

## 2013

### Crypto-World 1-2/2013

- A. Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni, část II. (J.Mírka) 2 -12
- B. Lúštitelia historických šifriér - A.V. Maloch a Josef Šusta (J. Krajčovič) 13 - 21
- C. Elektronický podpis v praxi (P.Vondruška, J.Peterka) 22
- D. SOOM.cz - Hacking & Security konference #2 (R.Kümmel) 23
- E. Security and Protection of Information 2013 (předběžná informace) 24 - 25
- F. O čem jsme psali za posledních 12 měsíců 26 - 27
- G. Závěrečné informace 28

Příloha: Obrazová příloha k části II. Mírka, J.: Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni

<http://crypto-world.info/casop15/obr2.zip>

### Crypto-World 3-4/2013

- A. Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni, část III. (J.Mírka) 2 -14
- B. Andreas Figl – rakúsky dôstojník a kryptológ (J.Kollár) 15 - 23
- C. Central European Conference on Cryptology 2013 24
- D. call for papers - CYBERSPACE 2013 25 - 26
- E. O čem jsme psali za posledních 12 měsíců 27 - 28
- F. Závěrečné informace 29

Příloha: Obrazová příloha k části III. Mírka, J.: Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni

<http://crypto-world.info/casop15/obr3.zip>

### Crypto-World 5-6/2013

- A. Konec aktualit v Crypto-News a Bezpečnostních střípků (J.Pinkava) 2
- B. Tajomstvo šifrovacieho stroja G. W. Leibniza (J.Krajčovič) 3 – 11
- C. Kaspersky Lab odhalila novou kyberšpionážní operaci NetTraveler 12
- D. Reakcia na článok „Andreas Figl – rakúsky dôstojník a kryptológ“ (J.Krajčovič) 13 – 15
- E. Cvičný CISSP test z kryptografie 16 – 18
- F. Central European Conference on Cryptology 2013 26.-28. června, Telč 19 – 20
- G. Call for Papers Mikulášská kryptobesídka 21
- H. O čem jsme psali za posledních 12 měsíců 22
- I. Závěrečné informace 23

### Crypto-World 7-8/2013

- A. Reino Häyhänen – sovietsky špión (J. Kollár) 2 – 9
- B. Dosud nevyluštný dopis českého pobělohorského emigranta Karla Rabenhaupta ze Suché z doby třicetileté války. (Soutěž o ceny) (J. Mírka) 10 – 18
- C. Soutěž 2013, luštění originálního šifrovaného dopisu ze 17. století (P.Vondruška) 19 – 21
- D. Diskrétní logaritmus a metody jeho výpočtu (J. Pulec) 22 – 26
- E. Kaspersky v Praze - Kybernetické zbraně jsou nejhorším vynálezem století 27 – 28
- F. Pozvánka k podzimním kurzům Akademie CZ NIC 29 – 31
- G. O čem jsme psali za posledních 12 měsíců 32 – 33
- H. Závěrečné informace 34

### **Crypto-World 9-10/2013**

- |    |  |         |
|----|--|---------|
| A. | Sovietska šifra VIC (J.Kollár)   | 2 – 16  |
| B. | Prolamování hash otisků (R.Kümmel)   | 17 – 24 |
| C. | Upoutávka na knihu K.Burdy – Aplikovaná kryptografie   | 25      |
| D. | Soutěž v luštění / Dosud nevyluštěný dopis českého pobělohorského emigranta Karla Rabenhaupta ze Suché z doby třicetileté války (J.Mírka, P.Vondruška) | 26 – 27 |
| E. | O čem jsme psali za posledních 12 měsíců   | 28 – 29 |
| F. | Závěrečné informace  | 29      |

Příloha: ukázka z knihy Aplikovaná kryptografie

[http://crypto-world.info/casop15/Burda\\_akryptografie.pdf](http://crypto-world.info/casop15/Burda_akryptografie.pdf)

### **Crypto-World 11-12/2013**

- |    |  |         |
|----|--|---------|
| A. | Ukládání hesel bezpečně (J.Vrána)                              | 2 - 3   |
| B. | Nomenklátory 17. a 18. století (J.Mírka, P.Vondruška)          | 4 - 6   |
| C. | Letošní soutěž v luštění skončila – výsledky (P.Vondruška)     | 7 - 8   |
| D. | Analýza Rabenhauptovho zašifrovaného dopisu (E.Antal, P.Zajac) | 9 – 17  |
| E. | PF 2013 (P.Vondruška)  | 18      |
| F. | O čem jsme psali za posledních 12 měsíců                       | 19 – 20 |
| G. | Závěrečné informace  | 21      |

Příloha k článku D: [http://web.telecom.cz/depotpv/ASD12/priloha\\_k\\_D.zip](http://web.telecom.cz/depotpv/ASD12/priloha_k_D.zip)