

2005

Crypto-World 1/2005

A.	Předávání dat na Portál veřejné správy (J.Klimeš)	2-6
B.	Praktická ukážka využitia kolízií MD5 (O.Mikle)	7-9
C.	Kryptografie a normy - Formáty elektronických podpisů, část 2 (J.Pinkava)	10-13
D.	Test elektronickej svojprávnosti (A.Olejník, I.Pullman)	14-19
E.	Vojničův rukopis - výzva (J.B.Hurych)	20-21
F.	O čem jsme psali v lednu 2000-2004	22
G.	Závěrečné informace	23

Příloha :

Speciál 2004 - přehled článků a prezentací členů redakce Crypto-World za rok 2004
(http://crypto-world.info/casop6/prehled_2004.pdf)

Crypto-World 2/2005

A.	Mikulášská kryptobesídka 2004 (V. Matyáš, D. Cvrček)	2-3
B.	Útoky na šifru Hiji-bij-bij (HBB) (V. Klíma)	4-13
C.	A Concise Introduction to Random Number Generators (P. Hellekalek)	14-19
D.	Útoky na a přes API: PIN Recovery Attacks (J. Krhovják, D. Cvrček)	20-29
E.	MoraviaCrypt'05 (CFP)	30
F.	O čem jsme psali v únoru 2000-2004	31
G.	Závěrečné informace	32

Crypto-World 3/2005

A.	Nalézání kolízií MD5 - hračka pro notebook (V.Klíma)	2-7
B.	Co se stalo s hašovacími funkcemi?, část 1 (V.Klíma)	8-10
C.	Popis šifry PlayFair (P. Vondruška)	11-14
D.	První rotorové šifrovací stroje (P. Vondruška)	15-16
E.	Recenze knihy: Guide to Elliptic Curve Cryptography	17-18
F.	O čem jsme psali v březnu 2000-2004	19
G.	Závěrečné informace	20

Crypto-World 4/2005

A.	Co se stalo s hašovacími funkcemi?, část 2. (V.Klíma)	2-11
B.	Neviditelné (sympatetické) inkousty (P. Vondruška)	12-15
C.	Formáty elektronických podpisů - část 3.(J.Pinkava)	16-21
D.	O čem jsme psali v dubnu 2000-2004	22
E.	Závěrečné informace	23

Příloha (PR) :

J.Strelec (Secunet) : SINA - BEZPEČNÁ KOMUNIKAČNÍ INFRASTRUKTURA

Crypto-World 5/2005

A.	Výzva k rozluštění textu zašifrovaného Enigmou (P. Vondruška)	2-3
B.	Přehledová zpráva o významných publikacích a projektech na téma poskytování anonymity, klasifikace a měřitelnost informačního soukromí (privacy), část 1. (M. Kumpošt)	4-8
C.	Formáty elektronických podpisů - část 4. (J. Pinkava)	9-13
D.	Jak psát specifikaci bezpečnosti produktu nebo systému (P.Vondruška)	14-20
E.	O čem jsme psali v dubnu 2000-2004	21
F.	Závěrečné informace	22

Příloha : zpráva vysílaná radioamatérskou stanicí GB2HQ - nedele_30m.wav

Crypto-World 6/2005

A.	Informace pro čtenáře a autory (P.Vondruška)	2-3
B.	Kontrola certifikační cesty, část 1. (P. Rybár)	4-11
C.	O nezískatelnosti rodného čísla z jeho hashu (M. Pivoluska)	12-13
D.	Přehledová zpráva o významných publikacích a projektech na téma poskytování anonymity, klasifikace a měřitelnost informačního soukromí (privacy), část 2. (M. Kumpošt)	14-17
E.	Kryptografické eskalační protokoly, část 1. (J. Krhovják)	18-21
F.	Recenze knihy Jon Erickson: Hacking - umění exploitace	22
G.	O čem jsme psali v červnu 2000-2004	23
H.	Závěrečné informace	24

Crypto-World 78/2005

A.	Pozvánka k tradiční podzimní soutěži v luštění ... (P.Vondruška)	2
B.	Kontrola certifikační cesty, část 2. (P. Rybár)	3-9
C.	Honeypot server zneužit k bankovním podvodům, část 1. (O. Suchý)	10-13
D.	Potenciální právní rizika provozu Honeypot serveru (T.Sekera)	14-15
E.	K některým právním aspektům provozování serveru Honeypot (J.Matejka)	16-18
F.	Přehledová zpráva o významných publikacích a projektech na téma poskytování anonymity, klasifikace a měřitelnost informačního soukromí (privacy), část 3. (M. Kumpošt)	19-22
G.	Kryptografické eskalační protokoly, část 2. (J. Krhovják)	23-26
H.	O čem jsme psali v létě 2000-2004	27
I.	Závěrečné informace	28

Příloha : Dešifrace textu zašifrovaného Enigmou (enigma.pdf)

(volně pokračování článku z Crypto-Worldu 5/2005, str. 2-3 : Výzva k rozluštění textu zašifrovaného Enigmou)

Crypto-World 9/2005

A.	Soutěž v luštění 2005 začíná! (P.Vondruška)	2-5
B.	Bude kryptoanalýza v Česku trestána vězením? (V.Klíma)	6-10
C.	Hardening GNU/Linuxu na úrovni operačního systému, část 1.(J.Kadlec)	11-16
D.	Mikulášská kryptobesídka 2005 (D.Cvrček)	16
E.	Honeypot server zneužit k bankovním podvodům, část 2. (O. Suchý)	17-22
F.	Eskalační protokoly, část 3. (J. Krhovják)	23-26
G.	O čem jsme psali v létě 2000-2004	27
H.	Závěrečné informace	28

Crypto-World 10/2005

A.	Soutěž v luštění 2005 – přehled úkolů I. a II. kola (P.Vondruška)	2-11
B.	Bude kryptoanalýza v Česku trestána vězením? - zřejmě už ne! (V.Klíma)	12-22
C.	Hardening GNU/Linuxu, Časté problémy a chyby administrátorů, část 2. (J.Kadlec)	23-28
D.	O čem byl CHES 2005 a FDTC 2005? (J.Krhovják)	29-32
E.	O čem jsme psali v říjnu 1999-2004	33
F.	Závěrečné informace	34

Příloha : Další informace k článku V.Klímy - přílohy.zip (53 kB)

(Obsahuje: Žádost a podpisy odborníků, Návrh Šámal, Návrh Smejkal, Návrh VK_IURE, překlad části úmluvy, průvodní dopis vk_iure, link psp, stenozáznam jednání PSP, tisk zpráva ČTK)

Crypto-World 11/2005

A.	Soutěž v luštění 2005 – přehled úkolů III. kola (P.Vondruška)	2-7
B.	Hardening GNU/Linux, Komplexnější prostředky pro lokální hardening OS Linux, část 3.(J.Kadlec)	8-12
C.	Může biometrie sloužit ke kryptografii? (Martin Drahanský, Filip Orság)	13-18
D.	Mikulášská kryptobesídka 2005 (D.Cvrček)	19-21
E.	Konference IT SECURITY GigaCon (P.Vondruška)	22
F.	O čem jsme psali v listopadu 1999-2004	22-23
G.	Závěrečné informace	24

Crypto-World 12/2005

A.	Soutěž v luštění 2005 – jak šly „dějiny“...	2
B.	Soutěž v luštění 2005 – řešení úloh I. kola	3-10
C.	Soutěž v luštění 2005 – řešení úloh II. kola	11-26
D.	Soutěž v luštění 2005 – řešení úloh III. kola	27-39
E.	Soutěž v luštění 2005 – z poznámek soutěžících	40-46
F.	O čem jsme psali v prosinci 1999-2004	47-48
G.	Závěrečné informace	49