

2014

Crypto-World 1-3/2014

A.	Československá šifra TTS a jej lúštenie (P. Javorka)	2 - 12
B.	Nový (souhrnný) pohled na otázky bezpečnosti eliptické kryptografie (J.Pinkava)	13 - 14
B.	Vyhláška o kybernetické bezpečnosti – výzva k připomínkám	15
C.	Několik poznámek ke kryptografickým požadavkům uvedeným ve Vyhlášce o kybernetické bezpečnosti (P.Vondruška)	16 - 23
E.	O čem jsme psali v předchozích 149 číslech ...	24
F.	Závěrečné informace	25

Crypto-World 4-5/2014

A.	Definice Off-The-Record (OTR) protokolu a jeho využití (L. Langhammer, J. Polák)	2 – 9
B.	Lúštenie a analýza šifry Straddling Checkerboard (M.Hornák)	10 – 20
C.	Nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu - eIDAS (P.Vondruška)	21 - 23
D.	Call for Papers, Mikulášská kryptobesídka (V.Matyáš)	24
E.	Pozvánka ke kurzu PKI (+eIDAS) Akademie CZ.NIC (P.Vondruška)	25
F.	O čem jsme psali v předchozích 150 číslech ...	26
G.	Závěrečné informace	27

Příloha: CFP_MKB2014.pdf http://crypto-world.info/casop16/CFP_MKB2014.pdf

Crypto-World 6-7/2014

A.	Identifikácia zmysluplného textu pri klasických šifrách (P. Matiaško)	2 – 14
B.	Cryptorbit, 1.díl (V.Klíma, M.Kákona)	15 - 26
C.	Pár poznámek k šifrátoru MAFFIE (P.Vondruška)	27 - 31
D.	Call for Papers, Mikulášská kryptobesídka (V.Matyáš)	32
E.	O čem jsme psali v předchozích 151 číslech ...	33 - 34
F.	Závěrečné informace	35

Příloha: CFP_MKB2014.pdf http://crypto-world.info/casop16/CFP_MKB2014.pdf

Crypto-World 8-9/2014

A.	Ukončení vydávání e-zinu Crypto-World (P.Vondruška)	2
B.	Poděkování autorům (P.Vondruška)	3
C.	Příspěvek k luštění šifry Cryptorbit (B.Rudolf)	4 - 19
D.	Call for Papers, Mikulášská kryptobesídka (V.Matyáš)	20
E.	Pozvánka ke kurzu PKI (+eIDAS) Akademie CZ.NIC (P.Vondruška)	21
F.	O čem jsme psali v předchozích 152 číslech ...	22
G.	Závěrečné informace	23

Příloha: CFP_MKB2014.pdf http://crypto-world.info/casop16/CFP_MKB2014.pdf