

2006

Crypto-World 1/2006

A.	Elektronická fakturace (přehled některých požadavků) (P.Vondruška)	2-8
B.	Biometrika a kryptologie (J.Pinkava)	9-11
C.	Nejlepší práce – KeyMaker 2005, Kryptoanalýza německé vojenské šifry Enigma (J.Vábek)	12-23
D.	O čem jsme psali v lednu 1999-2005	24
E.	Závěrečné informace	25

Crypto-World 2/2006

A.	Statistika vydaných elektronických podpisů (P.Vondruška)	2-5
B.	Kryptologie, šifrování a tajná písma (P.Vondruška)	6-8
C.	NIST (National Institute of Standards and Technology - USA) a kryptografie, část 1. (J.Pinkava)	9-12
D.	E-Mudžahedínové, virtuální strana štěstí a e-sprejeři ... (P.Vondruška)	13-16
E.	O čem jsme psali v únoru 1999-2005	17
F.	Závěrečné informace	18

Crypto-World 3/2006

A.	Klíče a hesla (doporučení pro začátečníky) (P.Vondruška)	2-6
B.	Poznámky k internetovému podvodu zaměřenému na klienty české Citibank (O. Suchý)	7-12
C.	NIST (National Institute of Standards and Technology - USA) a kryptografie, část 2. (J.Pinkava)	13-15
D.	Elektronické volby v ČR ? (J.Hrubý)	16-20
E.	O čem jsme psali v březnu 1999-2005	21
F.	Závěrečné informace	22

Crypto-World 4/2006

A.	Kolize MD5 do minuty aneb co v odborných zprávách nenajdete (V.Klíma)	2-6
B.	Po Tunely v hašovacích funkcích: kolize MD5 do minuty (V.Klíma)	7-23
C.	Porovnání rychlosti zveřejněných algoritmů pro hledání kolizí MD5 (P.Vondruška, R.Cinkais, R.Barczy, P.Sušil)	24-25
D.	O čem jsme psali v dubnu 1999-2005	26-27
E.	Závěrečné informace	28

Příloha: version_0.zip, version_1.zip (programy pro hledání kolizí MD5 , Klíma: 18.3, 28.3)

Crypto-World 5/2006

A.	Hledá se náhrada za kolizní funkce ... (P.Vondruška)	2-5
B.	Bezpečnost IP Telefonie nad protokolem SIP (J. Růžička, M.Vozňák)	6-11
C.	NIST (National Institute of Standards and Technology - USA) a kryptografie, Recommendation on Key Management – část 1. (J.Pinkava)	12-15
D.	Call for Papers – Mikulášská kryptobesídka (D.Cvrček)	16
E.	O čem jsme psali v květnu 1999-2005	17-18
F.	Závěrečné informace	19

Crypto-World 6/2006

A.	PKI roaming (L. Dostálek)	2-4
B.	Vyhláška o podrobnostech atestačního řízení pro elektronické nástroje a lehký úvod do časové synchronizace (P. Vondruška)	5-9
C.	Univerzální posilovače hašovacích funkcí, včetně MD5 a SHA1 aneb záchranné kolo pro zoufalce (V. Klíma)	10-14
D.	NIST (National Institute of Standards and Technology - USA) a kryptografie, Recommendation on Key Management – část 2. (J. Pinkava)	15-18
E.	O čem jsme psali v červnu 1999-2005	19-20
F.	Závěrečné informace	21

Crypto-World 78/2006

A.	Pozvánka k tradiční podzimní soutěži v luštění (P. Vondruška)	2-3
B.	Lektorský posudek na knihu Kryptologie, šifrování a tajná písma (V. Klíma)	4-6
C.	Ukázky z knihy Kryptologie, šifrování a tajná písma (P. Vondruška)	7-10
D.	Chcete si zaluštit? (P. Vondruška)	11
E.	NIST (National Institute of Standards and Technology - USA) a kryptografie, Recommendation on Key Management – část 3. (J. Pinkava)	12-15
F.	O čem jsme psali v létě 1999-2005	16-17
G.	Závěrečné informace	18

Crypto-World 9/2006

A.	Soutěž v luštění 2006 začala! (P. Vondruška)	2-6
B.	Přehled úkolů „Soutěž v luštění 2006“ (P. Vondruška)	7-12
C.	Systém Gronsfeld (P. Vondruška)	13-14
D.	Mikulášská kryptobesídka - MKB 2006 (D. Cvrček)	15-16
E.	O čem jsme psali v září 1999-2005	17-18
F.	Závěrečné informace	19

Crypto-World 10/2006

A.	Soutěž v luštění 2006 - průběh (P. Vondruška)	2-3
B.	Elektronické cestovní doklady, část 1 (L. Rašek)	4-18
C.	Bezpečnost elektronických pasů (Z. Říha)	19-26
D.	Říjnové akce – pozvánka	27
E.	O čem jsme psali v říjnu 1999-2005	28-29
F.	Závěrečné informace	30

Příloha: doprovodné materiály k Soutěži v luštění 2006 - vystava.pdf , epilog.pdf

Crypto-World 11/2006

A.	Soutěž v luštění 2006 skončila (P. Vondruška)	2
B.	Nový koncept hašovacích funkcí SNMAC s využitím speciální blokové šifry a konstrukcí NMAC/HMAC (V. Klíma)	3-16
C.	Elektronické cestovní doklady, část 2 (L. Rašek)	17-24
D.	Počítačová (ne)bezpečnost (J. Pinkava)	25-31
E.	Mikulášská kryptobesídka (D. Cvrček)	32-33
F.	O čem jsme psali v listopadu 1999-2005	34-35
G.	Závěrečné informace	36

Crypto-World 12/2006

A.	Soutěž v luštění 2006 – řešení soutěžních úloh (P. Vondruška)	2-31
B.	Z e-mailů soutěžících (vybral P. Vondruška)	32-33
C.	O čem jsme psali v prosinci 1999-2005	34-35
D.	Závěrečné informace	36

Příloha : Šifra Delastelle – BIFID.pdf