

2009

Crypto-World 1/2009

A.	Novoroční perlička o luštění šifrových zpráv (K. Šklíba)	2-5
B.	Mohutné multikolize a multivzory hašovacích funkcí BLENDER-n (V. Klíma)	6-13
C.	Proč se přestala používat bomba pro luštění Enigmy až v roce 1955?(P.Vondruška)	14-15
D.	Senát schválil nový trestní zákoník (P. Vondruška)	16-20
E.	Pozvánka na konferenci Trendy v internetové bezpečnosti	21
F.	O čem jsme psali v lednu 1999-2008	22-23
G.	Závěrečné informace	24

Crypto-World 2/2009

A.	Blue Midnight Wish, kandidát na SHA-3 aneb poněkud privátně o tom, jak jsem k BMW přišel (V. Klíma)	2-12
B.	Nastal čas změn (nejde o Obamův citát, ale o používání nových kryptografických algoritmů) (P. Vondruška)	13-17
C.	Pozvánka na konferenci IT-Právo	18-19
D.	O čem jsme psali v únoru 1999-2008	20-21
E.	Závěrečné informace	22

Crypto-World 3/2009

A.	Prvá konferencia SHA-3 kandidátov (M.Hojsík)	2-6
B.	Blue Midnight Wish, popis a principy (V. Klíma)	7-21
C.	Pozvánka na konferenci SmartCard Forum 2009	22
D.	O čem jsme psali v březnu 1999-2008	23-24
E.	Závěrečné informace	25

Crypto-World 4/2009

A.	Apríl (který se však až tak úplně nekonal)	2
B.	Popis a principy EDON-R (V. Klíma)	3-8
C.	Aplikace e-notáře a vícenásobného elektronického podpisu v rámci zavádění ISDS ? (J.Hrubý)	9-16
D.	Bedna 2009 - pozvánka	17
E.	O čem jsme psali v dubnu 1999-2008	18-19
F.	Závěrečné informace	20

Příloha: april.htm (ukázka aprílového žertíku s využitím XSS zranitelnosti)

Crypto-World 5/2009

A.	O bezpečnosti objevování sousedů (SEND + CGA) (P.Vondruška)	2-6
B.	SIM karta mobilu ako bezpečné zariadenie pre vytváranie zaručeného elektronického podpisu (ZEP) (P.Rybár)	7-10
C.	Mikulášská kryptobesídka , Call for Papers	11-12
D.	Akademie CZ.NIC nabízí vysoce specializované kurzy o internetových technologiích (PR)	13-14
D.	O2 a PMDP představují Plzeňskou kartu v mobilu	15
E.	O čem jsme psali v květnu 1999-2008	16-17
F.	Závěrečné informace	18

Příloha: Call for Papers Mikulášská kryptobesídka 2009 - CFP_MKB2009.pdf

Crypto-World 6/2009

A.	Výprava za obsahem javascriptu (J.Vorlíček, J.Suchý)	2-6
B.	Anonymita v globální síti (J.Hajný)	7-11
C.	Formát elektronické fakturace ISDOC (P.Kuchař)	12-18
D.	Malá soutěž v luštění RSA (P.Vondruška)	19-20
E.	O čem jsme psali v červnu 1999-2008	21-22
F.	Závěrečné informace	23

Příloha: javascript-priloha.pdf (179 kB)

javascript-priloha_1_3.rtf (64 kB)

Crypto-World 7-8/2009

A.	Do druhého kola soutěže SHA-3 postoupilo 14 kandidátů, mezi nimi i BMW (V.Klíma)	2-4
B.	Datové schránky, ale co s nimi? (T.Sekera)	5-7
C.	Rekonstrukce šifrovacího stroje ŠD-2 (V.Brtník)	8-15
D.	Malá soutěž v luštění RSA – řešení (P.Vondruška)	16-19
E.	CD Crypto-World (P.Vondruška)	20
F.	O čem jsme psali v létě 1999-2008	21-22
G.	Závěrečné informace	23

Přílohy:

Simulátor šifrátoru ŠD-2 <http://crypto-world.info/soutez2009/sd2/cti.txt>

(viz článek Rekonstrukce šifrovacího stroje ŠD-2)

Program RSAM.EXE (viz článek Malá soutěž v luštění RSA – řešení).

Dotazník CD Crypto-World (po vyplnění v jednom z příložených formátů doc/rtf/txt zašlete zpět na e-zin@crypto-world.info , viz článek CD Crypto-World)

Crypto-World 9/2009

A.	CD k 11.výročí založení e-zinu Crypto-World (P.Vondruška)	2-3
B.	Podzimní Soutěž v luštění 2009, úvodní informace (P.Vondruška)	4
C.	Poznámka k lineárním aproximacím kryptografické hašovací funkce BLUE MIDNIGHT WISH (V.Klíma, P.Sušil)	5-14
D.	Co provádí infikovaný počítač? (J.Vorlíček)	15-21
E.	Ze vzpomínek armádního šifranta (J.Knížek)	22-23
D.	Pozvánka / CFP na MKB 2009	24-25
E.	O čem jsme psali v září 1999-2008	26-27
F.	Závěrečné informace	28

Příloha:

Objednávka CD k 11.výročí založení e-zinu Crypto-World

Příloha k článku Co provádí infikovaný počítač? : priloha.pdf

CFP – MKB 2009 : cfp_mkb_2009.pdf

CFP – KEYMAKER : cfp_keymaker_2009.pdf

Crypto-World 10/2009

A.	Podzimní Soutěž v luštění 2009 začíná	2
B.	Pravidla Soutěže 2009	2-3
C.	Soutěž 2009 – ceny	3-4
D.	Doprovodný příběh k Soutěži v luštění 2009 (P.Vondruška)	5- 10
E.	Luštitelské etudy I. Rusko 1918 (K.Šklíba)	11- 21
F.	O čem jsme psali v říjnu 1999-2008	22-23
G.	Závěrečné informace	24

Crypto-World 11/2009

A.	Soutěž v luštění 2009 skončila!	2
B.	JAK SE STAL VÁCLAV PROKOPEC VĚZNĚM	3-4
C.	JAK SE STAL VÁCLAV PROKOPEC KRYPTOLOGEM	4-5
D.	JAK SE STAL VÁCLAV PROKOPEC ZRÁDCEM	6-9
E.	JAK BYL PROLOMEN ŠIFROVÝ TEXT ZAŠIFROVANÝ POMOCÍ CM-1	9
F.	Příloha č.1: Úlohy z PVS	10-11
G.	Řešení úloh č.1,č.2 a č.3 - Úlohy z PVS	11-12
H.	Příloha č.2: Administrativní kurz C v Tloskově 1	12-14
I.	Příloha č.3: Administrativní kurz C v Tloskově 2	14-15
J.	Řešení úloh č.4,č.5 a č.6- Administrativní kurz C v Tloskově 1,2	15-19
K.	Příloha č.4: Administrativní kurz C v Tloskově 3	19-20
L.	Řešení úloh č.7,č.8 a č.9 - Administrativní kurz C v Tloskově 3	20-23
M.	Příloha č.5: Administrativní kurz C v Tloskově 4	23-24
N.	Řešení úloh č.10 - Administrativní kurz C v Tloskově 4	24-26
O.	Příloha č.6: Zvláštní správa - analýza dopisů	26-27
P.	Řešení úloh č.11 a č.12 - Zvláštní správa - analýza dopisů	27-29
Q.	Příloha č.7: Zpráva centrále	29-30
R.	Řešení úlohy č.13 - Zpráva centrále	30-32
S.	Příloha č.8: Dešifrace ŠD-2 / CM-1	32-33
T.	Řešení úloh č. 14 a č.15 - Dešifrace ŠD-2 / CM-1	34-37
U.	Ohlasy a komentáře soutěživých	38-39
V.	O čem jsme psali v listopadu 1999-2008	40-41
W.	Závěrečné informace	42

Crypto-World 12/2009

A.	Predikce finalistů SHA-3 (V.Klíma)	2-3
B.	Chcete si ještě zaluštit? (M.Kolařík, P.Vondruška)	3
C.	Posílený Blue Midnight Wish a druhé kolo soutěže SHA-3 (V.Klíma)	4-16
D.	Jak prolomit SSL ... (P.Vondruška)	17-26
E.	Datové schránky v právním řádu ČR. Zákon č.300/2008 Sb., o elektronických úkonech a autorizované konverzi s komentářem (recenze knihy V.Smejkala)	27-28
F.	O čem jsme psali v říjnu 1999-2008	29-30
G.	Závěrečné informace	31