

2011

Crypto-World 1/2011

| | | |
|----|---|-------|
| A. | Seriál Československé šifry z období 2. světové vojny (J.Kollár) 2 | |
| B. | Československé šifry z období 2. světové vojny, Díl 1., Šifra TTS (J.Kollár) | 3-11 |
| C. | Nové užitečné statistické testy (V.Klíma) | 12-13 |
| D. | Československý šifrátor MAGDA – dodatek k popisu v e-zinu Crypto-World 5/2007 (K.Šklíba) | 14-15 |
| E. | Báječný svět elektronického podpisu J.Peterky | 16 |
| F. | Poslední výzva k příspěvku na mezinárodní konferenci Security and Protection of Information konanou 10.– 12. května v Brně (J.Dočkal) | 17-18 |
| G. | Problematika infrastruktury veřejných klíčů (PKI), dvoudenní kurz Akademie CZ.NIC (P.Vondruška) | 19-20 |
| H. | O čem jsme psali v lednu 1999-2010 | 21-22 |
| I. | Závěrečné informace | 23 |

Crypto-World 2/2011

| | | |
|----|--|---------|
| A. | Československé šifry z období 2. světové vojny Díl 2., Šifra „Římska dva“ (J.Kollár) | 2 - 11 |
| B. | Pár poznámek k šifře použité v deníku Karla Hynka Máchy (P.Vondruška) | 12 - 20 |
| C. | O čem jsme psali v únoru 1999-2010 | 21 - 22 |
| D. | Závěrečné informace | 23 |

Crypto-World 3/2011

| | | |
|----|--|---------|
| A. | Československé šifry z období 2. světové vojny Díl 3., Šifra „Římska osm“ (J.Kollár) | 2 - 12 |
| B. | Blinkry blikají aneb komentář ke zprávě NISTu o výběru finalistů SHA-3 (V.Klíma) | 13 - 16 |
| C. | Charakteristiky Booleovských funkcí osmi proměnných (P.Tesař) | 17 – 22 |
| D. | Odborná skupina kryptologie při JČMF (J.Hrubý) | 23 - 24 |
| E. | O čem jsme psali v březnu 2000-2010 | 25 - 26 |
| F. | Závěrečné informace | 27 |

Crypto-World 4/2011

| | | |
|----|---|---------|
| A. | Československé šifry z období 2. světové vojny Díl 4., Šifra „Římska devět“ (J.Kollár) | 2 - 16 |
| B. | Rotorový šifrátor Fialka M-125, Úvod k seriálu (E.Antal, M.Jókay) | 17 |
| C. | Rotorový šifrátor Fialka M-125, Díl 1., Popis šifrátoru (E.Antal, M.Jókay) | 18 – 27 |
| D. | Problematika infrastruktury veřejných klíčů (PKI), dvoudenní kurz Akademie CZ.NIC (P.Vondruška) | 28 - 29 |
| E. | O čem jsme psali v dubnu 2000 – 2010 | 30 – 31 |
| F. | Závěrečné informace | 32 |

Crypto-World 5/2011

| | | |
|----|---|---------|
| A. | Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 5., Šifra „Rímska desiat“ (J.Kollár) | 2 - 13 |
| B. | Vzpomínky a poznámky čtenáře k tématu Fialka M-125 (J.Knížek) | 14 |
| C. | Rotorový šifrátor Fialka M-125, Diel 2., Porovnanie s viacerimi rotorovými sifratormi (E.Antal, M.Jókay) | 15 – 23 |
| D. | Call for Papers Mikulášská kryptobesídka | 24 |
| E. | O čem jsme psali v květnu 2000 – 2010 | 25 - 26 |
| F. | Závěrečné informace | 27 |

Crypto-World 6/2011

| | | |
|----|--|---------|
| A. | Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 6., Šifra „Rímska trinásť“ (J.Kollár) | 2 - 11 |
| B. | Kryptografický softwarový nástroj CipherCAD a kryptoanalýza (V.Klíma, V.Plátěnka) | 12 - 22 |
| C. | Rotorový šifrátor Fialka M-125, Diel 3., Vybrané vlastnosti šifry (E.Antal, M.Jókay) | 23 – 32 |
| D. | Keymaker – studentská soutěž | 33 |
| E. | Konference EUROOPEN 2011 | 34 |
| F. | O čem jsme psali v červnu 2000 – 2010 | 35 - 36 |
| G. | Závěrečné informace | 37 |

Crypto-World 78/2011

| | | |
|----|--|---------|
| A. | Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 7., Šifra „Eva“ (J.Kollár) | 2 - 9 |
| B. | sCrib – Hardwarový správce hesel aneb kapesní Enigma (D.Cvrček) | 10 - 13 |
| C. | Problematika infrastruktury veřejných klíčů (PKI), dvoudenní kurz Akademie CZ.NIC (P.Vondruška) | 14 - 15 |
| D. | Keymaker – studentská soutěž | 16 |
| E. | O čem jsme psali v létě 2000 – 2010 | 17 - 19 |
| F. | Závěrečné informace | 20 |

Crypto-World 9/2011

| | | |
|----|--|---------|
| A. | Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 8., Šifra „Marta“ (J.Kollár) | 2 - 8 |
| B. | Rotorový šifrátor Fialka M-125, Diel 4., Implementácia a možnosti využitia (E.Antal, M.Jókay) | 9 – 15 |
| C. | Stále mám přístup k dalším CA, tvrdí útočník na DigiNotar (J.Pinkava) | 16 - 22 |
| D. | Soutěž 2011 (P.Vondruška) | 23 |
| E. | O čem jsme psali v září 2000 – 2010 | 24 - 26 |
| F. | Závěrečné informace | 27 |

Crypto-World 10/2011

- | | | |
|----|--|---------|
| A. | Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 9., Šifra „Růžena“ (J.Kollár) | 2 - 12 |
| B. | Soutěž 2011 (P.Vondruška) | 13 -14 |
| C. | CryptoWars I. (P.Vondruška) | 16 - 20 |
| D. | O čem jsme psali v zříjnu 2000 – 2010 | 21 - 22 |
| E. | Závěrečné informace | 23 |

Crypto-World 11/2011

nevyšel

Crypto-World 12/2011

nevyšel