

2007

Crypto-World 1/2007

A.	Osobní doklady x identifikace, autentizace, autorizace (L.Dostálek, M.Hojsík)	2-5
B.	Bezpečnost elektronických pasů, část II. (Z.Říha, P.Švenda, V.Matyáš)	6-12
C.	XML bezpečnost, část I. (D. Brechlerová)	13-25
D.	Elektronická fakturace (L.Dostálek, M.Hojsík)	26-33
E.	O čem jsme psali v lednu 2000 -2006	34
F.	Závěrečné informace	35

Crypto-World 2/2007

A.	Najväčšia tma je pod lampou – STEGANOGRAFIA, část I. (R.Cinkais)	2-9
B.	XML bezpečnost, část II. (D. Brechlerová)	10-20
C.	Přehled dokumentů ETSI v oblasti elektronického podpisu, časových razítek a kvalifikovaných certifikátů (V.Sudzina)	21-22
D.	O čem jsme psali v únoru 2000 - 2006	23-24
E.	Závěrečné informace	25

Crypto-World 3/2007

A.	O speciální blokové šifře DN a hašovací funkci HDN (T.Rosa)	2-3
B.	Rodina speciálních blokových šifer DN a hašovacích funkcí nové generace HDN typu SNMAC (V.Klíma)	4-26
C.	Najväčšia tma je pod lampou – STEGANOGRAFIA, část II. (R.Cinkais)	27-33
D.	Šifrování v MS Office (P.Tesař)	34
E.	O čem jsme psali v březnu 2000 – 2006	35-36
F.	Závěrečné informace	37

Crypto-World 4/2007

A.	Rodina speciálních blokových šifer DN a hašovacích funkcí nové generace HDN typu SNMAC, část II. - Dodatky (V.Klíma)	2-14
B.	Zachycené a šifrové telegramy dokazují, že demokraté se během voleb snažili podplácet! (P.Vondruška)	15-21
C.	Kircherovo šifrování aneb Dobrý voják Švejk	22-25
D.	Úloha k luštění ... (P.Vondruška)	26
E.	O čem jsme psali v dubnu 2000 -2006	27-28
F.	Závěrečné informace	29

Crypto-World 5/2007

A.	Z dějin československé kryptografie, část I., Československý šifrátor MAGDA (K.Šklíba)	2-5
B.	Řešení dubnové úlohy (P.Vondruška)	6-7
C.	Bealovy šifry (P.Vondruška)	8-19
D.	O čem jsme psali v květnu 2000-2006	20-21
E.	Závěrečné informace	22

Crypto-World 6/2007

A.	Přehled a historie polyalfabetických šifer (P.Vondruška)	2-11
B.	Matematizace komplexní bezpečnosti v ČR, část I. (J.Hrubý)	12-20
C.	Mikulášská kryptobesídka, Call for Papers	21
D.	O čem jsme psali v červnu 2000-2006	22-23
E.	Závěrečné informace	24

Příloha: Mikulášská kryptobesídka (6.-7.12.2007)- MKB2007_CallForPapers_cerven.pdf

Crypto-World 7/2007 (mimořádné vydání)

- | | | |
|----|---|-----|
| A. | Počítačová kriminalita v návrhu nového trestního zákoníku (2007),
Výzva ke kontrole navrženého paragrafového znění (V.Klíma) | 2-5 |
| B. | Závěrečné informace | 6 |

Crypto-World 78/2007

- | | | |
|----|---|-------|
| A. | Podzimní soutěž v luštění 2007, úvodní informace | 2 |
| B. | Štěpán Schmidt (prolog Soutěže 2007) | 3-4 |
| C. | Z dějin československé kryptografie, část II.,
Československé šifrovací stroje z období 1930–1939 a 1945–1955 (K.Šklíba) | 5-9 |
| D. | Matematizace komplexní bezpečnosti v ČR, část II. (J.Hrubý) | 10-16 |
| E. | O čem jsme psali v létě 2000-2006 | 17-18 |
| F. | Závěrečné informace | 19 |

Crypto-World 9/2007

- | | | |
|----|---|-------|
| A. | Soutěž v luštění 2007 začala! (P.Vondruška) | 2-4 |
| B. | Mládí Štěpána Schmidta (doprovodný text k I.kolu soutěže) | 5-11 |
| C. | Názor čtenáře k návrhu TrZ (T.Sekera) | 12 |
| D. | Mikulášská kryptobesídka | 13 |
| E. | O čem jsme psali v září 2000-2006 | 14-15 |
| F. | Závěrečné informace | 16 |

Příloha: Mikulášská kryptobesídka - Call for Papers (MKB_CFP.PDF)

Crypto-World 10/2007

- | | | |
|----|---|-------|
| A. | Štěpán Schmidt v Černé komoře (doprovodný text k III.kolu soutěže) | 2-9 |
| B. | Z dějin československé kryptografie, část III.,
Paměti armádního šifranta (J.Knížek) | 10-23 |
| C. | O čem jsme psali v říjnu 2000-2006 | 24-25 |
| D. | Závěrečné informace | 26 |

Crypto-World 11/2007

- | | | |
|----|---|-------|
| A. | Soutěž v luštění 2007 skončila (P.Vondruška) | 2 |
| B. | Z dějin československé kryptografie, část IV., Československé šifrovací
stroje z období 1955 – 1960. Šifrovací stroj ŠD – 1 (K.Šklíba) | 3-5 |
| C. | Testy obrazové kvality snímačů otisků prstů Suprema
(M.Drahanský, O.Nezhyba) | 6-11 |
| D. | Možnosti odposlechu optických vláken (J.Dušátko) | 12-30 |
| E. | Mikulášská kryptobesídka 2007 – Program (V.Matyáš) | 31-32 |
| F. | Konference EOIF GigaCon (A.Ušcińska) | 33 |
| G. | O čem jsme psali v listopadu 2000-2006 | 33-35 |
| H. | Závěrečné informace | 36 |

Příloha: Příběh Štěpána Schmidta (všechny 4 části ve formátu doc) pribeh.doc

Crypto-World 12/2007

- | | | |
|----|--|-------|
| A. | Soutěž v luštění 2007 – řešení úloh I. kola | 2-10 |
| B. | Soutěž v luštění 2007 – řešení úloh II. kola | 11-15 |
| C. | Soutěž v luštění 2007 – řešení úloh III. kola | 16-25 |
| D. | Soutěž v luštění 2007 – řešení úloh IV. kola | 26-29 |
| E. | Soutěž v luštění 2007 – z poznámek soutěžících | 30-35 |
| F. | O čem jsme psali v prosinci 1999-2006 | 36-37 |
| G. | Závěrečné informace | 38 |

Příloha: program na šifrování a dešifrování homofonních substitucí a nomenklátorů - nomenklator.exe