

2008

Crypto-World 1/2008

A.	O kolizích hašovací funkce Turbo SHA-2 (V. Klíma)	2-13
B.	Z dějin československé kryptografie, část V., Československé šifrovací stroje z období 1955 – 1960. Šifrovací stroj ŠD – 2 (1. díl) (K. Šklíba)	14-17
C.	První česká kryptografická příručka (P. Vondruška)	18-20
D.	Pozvánka - Konference EOIF GigaCon 2008 – Elektronický oběh informací ve firmě	21
E.	O čem jsme psali v lednu 1999-2007	22-23
F.	Závěrečné informace	24

Crypto-World 2/2008

A.	O chystané demonstraci prolomení šifer A5/1 a A5/2	2-9
B.	Podmínky důvěryhodnosti elektronických dokumentů v archívu (Z.Loebel, B.Procházková, J.Šiška, P.Vondruška, I.Zderadička)	10-20
C.	Rozhovor na téma bezpečnost našich webmailů (.cCuMiNn. , P.Vondruška)	21-22
E.	O čem jsme psali v únoru 1999-2007	23-24
F.	Závěrečné informace	25

Crypto-World 3/2008

A.	E-zin 3/2008 + Voynichův rukopis (P.Vondruška)	2-3
B.	Voynichův rukopis (Wikipedia)	4-7
C.	Záhadný Dr. Rafael (J.Hurych)	8-12
D.	Z dějin československé kryptografie, část VI., Československé šifrovací stroje z období 1955 – 1960. Šifrovací stroj ŠD – 2 (2. díl) (K.Šklíba)	13-22
E.	O čem jsme psali v březnu 1999-2007	23-24
F.	Závěrečné informace	25

Crypto-World 4/2008

A.	Hakin9 - jak se bránit ? (P.Vondruška)	2 - 4
B.	MIME formát a NBÚ formát ZEP(ZIP) pre uľahčenie splnenia požiadavky WYSIWYS pri QES (P.Rybár)	5 - 6
C.	Trusted Computing (P.Sušil)	7 - 10
D.	Ještě o Dr. Rafaelovi (Jan B. Hurych)	11-17
E.	O čem jsme psali v dubnu 1999-2007	18-19
F.	Závěrečné informace	20

Crypto-World 5/2008

A.	Příklad útoku na podepsovaný dokument, ktorého typ nie je chránený samotným podpisom (P.Rybar)	2
B.	Speciální bloková šifra - Nová hešovací funkce. (P.Sušil)	3 – 9
C.	Z dějin československé kryptografie, část VI., Československé šifrovací stroje z období 1960– 1970. Šifrovací stroj ŠD – 3 (K.Šklíba)	10-14
D.	Mikulášská kryptobesídka, Call for Papers	15-17
E.	O čem jsme psali v květnu 2000-2007	18-19
F.	Závěrečné informace	20

Příloha:

- 1) Mikulášská kryptobesídka (4.-5.12.2008): CFP_MKB2008_May.pdf
- 2) Příloha k článku „Příklad útoku na podepsaný dokument ... “ : prikklad.bmp

Crypto-World 6/2008

A.	RFID: Co to vlastně máme v kapse? (M.Hlaváč, T.Rosa)	2 - 17
B.	Bezpečnost PHP aplikací (J.Vrána)	18 - 22
C.	Popis šifrovacího algoritmu Serpent (J.Jeřábek)	24 - 29
D.	O čem jsme psali v červnu 2000-2007	30 – 31
E.	Závěrečné informace	32

Crypto-World 78/2008

A.	Současná kryptologie v praxi (V.Klíma)	2-10
B.	Zabezpečení souborů v kanceláři (L.Caha)	11-17
C.	Z dějin československé kryptografie, část VIII., Trofejní šifrovací stroje používané v Československu v letech 1945 - 1955. Šifrátory ENIGMA, ANNA a STANDARD (K.Šklíba)	18-24
D.	Nové knihy (Biometrie a identita člověka, Autentizace elektronických transakcí a autorizace dat i uživatelů)	25
E.	O čem jsme psali v létě 1999-2007	26-27
F.	Závěrečné informace	28

Crypto-World 9/2008

A.	Podzimní Soutěž v luštění 2008, úvodní informace (P.Vondruška)	2-3
B.	John Wellington (prolog Soutěže 2008) (P.Vondruška)	4-6
C.	Autentizace pomocí Zero-Knowledge protokolů (J.Hajný)	7-13
D.	Recenze knihy: Matyáš, V., Krhovják, J. a kol.: Autorizace elektronických transakcí a autentizace dat i uživatelů (V.J.Jákl)	14-15
E.	O čem jsme psali v září 1999-2007	16-17
F.	Závěrečné informace	18

Crypto-World 10/2008

A.	Podzimní Soutěž v luštění 2008 začíná (P.Vondruška)	2
B.	John Wellington vzpomíná, pokračování příběhu (P.Vondruška)	3-5
C.	Příběh šifrovacího stroje Lorenz SZ (P.Veselý)	6-17
D.	Hašovací funkce COMP128 (P. Sušil)	18-26
E.	O čem jsme psali v říjnu 1999-2007	27-28
F.	Závěrečné informace	29

Příloha: simulátor historického šifrátoru Lorenz SZ 40- lorenz.zip

Crypto-World 11/2008

A.	Podzimní Soutěž v luštění 2008 skončila! (P. Vondruška)	2-4
B.	KYBERNETICKÉ ÚTOKY: RUSKO? – GRUZIE a SVĚT (T.Sekera)	5-11
C.	Kvantový šumátor ve Společné laboratoři optiky UP a Fyzikálního ústavu AV ČR (J. Hrubý)	12-17
D.	Mikulášská kryptobesídka 2008 / SantaCrypt 2008	18-19
E.	O čem jsme psali v listopadu 1999-2007	20-21
F.	Závěrečné informace	22

Crypto-World 12/2008

A.	Závěr soutěže 2008, úlohy, použité systémy, řešení, komentáře řešitelů (P.Vondruška, řešitelé)	2-24
B.	Příběhy Johna Wellingtona (P.Vondruška)	25-33
C.	O čem jsme psali v únoru 1999-2007	34-35
D.	Závěrečné informace	36

Příloha:

- 1) simulátor šifrátoru Lorenz SZ40 <http://soutez2008.crypto-world.info/pribeh/lorenz.zip>
- 2) nastavení pro řešení soutěžních úloh 07,14,15,01: set.zip