round Feistel ciphers* cituje článok *A New Stream Cipher Based on Fialka M-125*.

NSA's National Cryptologic Museum Library uvádza článok *Key Space and Period of Fialka M-125 Cipher Machine* v katalógu publikácií:
"The Museum Library maintains a collection of unclassified and declassified books and documents relating to every aspect of cryptology. The books and records complement the museum exhibits and artifacts, but also offer unique and in-depth sources of information for researchers."

## 5.2 Aktívna prezentácia výsledkov a prednášky

Miesto: Prednáška z predmetu klasické šifry, FEI STU, Bratislava
Rok: 2012 - 2015
Príspevky: Rotorový šifrátor Fialka M-125; Počítačové lúštenie klasických šifier; Rotorové šifrovacie stroje

Miesto: ISCAMI 2012 (International Student Conference on Applied Mathematics and Informatics), Malenovice, CZ
Rok: 2012
Príspevok: Evaluation functions in the cryptoanalysis of homophonic substitution

Miesto: Elitech 2012, FEI STU, Bratislava
Rok: 2012
Príspevok: Computer processing of the Rohonczi codex

Miesto: Seminár CRYPTO, FEI STU, Bratislava
Rok: 2012
Príspevok: Záhada kódexu Rohonczi

Miesto: Seminár CRYPTO, FEI STU, Bratislava
Rok: 2013
Príspevok: Lúštenie Hillovej šifry

Miesto: Seminár CRYPTO, FEI STU, Bratislava
Rok: 2013
Príspevok: Lúštenie šifry (Rabenhaupt) zo 17. storočia

Miesto: ISCAMI 2013 (International Student Conference on Applied Mathematics and Informatics), Malenovice, CZ
Rok: 2013
Príspevok: Solving homophonic cipher using heuristic methods

Miesto: EurOpen, Vranov nad Dyjí, CZ
Rok: 2013
Príspevok: Techniky získavania citlivých údajov z Apple iOS zariadení

Miesto: CECC 2013 (Central European Conference on Cryptology), Telč, CZ
Rok: 2013
Príspevok: Lightweight cipher based on FIALKA M-125 design

Miesto: ISCAMI 2014 (International Student Conference on Applied Mathematics and Informatics), Malenovice, CZ
Rok: 2014
Príspevok: Nature-inspired heuristic methods in classical cipher cryptanalysis

Miesto: MKB 2014 (konferencia Mikulášská kryptobesídka), Praha, CZ
Rok: 2014
Príspevok: Preliminary analysis of the Rohoncz codex (rump session)

Miesto: Prednáška pre študentov z USA (v rámci projektu NATO SPS 984520), FEI STU, Bratislava
Rok: 2014
Príspevok: Nature-inspired heuristic methods in classical cipher cryptanalysis

Miesto: Prednáška pre študentov z Nórska (v rámci projektu EEA Grant SK06-IV-01-001), FEI STU, Bratislava
Rok: 2015
Príspevok: Nature-inspired heuristic methods in classical cipher cryptanalysis

Miesto: Norwegian-Slovakian Workshop in Crypto, Bergen, Nórsko
Rok: 2016
Príspevok: Nature-inspired heuristic methods in classical cipher cryptanalysis

Miesto: Seminár CRYPTO, FEI STU, Bratislava
Rok: 2016
Príspevok: 2ND historic ciphers colloquium, 2016 Kassel

Miesto: CECC 2016 (Central European Conference on Cryptology), Pieštany
Rok: 2016
Príspevok: Modern cryptanalysis of classical ciphers

# Summary

At the beginning, this dissertation summarizes the state of the art of modern cryptanalysis of classical ciphers by meta-heuristics. In more details, this part is divided into 3 parts, namely introduction to the problem, text analysis and meta-heuristics.

The transformation of cryptanalytical task to an optimization problem, and the choice of a suitable fitness function form an important part of the topic included in Chapter 4. We demonstrate our methodology by solving a monoalphabetic substitution. We achieved our best results by Steepest Ascent Hill Climbing (SAHC) meta-heuristic with reinitialization. The average achieved match rate with the correct solution was more than 90% for texts of length 200 letters. This is an improvement in comparison with the best known result 74% from [12].

We found out that the success rate of solving a monoalphabetic substitution depends mainly on the selected language model and fitness function. We recommend to choose a bigram language model ($M_2$), and fitness function Manhattan distance (Manhattan) or Jensen-Shannon's divergence (JSD). In case of the $M_2$ language model the global optimum of the fitness function does not represent the correct solution, but it is very close to it. Fitness functions Manhattan and JSD, in case of the $M_2$ language model, do not contain large neutral areas, but contain a lot of local optimas (up to texts of length 1000 letters). This problem can be solved by selecting nature-inspired heuristics DPSO, FFA or by selecting SAHC heuristic with reinitialization.

The next part is devoted to cryptanalysis of a homophonic substitution (Chapter 5). We investigated how to utilize the information achieved from the cipher's construction in the cryptanalysis. Based on the cipher's key structure we can construct a representation where we can successfully solve homophonic substitution up to 60 homophones. We were able to highly improve our success rate by expanding our method with an additional evaluation. The achieved results were better than those presented in [3]. Moreover in case of cyclic homophones we were able to create a method where the homophonic substitution is reduced into a monoalphabetic. We transformed the problem of finding cyclic homophones into a clique finding graph problem. We were able to achieve 90% match rate with the correct solution also for very short texts (from length of 300 letters) in case of 60 homophones.

To verify the quality of proposed methodology in practice, we present the results (Chapter 6) by breaking several selected substitution ciphers from various sources, e.g. the Gentlemen's Cipher, two cryptograms from the US presidential election of 1876, cryptogram form the Thirty Years War, and the Zodiac Z408 cipher.