

2010

Crypto-World 1/2010

A.	Analýza Blue Midnight Wish – útok na vzor (V.Klíma, D. Gligoroski)	2-11
B.	Tajné písmo Martina Kukučína (J.Kollár)	12-16
C.	Chcete si zaluštit? (M.Kolařík)	17
D.	Telefónica O2 poskytuje podklady pro stavební povolení elektronicky	18
E.	Science Café - Dobrodružství kryptologie	19
F.	O čem jsme psali v lednu 1999-2009	20-21
G.	Závěrečné informace	22

Crypto-World 2/2010

A.	Analýza Blue Midnight Wish – útok na vzor (V.Klíma, D. Gligoroski)	2-11
B.	Kryptologie, šifrování a tajná písma – ukázka z knihy (P.Vondruška)	12-16
C.	Chcete si zaluštit? Díl 3. (M.Kolařík)	17
D.	Matrix - tak trochu jiná šifrovačka (M.Kesely, M.Švagerka)	18-19
E.	O čem jsme psali v únoru 1999-2009	20-21
F.	Závěrečné informace	22

Crypto-World 3/2010

A.	Analýza Blue Midnight Wish – útoky na stavební bloky (V.Klíma, D.Gligoroski)	2-13
B.	Přehled některých základních kritérií hodnocení bezpečnosti IT (P.Vondruška)	14 - 20
C.	Chcete si zaluštit? Díl 4. (M.Kolařík)	21
D.	Aktuální situace v oblasti uznávání zahraničních kvalifikovaných certifikátů (P.Vondruška)	22-24
E.	O čem jsme psali v březnu 1999-2009	25-26
F.	Závěrečné informace	27

Crypto-World 4/2010

A.	Analýza Blue Midnight Wish – srovnání složitosti (bezpečnosti) BMW a dalších kandidátů SHA-3 (V.Klíma, D. Gligoroski)	2-5
B.	Rozhovor: Šifry mistrů kryptologů (L.Soukup)	6-9
C.	Index koincidence (L.Fojtová)	10-13
D.	Chcete si zaluštit? Díl 4. (M.Kolařík)	14
E.	Tajemství ukryté v 11-ti pohlednicích (upoutávka) (P.Vondruška, M.Janošová)	15-16
F.	Telegramy pořád žijí (V.David)	17-18
G.	O čem jsme psali v dubnu 1999-2009	19-20
H.	Závěrečné informace	21

Crypto-World 5/2010

A.	Analýza Blue Midnight Wish – současné útoky na BMW-n (V.Klíma, D. Gligoroski)	2-6
B.	Dílní diferenciální vlastnosti zobrazení $A2(A1(M))$ ve funkci f_0 , v návrhu hašovací funkce BMW (V.Plátěnka)	7-9
C.	Ze vzpomínek armádního šifranta II. (J.Knížek)	10-12
D.	Tajemství ukryté v 11-ti pohlednicích (M.Janošová)	13-21
E.	Chcete si zaluštit? Díl 5. (M.Kolařík)	22

F.	Problematika infrastruktury veřejných klíčů (PKI), kurz Akademie CZ.NIC (P.Vondruška)	23-24
G.	Call for Papers Mikulášská kryptobesídka	25
H.	KEYMAKER – studentská soutěž	26
I.	O čem jsme psali v květnu 1999-2009	27-28
J.	Závěrečné informace	29

Crypto-World 6/2010

A.	Utajená míra složitosti (V. Klíma)	2-6
B.	Ze vzpomínek armádního šifranta III. (J. Knížek)	7-9
C.	Hláskovací tabulka (P. Vondruška)	10-13
D.	Chcete si zaluštit? Díl 6. (M. Kolařík)	14
E.	Bezpečnostní střípky (J.Pinkava)	15-21
F.	O čem jsme psali v červnu 1999-2009	22-23
G.	Závěrečné informace	24

Crypto-World 7-8/2010

A.	Blížící se konference k SHA-3 a rušno mezi kandidáty (V. Klíma)	2-9
B.	Generické kolizní útoky na úzké hašovací funkce rychlejší než narozeninový paradox, aplikovatelné na třídy funkcí MDx, SHA-1, SHA-2 a úzké kandidáty na SHA-3 (V.Klíma, D. Gligoroski)	10-12
C.	Podzimní Soutěž v luštění 2010, úvodní informace (P. Vondruška)	13-14
D.	Chcete si zaluštit? Díl 8. (závěrečný) (M. Kolařík)	15
E.	O čem jsme psali v létě 1999-2009	17-18
F.	Závěrečné informace	19

Crypto-World 9/2010

A.	Z dějin československé kryptografie, část IX. Vzpomínky Jiřího Václava na výrobu dálkopisů a částí šifrátorů ve Zbrojovce Brno (Jiří Václav)	2 - 4
B.	Podzimní Soutěž v luštění 2010 začíná (P.Vondruška)	5 - 7
C.	Doprovodný příběh k Soutěži v luštění 2010 (P.Vondruška) Giacomo Casanova - Tajnosti mého života (Secrets de ma vie)	8 – 11
D.	Giacomo Casanova - Příběh mého života (Histoire de ma vie)	12 – 17
E.	Jan Josef Antonín Eleazar Kittel	18 – 19
F.	Call for Papers Mikulášská kryptobesídka	20
G.	KEYMAKER – studentská soutěž	21
H.	O čem jsme psali v září 1999-2009	22 - 24
I.	Závěrečné informace	25

Crypto-World 10/2010

A.	Jak dopadla soutěž SHA-3? (Vlastimil Klíma)	2 - 10
B.	Podzimní Soutěž v luštění 2010 jde do finále (P.Vondruška)	11 - 12
C.	Doprovodné příběhy k úlohám Soutěže v luštění 2010 (P.Vondruška)	13 – 23
D.	Problematika infrastruktury veřejných klíčů (PKI), dvoudenní kurz Akademie CZ.NIC (P.Vondruška)	24-25
E.	O čem jsme psali v říjnu 1999-2009	26 - 27
F.	Závěrečné informace	28

Crypto-World 11/2010

A.	Soutěž v luštění 2010 skončila ! (P.Vondruška)	2 - 3
B.	Doprovodné příběhy k úlohám (P.Vondruška)	4 - 8
C.	Soutěžní příklady roku 2010, použitý systém, dešifrované texty (P.Vondruška)	9 – 28
D.	Ohlasy, připomínky a komentáře soutěžících	29 - 33
E.	Mikulášská kryptobesídka /Santa Cryptt 2010 / Program	34 -35
F.	O čem jsme psali v listopadu 1999-2009	36 - 38
G.	Závěrečné informace	39

Crypto-World 12/2010

A.	Finále SHA-3 - překvapení a zklamání (V. Klíma)	2 - 3
B.	Finále SHA-3 – jak to vidím já (P.Vondruška)	4
C.	Novela rozhodnutí Komise 2009/767/ES	5 – 10
D.	Šifra mistra Leonarda ☺	11 - 12
E.	O čem jsme psali v prosinci 1999-2009	13 - 15
F.	Závěrečné informace	16