

1999

Crypto-World 9/1999

A.	Nový šifrový standard AES	1-2
B.	O novém bezpečnostním problému v produktech Microsoftu	3-5
C.	HPUX a UNIX Crypt Algoritmus	5
D.	Letem "šifrovým" světem	5-7
E.	e-mailové spojení (aktuální přehled)	7

Crypto-World 10/1999

A.	Back Orifice 2000	2-3
B.	Šifrování disku pod Linuxem	3-5
C.	Microsoft Point-to-Point Tunneling Protocol (PPTP)	5-6
D.	Letem šifrovým světem	7-8
E.	E-mail spojení	8
Příloha : INRIA leads nearly 200 international scientists in cracking code following challenge by Canadian company Certicom"		9-10

Crypto-World 11/1999

A.	Jak je to s bezpečností eliptických kryptosystémů ? (Ing. Pinkava)	2-4
B.	Známý problém přístupu k zabezpečeným serverům pomocí protokolu https s aplikací Internet Explorer 5 v systému Windows NT 4.0 s aktualizací SP4	4-5
C.	Y2Kcount.exe - Trojský kůň v počítačích	5
D.	Matematické principy informační bezpečnosti (Dr. Souček)	6
E.	Letem šifrovým světem	6-8
F.	E-mail spojení	8
G.	Trocha zábavy na závěr (malované křížovky)	9

Crypto-World 12/1999

A.	Microsoft nás zbavil další iluze! (P.Vondruška)	2
B.	Matematické principy informační bezpečnosti (Dr. J. Souček)	3
C.	Pod stromeček nové síťové karty (P.Vondruška)	3
D.	Konec filatelie (J.Němejc)	4
E.	Y2K (Problém roku 2000) (P.Vondruška)	5
F.	Patálie se systémem Mickeysoft fritéza CE (CyberSpace.cz)	6
G.	Letem šifrovým světem	7-8
H.	Řešení malované křížovky z minulého čísla	9
I.	Spojení	9

2000

Crypto-World 1/2000

A.	Slovo úvodem (P.Vondruška)	2
B.	Země vstoupila do roku 19100 (P.Vondruška)	3 - 4
C.	Nový zákon o ochraně osobních údajů (P.Vondruška)	4 - 5
D.	Soukromí uživatelů GSM ohroženo (P.Vondruška)	6
E.	Letem šifrovým světem	7 - 9
F.	Závěrečné informace	9

Crypto-World 2/2000

A.	Dokumenty ve formátu PDF (M.Kaláb)	2
B.	Kevin Mitnick na svobodě (P.Vondruška)	3
C.	Velká Fermatova věta (historické poznámky) (P.Vondruška)	4
D.	Fermat Last Theorem (V.Sorokin)	5
E.	Zákon o elektronickém podpisu otevírá cestu do Evropy ? (Souček, Hrubý, Beneš, Vondruška)	6-8
F.	Letem šifrovým světem	9-10
G.	Závěrečné informace	11

Crypto-World 3/2000

A.	Nehledá Vás FBI ? (P.Vondruška)	2-3
B.	Aktuality z problematiky eliptických křivek v kryptografii (J. Pinkava)	3-4
C.	Hrajeme si s mobilním telefonem Nokia (anonym)	5
D.	TISKOVÉ PROHLÁŠENÍ - POZMĚŇOVACÍ NÁVRHY K ZÁKONU O ELEKTRONICKÉM PODPISU BUDE PROJEDNÁVAT HOSPODÁŘSKÝ VÝBOR PARLAMENTU	6
E.	Digital Signature Standard (DSS)	7-8
F.	Matematické principy informační bezpečnosti	9
G.	Letem šifrovým světem	9-10
H.	Závěrečné informace	11

Crypto-World 4/2000

A.	Prohlášení odborné skupiny pro zpracování pozměňovacích návrhů k předloze zákona o elektronickém podpisu	2 - 3
B.	Fermatova čísla (P.Vondruška)	4 - 6
C.	Lekce pro tajné agenty - č.1 : "Neztrácejte své laptopy "	6
D.	Opět INRIA ! (J.Pinkava)	7
E.	Nový efektivní kryptosystém s veřejným klíčem na světě? (J.Pinkava)	7
F.	Code Talkers (I.díl) , (P.Vondruška)	8 - 10
G.	Letem šifrovým světem	11 - 12
H.	Závěrečné informace	13

Crypto-World 5/2000

A.	Statistický rozbor prvního známého megaprvočísla (P.Tesař, P.Vondruška)	2-3
B.	Mersennova prvočísla (P.Vondruška)	4-7
C.	Quantum Random Number Generator (J. Hruby)	8
D.	Sdružení pro bezpečnost informačních technologií a informačních systémů (BITIS)	9
E.	Code Talkers (II.díl) , (P.Vondruška)	10-11
F.	Letem šifrovým světem	12-15
G.	Závěrečné informace	15

+ příloha : J.Hrubý , soubor QNG.PS

Crypto-World 6/2000

A.	Nová evropská iniciativa v oblasti kryptografie (J.Pinkava)	2
B.	Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla (P.Vondruška)	3 -5
C.	Červ LOVE-LETTER-FOR-YOU.TXT.VBS (P.Vondruška)	6-8
D.	EUROCRYPT 2000 (P.Vondruška)	9-11
E.	Code Talkers (III.díl) (P.Vondruška)	12-14
F.	Letem šifrovým světem	15
G.	Závěrečné informace	16

Příloha : Navajo Code Talkers , revize z 15.6.1945, soubor Dictionary.htm

Crypto-World 78/2000

A.	Ohlédnutí za I.ročníkem sešitu Crypto-World (P.Vondruška)	2-4
B.	Kryptosystém s veřejným klíčem XTR (J.Pinkava)	4-6
C.	Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla (P.Vondruška)	7-9
D.	Počátky kryptografie veřejných klíčů (J.Janečko)	10-14
E.	Přehled některých českých zdrojů - téma : kryptologie	15-16
F.	Letem šifrovým světem	17-18
G.	Závěrečné informace	19

Příloha : 10000.txt , soubor obsahuje prvních 10 000 prvočísel (další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

Crypto-World 9/2000

A.	Soutěž ! Část I. - Začínáme steganografií	2 - 5
B.	Přehled standardů pro elektronické podpisy(P.Vondruška)	6 - 9
C.	Kryptografie a normy I. (PKCS #1) (J.Pinkava)	10-13
D.	P=NP aneb jak si vydělat miliony (P.Vondruška)	14-16
E.	Hrajeme si s mobilními telefony (tipy a triky)	17
F.	Letem šifrovým světem	18-19
G.	Závěrečné informace	20

+ příloha : gold_bug.rtf , dnešní přílohou je klasická povídka The Gold Bug od Edgara Allana Poea (další informace k příloze viz závěr článku "Část I.- Začínáme steganografií" , str.10) .

Crypto-World 10/2000

A.	Soutěž ! Část II. - Jednoduchá záměna	2 - 4
B.	Král DES je mrtev - ať žije král AES ! (P.Vondruška)	5 - 9
C.	Kde si mohu koupit svůj elektronický podpis? (P.Vondruška)	10-12
D.	Kryptografie a normy II. (PKCS #3) (J.Pinkava)	13-15
E.	Prohlášení ÚOOÚ pro tisk	16-19
F.	Statistika návštěvnosti www stránky GCUCMP	20-22
G.	Letem šifrovým světem	23-24
H.	Závěrečné informace	24

Příloha : ZoEP.htm

Dnešní užitečnou přílohou je plné znění zákona č.227/2000 Sb.- "Zákon o elektronickém podpisu a o změně některých dalších zákonů (Zákon o elektronickém podpisu)", který nabyl účinnosti 1.10.2000.

Crypto-World 11/2000

A.	Soutěž ! Část III. - Jednoduchá transpozice	2 - 6
B.	Působnost zákona o elektronickém podpisu a výklad hlavních pojmů -Informace o přednášce	7 - 9
C.	Rozjímání nad ZoEP, zvláště pak nad § 11 (P.Vondruška)	10 - 13
D.	Kryptografie a normy III. (PKCS #5) (J.Pinkava)	14 - 17
E.	Letem šifrovým světem	18 - 19
F.	Závěrečné informace	19

Crypto-World 12/2000

A.	Soutěž (průběžný stav, informace o 1.ceně) (P.Vondruška)	2 - 3
B.	Substituce složitá - periodické heslo, srovnaná abeceda (P.Tesař)	4 - 10
C.	CRYPTONESSIE (J.Pinkava)	11 - 18
D.	Kryptografie a normy IV. (PKCS #6, #7, #8) (J.Pinkava)	18 - 19
E.	Letem šifrovým světem	20 - 21
F.	Závěrečné informace	21

Příloha : teze.zip - zkrácené verze prezentací ÚOOÚ použité při předložení tezí k Zákonu o elektronickém podpisu (§6, §17) dne 4.12.2000 a teze příslušné vyhlášky.

Crypto-World Vánoce/2000

A.	Vánoční rozjímání nad jistými historickými analogiemi Zákona o elektronickém podpisu a zákony přijatými před sto a před tisícem let	2 -3
B.	Soutěž - závěrečný stav	4
C.	I.kolo	5 -7
D.	II.kolo	8 -9
E.	III.kolo	10-12
F.	IV.kolo	12-13
G.	PC GLOBE CZ	14
H.	I.CA	15
I.	Závěrečné informace	16

2001

Crypto-World 1/2001

A.	Je RSA bezpečné ? (P.Vondruška)	2 - 10
B.	Připravované normy k EP v rámci Evropské Unie (J.Pinkava)	11 - 14
C.	Kryptografie a normy V. (PKCS #9, 10, 11, 12, 15) (J.Pinkava)	15 - 19
D.	Letem šifrovým světem	20 - 21
E.	Závěrečné informace	22

Příloha: trustcert.pdf (upoutávka na služby Certifikační Autority TrustCert)

Crypto-World 2/2001

A.	CRYPTREC - japonská obdoba NESSIE (informace) (J.Pinkava)	2 - 3
B.	Připravované normy k EP v rámci Evropské Unie II. (J.Pinkava)	4 - 6
C.	K návrhu zákona o elektronickém podpisu, jeho dopadu na ekonomiku a bezpečnostních hlediscích (J.Hrubý, I.Mokoš)	7 - 14
D.	Mobilní telefony (komunikace, bezpečnost) (J.Kobelka)	15- 17
E.	NIST software pro statistické testování náhodných a pseudonáhodných generátorů pro kryptografické účely (J.Pinkava)	18 - 27
F.	Letem šifrovým světem	27 - 28
G.	Závěrečné informace	29

Crypto-World 3/2001

A.	Typy elektronických podpisů (P.Vondruška)	2 - 9
B.	Tiskové prohlášení č.14, Microsoft, 15.2.2001	10
C.	Kryptografický modul MicroCzech I. (P. Vondruška)	11 - 16
D.	Názor na článek J.Hrubý, I.Mokoš z 2/2001 (P. Vondruška)	17 - 18
E.	Názor na článek J.Hrubý, I.Mokoš z 2/2001 (J. Pinkava)	19 - 20
F.	Letem šifrovým světem	21 - 22
G.	Závěrečné informace	23

Crypto-World 4/2001

A.	Kryptografie a normy, díl 6. - Normy IETF - S/MIME (J. Pinkava)	2 - 6
B.	e-komunikace, e-platby, e-projekty, e-platformy a „velcí hráči“ (P. Vondruška)	7 - 13
C.	Jak se lámal podpis (útok na PGP) (M. Šedivý)	14 - 18
D.	Smart-Card with Quantum Entanglement (J.Hrubý, O.Haděrka)	19 - 22
E.	Letem šifrovým světem	23 - 24
F.	Závěrečné informace	25

Crypto-World 5/2001

A.	Bezpečnost osobních počítačů (B. Schneier)	2 - 3
----	--	-------

B.	Záhadná páska z Prahy I.díl (P.Vondruška, J.Janečko)	4 - 6
C.	Ukončení platnosti, zneplatnění (a zrušení) certifikátu, I.díl (J.Prokeš)	7 - 8
D.	Identrus - celosvětový systém PKI (J.Ulehla)	9 -11
E.	Kryptografie a normy, díl 7. - Normy IETF - S/MIME (J. Pinkava)	12-17
F.	Letem šifrovým světem	18
G.	Závěrečné informace	19

Příloha : priloha.zip : součástí jsou soubory obsah.rtf (obsah všech dosud vyšlých e-zinů Crypto-World) a mystery.mid (viz. článek "Záhadná páska z Prahy")

Crypto-World 6/2001

A.	Záhadná páska z Prahy II.díl (P.Vondruška, J.Janečko)	2- 6
B.	Radioaktivní rozpad a kryptografické klíče (L.Smolík)	7-9
C.	Kryptografie a normy, díl 8. - Normy IETF - S/MIME (J. Pinkava)	10-13
D.	Počítačový kurs Lidových novin (P.Vondruška)	14-15
E.	Security and Protection of Information (D. Cvrček)	16
F.	Právní odpovědnost poskytovatelů (J.Matejka)	17-23
G.	Ukončení platnosti, zneplatnění (a zrušení) certifikátu, II.díl (J.Prokeš)	24-25
H.	Letem šifrovým světem	26-27
I.	Závěrečné informace	28

Příloha : priloha6.zip

(fotografie Security 2001, témata přednášek na konferenci Eurocrypt'2001)

Crypto-World 78/2001

A.	Malé ohlédnutí za dalším rokem Crypto-Worldu (P.Vondruška)	2-5
B.	Standardizační proces v oblasti elektronického podpisu v EU a ČR (D.Bosáková, P.Vondruška)	6-13
C.	XML signature (J.Klimeš)	14-18
D.	O základním výzkumu v HP laboratořích v Bristolu, průmyslovém rozvoji a ekonomickém růstu (J. Hrubý)	19-21
E.	Letem šifrovým světem	22-27
1.	Skljarov (ElcomSoft) zatčen za šíření demoverze programu ke čtení zabezpečených elektronických knih (P.Vondruška)	22
2.	FIPS PUB 140-2, bezpečnostní požadavky na kryptografické moduly (J.Pinkava)	23-24
3.	Faktorizace velkých čísel - nová podoba výzvy RSA (J.Pinkava)	24-25
4. -7.	Další krátké informace	26-27
F.	Závěrečné informace	28

Příloha : priloha78.zip (dopis pana Sůvy - detailní informace k horké sazbě, viz. článek Záhadná páska z Prahy, Crypto-World 6/2001)

Crypto-World 9/2001

A.	Soutěž 2001, I.část (Kódová kniha) (P.Vondruška)	2 - 8
B.	Dostupnost informací o ukončení platnosti a zneplatnění kvalifikovaného certifikátu (P.Vondruška)	8 -10
C.	Digitální certifikáty, Část 1. (J.Pinkava)	11-14

D.	E-Europe (přehled aktuální legislativy v ES) (J.Hobza, P.Vondruška)	15-16
E.	Útok na RSAES-OAEP (J.Hobza)	17-18
F.	Letem šifrovým světem	19-22
G.	Závěrečné informace	23

Crypto-World 10/2001

A.	Soutěž 2001, II.část (Absolutně bezpečný systém) (P.Vondruška)	2 - 5
B.	E-komunikace začíná ! (?) (P.Vondruška)	7-11
C.	Digitální certifikáty, Část 2. (J.Pinkava)	12-14
D.	Šifrátor do vrecka (L.Cechlár)	15-16
E.	Interview s hackerem	17-19
F.	Mikulášská kryptobesídka	20-21
G.	Letem šifrovým světem	22-23
H.	Závěrečné informace	24

Příloha : Vyhláška 366/2001 Sb. (366_2001.pdf)

(prováděcí vyhláška ÚOOÚ k Zákonu o elektronickém podpisu č.227/2000 ve tvaru předaném k vyhlášení ve Sbírce zákonů)

Crypto-World 11/2001

A.	Soutěž 2001, III.část (Asymetrická kryptografie - RSA)	2 - 7
B.	NESSIE, A Status Report (Bart Preneel)	8 -11
C.	Dostupnost informací o ukončení platnosti, zneplatnění a zrušení kvalifikovaného certifikátu (P.Vondruška)	12-16
D.	Odpovědnost a přechod odpovědnosti ve smyslu zákona o elektronickém podpisu (J.Hobza)	17-19
E.	Eliptické křivky a kryptografie (J.Pinkava)	20-22
F.	Mikulášská kryptobesídka (V.Matyáš,Z.Říha)	23
G.	Letem šifrovým světem	24 -25
H.	Závěrečné informace	26

Crypto-World 12/2001

A.	Soutěž 2001, IV.část (P.Vondruška)	2 - 7
B.	Kryptografie a normy - Norma X.509, verze 4 (J.Pinkava)	8 -10
C.	Asyřané a výhradní kontrola (R.Haubert)	11-13
D.	Jak se (ne)spoléhat na elektronický podpis (J.Hobza)	13-14
E.	Některé odlišnosti českého zákona o elektronickém podpisu a návrhu poslaneckého slovenského zákona o elektronickém podpisu (D.Brechlerová)	15-19
F.	Letem šifrovým světem	19-21
G.	Závěrečné informace	22

Příloha: uloha7.wav

2002

Crypto-World 1/2002

A.	Soutěž 2001 (výsledky a řešení) (P.Vondruška)	2 - 15
B.	Santa's Crypto – Mikulášská kryptobesídka (D.Cvrček,V.Matyáš)	16 -17
C.	O postranních kanálech, nové maskovací technice a jejím konkrétním využití proti Mangerovu útoku na PKCS#1 (Klíma, Rosa)	18 -32
D.	Velikonoční kryptologie	33
E.	Letem šifrovým světem	34
F.	Závěrečné informace	34

Crypto-World 2/2002

A.	Vyhláška č.366/2001 Sb., bezpečný prostředek pro vytváření elektronického podpisu a nástroj elektronického podpisu (P.Vondruška)	2 - 8
B.	RUNS testy (P.Tesař)	9 -13
C.	Velikonoční kryptologie (V.Matyáš)	13
D.	Terminologie (V.Klíma)	14
E.	Letem šifrovým světem	15-16
F.	Závěrečné informace	17

Příloha: Program pro naše čtenáře : "Hašák ver. 0.9" (viz. letem šifrovým světem)
(V programu Hasak.exe byla chyba, nyní lze stáhnout s opraveným programem DataHash)

Crypto-World 3/2002

A.	Vysvětlení základních pojmů zákona o elektronickém podpisu (D.Bosáková, P.Vondruška)	2-17
B.	Digitální certifikáty. IETF-PKIX část 1. (J.Pinkava)	17-20
C.	Bezpečnost RSA – význačný posun? (J.Pinkava)	21
D.	Terminologie II. (V.Klíma)	22
E.	Letem šifrovým světem	23-26
	1. O čem jsme psali v březnu roku 2000 a 2001	
	2. Encryption in corporate networks can be 'pried open'	
	3. ISO-registr kryptografických algoritmů byl zpřístupněn On-Line!	
	4. Velikonoční kryptobesídka , 3. - 4. dubna 2002 v Brno	
	5. Užší elektronický podpis podnikanie? Zámery a prvé praktické skúsenosti, 20.2.2002, Bratislava	
	6. Seminář GnuPG, 5. 4. 2002 v Praze	
	7. DATAKON 2002, 19. - 22. 10. 2002, Brno	
F.	Závěrečné informace	27

Crypto-World 4/2002

A.	Dubnová krypto-inspirace (připravil P.Vondruška)	2-3
B.	Kryptografické algoritmy a jejich parametry pro bezpečné vytváření a ověřování zaručeného elektronického podpisu (L.Stachovcová)	4-11
C.	Digitální certifikáty. IETF-PKIX část 2. (J.Pinkava)	12-15
D.	Kritika článku "Bezpečnost RSA - význačný posun?"(V.Klíma)	16-17
E.	Letem šifrovým světem	18-22

1.	Velikonoční kryptologie	
2.	Elektronický podpis autorů Bosáková, Kučerová, Peca, Vondruška	
3.	Eurocrypt 2002	
4.	e-Government v Dolním Sasku	
5.	České fórum pro informační společnost	
6.	O čem jsme psali v dubnu roku 2000 a 2001	
F.	Závěrečné informace	22

Crypto-World 5/2002

A.	Ověření certifikátu poskytovatele (P.Vondruška)	2-4
B.	Radioaktivní rozpad a kryptografické klíče (L.Smolík, D.Schmidt)	5-8
C.	Digitální certifikáty. IETF-PKIX část 3. (J.Pinkava)	9-12
D.	Je 1024-bitová délka klíče RSA dostatečná? (J.Pinkava)	13-18
E.	Studentská bezpečnostní a kryptologická soutěž - SBKS'02	19
F.	Letem šifrovým světem	20-22
G.	Závěrečné informace	23

Příloha: SBKS 2002 - výzva pro autory cfp.pdf

Crypto-World 6/2002

A.	Historie a statistika Crypto-Worldu (P.Vondruška)	2-4
B.	Digitální certifikáty. IETF-PKIX část 4. (J.Pinkava)	5-8
C.	Bezpečnost informačního systému pro certifikační služby (ISCS) a objektová bezpečnost (P.Vondruška)	9-16
D.	Informace - Cryptology ePrint Archive (V.Klíma)	17
E.	Letem šifrovým světem	18-19
1.	Kritika článku "Je 1024-bitová délka klíče RSA dostatečná?" (Crypto-World 5/2002)	
2.	Zákon o elektronickém podpisu novelizován !!! - Zákon č. 226/2002 Sb.	
3.	Hackeri pomozte !	
4.	O čem jsme psali v červnu 2000 a 2001	
F.	Závěrečné informace	20

Crypto-World 78/2002

A.	Hackeri pomozte II. (poučný příběh se šťastným koncem) (P.Vondruška)	2
B.	Režimy činnosti kryptografických algoritmů (P.Vondruška)	3-6
C.	Digitální certifikáty. IETF-PKIX část 5. (J.Pinkava)	7-10
D.	Elektronický podpis - projekty v Evropské Unii. I.část (J.Pinkava)	11-16
E.	Komparace českého zákona o elektronickém podpisu a slovenského zákona o elektronickom podpise s přihlédnutím k plnění požadavků Směrnice 1999/93/ES. I.část (J.Hobza)	17-18
F.	Malá poznámka k právnímu významu pojmu listina se zřetelem k jeho podepisování (J.Matejka)	19-21
G.	Pozvánka na BIN 2002 (11.9.2002)	22
H.	Letem šifrovým světem	23-26
I.	Závěrečné informace	27

Crypto-World 9/2002

A.	Deset kroků k e-komunikaci občana se státem (P.Vondruška)	2 - 8
B.	Digitální certifikáty. IETF-PKIX část 6. (J.Pinkava)	9 - 11
C.	Elektronický podpis - projekty v Evropské Unii. II.část (J.Pinkava)	12-16
D.	Komparace českého zákona o elektronickém podpisu a slovenského zákona o elektronickom podpise s přihlédnutím k plnění požadavků Směrnice 1999/93/ES. II.část (J.Hobza)	17-19
E.	Komentář k článku RNDr. Tesaře : Runs Testy (L.Smolík)	20-22
F.	Konference	23-25
G.	Letem šifrovým světem	26-27
H.	Závěrečné informace	28

Crypto-World 10/2002

A.	Úvodní komentář (P.Vondruška)	2 - 5
B.	Elektronický podpis (J.Hobza)	6 - 24
C.	Mikulášská kryptobesídka	25
D.	Letem šifrovým světem	26
E.	Závěrečné informace	27

Crypto-World 11/2002

A.	Topologie certifikačních autorit (P.Vondruška)	2 - 9
B.	Srovnání výkonnosti hašovacích algoritmů SHA-1, SHA-256, SHA-384 a SHA-512 (M.Kumpošt)	10-16
C.	Informace z aktuálních kryptografických konferencí (J.Pinkava)	
	Konference ECC2002	17-18
	Konference CHES 2002	18-20
	CRYPTO 2002	20-21
D.	The RSA Challenge Numbers	22-23
E.	Letem šifrovým světem	24-25
F.	Závěrečné informace	26

Crypto-World 12/2002

A.	Rijndael: beyond the AES (V.Rijmen, J.Daemen, P.Barreto)	1 -10
B.	Digitální certifikáty. IETF-PKIX část 7. (J.Pinkava)	11-13
C.	Profil kvalifikovaného certifikátu (J.Hobza)	14-21
D.	Nový útok (XSL) na AES (připravil P.Vondruška)	22
E.	Operační systém Windows 2000 získal certifikát bezpečnosti Common Criteria (připravil P.Vondruška)	23
F.	O čem jsme psali v prosinci 1999-2001	24
G.	Závěrečné informace	25

Příloha : EAL4.jpg (certifikát operačního systému W2k podle CC na EAL4)

2003

Crypto-World 1/2003

A.	České technické normy a svět (P.Vondruška)	2 - 4
B.	Digitální certifikáty. IETF-PKIX část 8. Protokol pro časové značky (J.Pinkava)	5 - 9
C.	Profil kvalifikovaného certifikátu, Část II. (J. Hobza)	10 - 17
D.	Letem šifrovým světem	18 - 20
E.	Závěrečné informace	21
Příloha : Crypto_p1.pdf		
CEN Workshop Agreements (dokumenty vztahující se k elektronickému podpisu)		

Crypto-World 2/2003

A.	České technické normy a svět, II.část (Národní normalizační proces) (P.Vondruška)	2 - 4
B.	Kryptografie a normy. Digitální certifikáty. IETF-PKIX část 9. Protokol SCVP (J.Pinkava)	5 - 10
C.	Faktorizace a zařízení TWIRL (J.Pinkava)	11-12
D.	NIST - dokument Key Management	13-16
E.	Letem šifrovým světem - Kurs "kryptologie" na MFF UK Praha - Za použití šifrování do vězení - Hoax jdbgmgr.exe - Interview - AEC uvedla do provozu certifikační autoritu TrustPort - 6. ročník konference - Information Systems Implementation and Modelling ISIM'03 - O čem jsme psali v únoru 2000 - 2002	17-21
F.	Závěrečné informace	22
Příloha : Crypto_p2.pdf		
Přehled dokumentů ETSI, které se zabývají elektronickým podpisem (ETSI - European Telecommunication Standards Institute)		10 stran

Crypto-World 3/2003

A.	České technické normy a svět, III.část (Národní normalizační proces) (P.Vondruška)	2 - 6
B.	Přehled norem v oblasti bezpečnosti informačních technologií (normy vyvíjené ISO/IEC JTC1 SC27 a ISO TC 68) zavedených do soustavy českých norem (P. Wallenfels)	7-10
C.	Digitální certifikáty. IETF-PKIX část 10. CVP(J.Pinkava)	11-13
D.	Obecnost neznamená nejednoznačnost, aneb ještě malá poznámka k některým nedostatkům zákona o elektronickém podpisu před jeho novelizací (J.Matejka)	14-19
E.	Letem šifrovým světem	20-23
F.	Závěrečné informace	24
Příloha : crypto_p3.pdf		
Mezinárodní a zahraniční normalizační instituce		3 strany

Crypto-World 4/2003

A.	Úvodní slovo (P.Vondruška)	2 - 3
B.	E-válka v zálivu (a okolí...) (P.Vondruška)	4 - 7
C.	Začátek roku 2003 protokolu SSL nepřeje.... (P.Vondruška)	8 - 9
D.	Elíptická kryptografie a kvantové počítače (J.Pinkava)	10 - 11
E.	Digitální certifikáty. IETF-PKIX část 11. Archivace elektronických dokumentů (J.Pinkava)	12-18
F.	Letem šifrovým světem - Mobilní telefon s vestavěným utajovačem TopSec GSM - SIM karty lze klonovat za sedm minut - Daňová přiznání s elektronickým podpisem Pozvánky (vstup zdarma): - 16.4.2003 – Cesty k unitární teorii z pohledu astrofyziky (RNDr. Jiří Grygar, CSc.) - 17.4.2003 - seminář "Broadband Visions 2003" - 24.4.2003 - seminář "Enterprise Content Management"	19-20
G.	Závěrečné informace	21

Crypto-World 5/2003

A.	E-podpisy? (P.Vondruška)	2 - 4
B.	RFC (Request For Comment) (P.Vondruška)	5 - 8
C.	Digitální certifikáty. IETF-PKIX část 12. Atributové certifikáty - profil dle rfc.3281 - díl 1. (J.Pinkava)	9 - 11
D.	Konference Eurocrypt 2003 (J.Pinkava)	12 - 13
E.	Standard pro kategorizaci bezpečnosti vládních informací a informačních systémů - FIPS PUB 199 (P.Vondruška)	14 - 16
F.	Směrnice OECD pro bezpečnost informačních systémů a sítí: směrem ke kultuře bezpečnosti (P.Vondruška)	17 - 18
G.	Letem šifrovým světem	19 - 23
H.	Závěrečné informace	24

Crypto-World 6/2003

A.	Nebezpečí internetových řešení (M.Kuchař)	2-6
B.	Digitální certifikáty. IETF-PKIX část 13. Atributové certifikáty – díl 2. (J.Pinkava)	7-10
C.	Kryptografické protokoly s nulovým předáním znalostí(J.Pinkava)	11-12
D.	Elektronické peníze (P.Vondruška)	13-20
E.	Letem šifrovým světem	21-23
F.	Závěrečné informace	24

Crypto-World 7-8/2003

A.	Cesta kryptologie do nového tisíciletí I. (P.Vondruška)	2 - 4
B.	Digitální certifikáty. IETF-PKIX část 14. Atributové certifikáty - 3.díl (J.Pinkava)	5-6
C.	Jak si vybrat certifikační autoritu (D.Doležal)	7-14
D.	K problematice šíření nevyžádaných a obtěžujících sdělení prostřednictvím Internetu, zejména pak jeho elektronické pošty, část I. (J.Matejka)	15-20
E.	TWIRL a délka klíčů algoritmu RSA (J.Pinkava)	21
F.	Postranní kanály v Cryptobytes (J.Pinkava)	22
G.	Podařilo se dokázat, že P není rovno NP? (J.Pinkava)	23-24
H.	Letem šifrovým světem (P.Vondruška)	25-28
I.	Závěrečné informace	29

Příloha: "zábavná steganografie" (steganografie.doc)

Crypto-World 9/2003

A.	Soutěž 2003 začíná ! (P.Vondruška)	2 – 3
B.	Cesta kryptologie do nového tisíciletí II. (Od zákopové války k asymetrické kryptografii) (P.Vondruška)	4 - 7
C.	Kryptografie a normy. Politika pro vydávání atributových certifikátů, část 1. (J.Pinkava)	8 -11
D.	K problematice šíření nevyžádaných a obtěžujících sdělení prostřednictvím Internetu, zejména pak jeho elektronické pošty, část II. (J.Matejka)	12-15
E.	Informace o konferenci CRYPTO 2003 (J.Hrubý)	16-19
F.	AEC Trustmail (recenze), (M.Till)	20-24
G.	Letem šifrovým světem	25-26
H.	Závěrečné informace	27

Crypto-World 10/2003

A.	Soutěž v luštění 2003 (P.Vondruška)	2
B.	Cesta kryptologie do nového tisíciletí III. (Od asymetrické kryptografie k elektronickému podpisu) (P.Vondruška)	3 - 7
C.	K oprávnění zaměstnavatele kontrolovat práci zaměstnance pomocí moderních technologií (J.Matejka)	8-19
D.	Jednoduchá a automatická aktualizace (D.Doležal)	20-21
E.	Recenze knihy „Řízení rizik“ autorů V. Smejkal a K. Raise (A. Katolický)	22-24
F.	Letem šifrovým světem	25-26
G.	Závěrečné informace	27

Crypto-World 11/2003

A.	Soutěž 2003 – průběžná zpráva (P.Vondruška)	2
B.	Mikulášská kryptobesídka – Program	3
C.	Cesta kryptologie do nového tisíciletí IV. (Od NESSIE ke kvantovému počítači) (P.Vondruška)	4– 7
D.	Kryptografie a normy. Politika pro vydávání atributových certifikátů, část 2. (J.Pinkava)	8 –11
E.	Archivace elektronických dokumentů (J.Pinkava)	12-16

F.	Unifikace procesů a normy v EU (J.Hrubý)	17-27
G.	Letem šifrovým světem	27-29
H.	Závěrečné informace	30

Crypto-World 12/2003

A.	Soutěž 2003 skončila (P.Vondruška)	2-4
B.	Soutěžní úlohy č.1-6 (P.Vondruška)	5-8
C.	Řešení úloh č.7-9 (J.Vorlíček)	9-20
D.	Letem šifrovým světem	21-23
	I. Nová regulace vývozu silné kryptografie z USA!	
	II. Čtyřicáté Mersennovo prvočíslo bylo nalezeno!	
	III. Nový rekord ve faktorizaci (RSA-576)	
	IV. Rozšířen standard pro hashovací funkce FIPS 180-2	
	V. GSMK CryptoPhone 100	
E.	Závěrečné informace	24

Příloha: pf_2004.jpg

2004

Crypto-World 1/2004

A.	Tajemství Voynichova rukopisu odhaleno? (P.Vondruška)	2
B.	Vztah důvěry mezi můstkovými certifikačními autoritami (P.Vondruška)	3-9
C.	Požadavky na politiku poskytovatele, který vydává atributové certifikáty, které lze používat spolu s kvalifikovanými certifikáty (Technical report ETSI 102 158), Část 1.(J.Pinkava)	10-13
D.	Archivace elektronických dokumentů, část 2.(J.Pinkava)	14-15
E.	ETSI a CEN/ISSS - nové normativní dokumenty(J.Pinkava)	16-17
F.	Letem šifrovým světem	18-20
G.	Závěrečné informace	21

Crypto-World 2/2004

A.	Opožděný úvodník (P.Vondruška)	2-4
B.	Jak jsem pochopil ochranu informace (T.Beneš)	5-9
C.	Požadavky na politiku poskytovatele, který vydává atributové certifikáty, které lze používat spolu s kvalifikovanými certifikáty (Technical report ETSI 102 158), Část 2. (J.Pinkava)	10-13
D.	Archivace elektronických dokumentů, část 3. (J.Pinkava)	14-15
E.	IFIP a bezpečnost IS (D.Brechlerová)	16-17
F.	Letem šifrovým světem	18-22
-	Novinky (23.1.2004-14.2.2004)	
-	O čem jsme psali v únoru 2000 - 2003	
G.	Závěrečné informace	23

Crypto-World 3/2004

A.	Nastavení prohlížeče IE pro používání kontroly CRL (P.Vondruška)	2-4
B.	Jak jsem pochopil ochranu informace, část 2. (T.Beneš)	5-9
C.	Požadavky na politiku poskytovatele, který vydává atributové certifikáty, které lze používat spolu s kvalifikovanými certifikáty (Technical report ETSI 102 158), část 3. (J.Pinkava)	10-12
D.	Archivace elektronických dokumentů, část 4. (J.Pinkava)	13-16
E.	Letem šifrovým světem (TR,JP,PV)	17-19
F.	Závěrečné informace	20

Crypto-World 4/2004

A.	Novela zákona o elektronickém podpisu a časové razítko (V.Smejkal)	2-3
B.	Jak jsem pochopil ochranu informace, část 3. (T.Beneš)	4-8
C.	Požadavky na politiku poskytovatele, který vydává atributové certifikáty, které lze používat spolu s kvalifikovanými certifikáty (Technical report ETSI 102 158), část 4. (J.Pinkava)	9-11
D.	Použití zabezpečených serverů v síti Internet a prohlížeč Mozilla (pro začátečníky), část 1. (P.Vondruška)	12-16
E.	Letem šifrovým světem (TR,JP,PV)	17-18
F.	Závěrečné informace	19

Crypto-World 5/2004

A.	Začněte používat elektronický podpis (P.Komárek)	2
B.	Program STORK - vstupní dokumenty, příprava E-CRYPT (J.Pinkava)	3-9
C.	Použití zabezpečených serverů v síti Internet a prohlížeč Mozilla (pro začátečníky), část 2. (P.Vondruška)	10-16
D.	Zabezpečení rozvoja elektronického podpisu v štátnej správe (NBÚ SK)	17-20
E.	Zmysel koreňovej certifikačnej autority (R.Rexa)	21-22
F.	Letem šifrovým světem	23-24
G.	Závěrečné informace	25

Crypto-World 6/2004

A.	Měsíc prvočísel (P.Vondruška)	2-5
B.	Statistický rozbor největšího prvočísla (P.Tesař)	6-7
C.	Program STORK - vstupní dokumenty, příprava (E-CRYPT), část 2. (J.Pinkava)	8-16
D.	Letem šifrovým světem	17-18
E.	Závěrečné informace	19

Crypto-World 78/2004

A.	Soutěž v luštění 2004 (P.Vondruška)	2-3
B.	Hackeři, Crakeři, Rhybáři a Lamy (P.Vondruška)	4-12
C.	Přehledy v oblasti IT bezpečnosti za poslední rok (J.Pinkava)	13-21
D.	Letem šifrovým světem	22-24
E.	Závěrečné informace	25

Crypto-World 9/2004

A.	Soutěž v luštění 2004 začala ! (P.Vondruška)	2-3
B.	Přehled úloh - I.kolo (P.Vondruška)	4-5
C.	Crypto-World slaví pět let od svého založení (P.Vondruška)	6-7
D.	Reverse-engineering kryptografického modulu (Daniel Cvrček, Mike Bond, Steven J. Murdoch)	8-14
E.	Hashovací funkce v roce 2004 (J.Pinkava)	15-18
F.	Letem šifrovým světem - O čem jsme psali	19-20
G.	Závěrečné informace	21

Crypto-World 10/2004

A.	Soutěž v luštění pokračuje druhým kolem ! (P.Vondruška)	2-4
B.	Rozjímání nad PKI (P.Vondruška)	5-8
C.	Platnost elektronického podpisu a hledisko času (J.Pinkava)	9-13
D.	Anotace - Hashovací funkce v roce 2004 (J.Pinkava)	14
E.	Komentář k nepřesnostem v článku J.Pinkava : Hashovací funkce v roce 2004 (Crypto-World 9/2004) (V.Klíma)	15-17
F.	O čem jsme psali v říjnu (1999-2003)	18
G.	Závěrečné informace	19

Příloha : J.Pinkava - Hashovací funkce v roce 2004 , hash_2004.pdf

Crypto-World 11/2004

A.	Soutěž 2004 – úlohy závěrečného kola! (P.Vondruška)	2-4
B.	Jedno-dvoumístná záměna (P.Vondruška)	5-6
C.	Fleissnerova otočná mřížka (P.Vondruška)	7-8
D.	Formáty elektronických podpisů (J.Pinkava)	9-13
E.	Elektronická faktúra a elektronické daňové priznanie aj bez zaručeného elektronického podpisu. (R.Rexa)	14
F.	Nedůvěřujte kryptologům (V.Klíma)	15
G.	O čem jsme psali v listopadu 1999-2003	16
H.	Závěrečné informace	17

Příloha : Crypto-World 11/2004 – speciál (24 stran)
(V.Klíma : Nedůvěřujte kryptologům, ke stažení na adrese :
<http://crypto-world.info/index2.php?vyber=casop6>)

Crypto-World 12/2004

A.	Soutěž 2004 – úlohy a jejich řešení (M.Foríšek, P.Vondruška)	2-22
B.	Čtenáři sobě (z e-mailů řešitelů soutěže 2004)	23-25
C.	O čem jsme psali v prosinci 1999-2003	26-27
D.	Závěrečné informace	28

Příloha : PF2005.jpg

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 neziskatelnosti 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

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 2000-2005	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 2000-2005	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 2000-2005	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 2000-2005	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 2000-2005	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 2000-2005	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 2000-2005	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 2000-2005	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 2000-2005	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

2007

Crypto-World 1/2007

A.	Osobní doklady x identifikace, autentizace, autorizace (L.Dostálek, M.Hojsík)	2-5
B.	Bezpečnost elektronických pasů, část II. (Z.Říha, P.Švenda, V.Matyáš)	6-12
C.	XML bezpečnost, část I. (D. Brechlerová)	13-25
D.	Elektronická fakturace (L.Dostálek, M.Hojsík)	26-33
E.	O čem jsme psali v lednu 2000 -2006	34
F.	Závěrečné informace	35

Crypto-World 2/2007

A.	Najväčšia tma je pod lampou – STEGANOGRAFIA, část I. (R.Cinkais)	2-9
B.	XML bezpečnost, část II. (D. Brechlerová)	10-20
C.	Přehled dokumentů ETSI v oblasti elektronického podpisu, časových razítek a kvalifikovaných certifikátů (V.Sudzina)	21-22
D.	O čem jsme psali v únoru 2000 - 2006	23-24
E.	Závěrečné informace	25

Crypto-World 3/2007

A.	O speciální blokované šifře DN a hašovací funkci HDN (T.Rosa)	2-3
B.	Rodina speciálních blokovaných šifer DN a hašovacích funkcí nové generace HDN typu SNMAC (V.Klíma)	4-26
C.	Najväčšia tma je pod lampou – STEGANOGRAFIA, část II. (R.Cinkais)	27-33
D.	Šifrování v MS Office (P.Tesař)	34
E.	O čem jsme psali v březnu 2000 – 2006	35-36
F.	Závěrečné informace	37

Crypto-World 4/2007

A.	Rodina speciálních blokovaných šifer DN a hašovacích funkcí nové generace HDN typu SNMAC, část II. - Dodatky (V.Klíma)	2-14
B.	Zachycené a šifrové telegramy dokazují, že demokraté se během voleb snažili podplácet! (P.Vondruška)	15-21
C.	Kircherovo šifrování aneb Dobrý voják Švejk	22-25
D.	Úloha k luštění ... (P.Vondruška)	26
E.	O čem jsme psali v dubnu 2000 -2006	27-28
F.	Závěrečné informace	29

Crypto-World 5/2007

A.	Z dějin československé kryptografie, část I., Československý šifrátor MAGDA (K.Šklíba)	2-5
B.	Řešení dubnové úlohy (P.Vondruška)	6-7
C.	Bealovy šifry (P.Vondruška)	8-19
D.	O čem jsme psali v květnu 2000-2006	20-21
E.	Závěrečné informace	22

Crypto-World 6/2007

A.	Přehled a historie polyalfabetických šifer (P.Vondruška)	2-11
B.	Matematizace komplexní bezpečnosti v ČR, část I. (J.Hrubý)	12-20
C.	Mikulášská kryptobesídka, Call for Papers	21
D.	O čem jsme psali v červnu 2000-2006	22-23
E.	Závěrečné informace	24

Příloha: Mikulášská kryptobesídka (6.-7.12.2007)- MKB2007_CallForPapers_cerven.pdf

Crypto-World 7/2007 (mimořádné vydání)

- | | | |
|----|---|-----|
| A. | Počítačová kriminalita v návrhu nového trestního zákoníku (2007),
Výzva ke kontrole navrženého paragrafového znění (V.Klíma) | 2-5 |
| B. | Závěrečné informace | 6 |

Crypto-World 78/2007

- | | | |
|----|---|-------|
| A. | Podzimní soutěž v luštění 2007, úvodní informace | 2 |
| B. | Štěpán Schmidt (prolog Soutěže 2007) | 3-4 |
| C. | Z dějin československé kryptografie, část II.,
Československé šifrovací stroje z období 1930–1939 a 1945–1955 (K.Šklíba) | 5-9 |
| D. | Matematizace komplexní bezpečnosti v ČR, část II. (J.Hrubý) | 10-16 |
| E. | O čem jsme psali v létě 2000-2006 | 17-18 |
| F. | Závěrečné informace | 19 |

Crypto-World 9/2007

- | | | |
|----|---|-------|
| A. | Soutěž v luštění 2007 začala! (P.Vondruška) | 2-4 |
| B. | Mládí Štěpána Schmidta (doprovodný text k I.kolu soutěže) | 5-11 |
| C. | Názor čtenáře k návrhu TrZ (T.Sekera) | 12 |
| D. | Mikulášská kryptobesídka | 13 |
| E. | O čem jsme psali v září 2000-2006 | 14-15 |
| F. | Závěrečné informace | 16 |

Příloha: Mikulášská kryptobesídka - Call for Papers (MKB_CFP.PDF)

Crypto-World 10/2007

- | | | |
|----|---|-------|
| A. | Štěpán Schmidt v Černé komoře (doprovodný text k III.kolu soutěže) | 2-9 |
| B. | Z dějin československé kryptografie, část III.,
Paměti armádního šifranta (J.Knížek) | 10-23 |
| C. | O čem jsme psali v říjnu 2000-2006 | 24-25 |
| D. | Závěrečné informace | 26 |

Crypto-World 11/2007

- | | | |
|----|---|-------|
| A. | Soutěž v luštění 2007 skončila (P.Vondruška) | 2 |
| B. | Z dějin československé kryptografie, část IV., Československé šifrovací
stroje z období 1955 – 1960. Šifrovací stroj ŠD – 1 (K.Šklíba) | 3-5 |
| C. | Testy obrazové kvality snímačů otisků prstů Suprema
(M.Drahanský, O.Nezhyba) | 6-11 |
| D. | Možnosti odposlechu optických vláken (J.Dušátko) | 12-30 |
| E. | Mikulášská kryptobesídka 2007 – Program (V.Matyáš) | 31-32 |
| F. | Konference EOIF GigaCon (A.Ušcińska) | 33 |
| G. | O čem jsme psali v listopadu 2000-2006 | 33-35 |
| H. | Závěrečné informace | 36 |

Příloha: Příběh Štěpána Schmidta (všechny 4 části ve formátu doc) pribeh.doc

Crypto-World 12/2007

- | | | |
|----|--|-------|
| A. | Soutěž v luštění 2007 – řešení úloh I. kola | 2-10 |
| B. | Soutěž v luštění 2007 – řešení úloh II. kola | 11-15 |
| C. | Soutěž v luštění 2007 – řešení úloh III. kola | 16-25 |
| D. | Soutěž v luštění 2007 – řešení úloh IV. kola | 26-29 |
| E. | Soutěž v luštění 2007 – z poznámek soutěžících | 30-35 |
| F. | O čem jsme psali v prosinci 1999-2006 | 36-37 |
| G. | Závěrečné informace | 38 |

Příloha: program na šifrování a dešifrování homofonních substitucí a nomenklátorů - nomenklator.exe

2008

Crypto-World 1/2008

A.	O kolizích hašovacích funkce Turbo SHA-2 (V. Klíma)	2-13
B.	Z dějin československé kryptografie, část V., Československé šifrovací stroje z období 1955 – 1960. Šifrovací stroj ŠD – 2 (1. díl) (K. Šklíba)	14-17
C.	První česká kryptografická příručka (P. Vondruška)	18-20
D.	Pozvánka - Konference EOIF GigaCon 2008 – Elektronický oběh informací ve firmě	21
E.	O čem jsme psali v lednu 2000-2007	22-23
F.	Závěrečné informace	24

Crypto-World 2/2008

A.	O chystané demonstraci prolomení šifer A5/1 a A5/2	2-9
B.	Podmínky důvěryhodnosti elektronických dokumentů v archívu (Z.Loebel, B.Procházková, J.Šiška, P.Vondruška, I.Zderadička)	10-20
C.	Rozhovor na téma bezpečnost našich webmailů (.cCuMiNn. , P.Vondruška)	21-22
E.	O čem jsme psali v únoru 2000-2007	23-24
F.	Závěrečné informace	25

Crypto-World 3/2008

A.	E-zin 3/2008 + Voynichův rukopis (P.Vondruška)	2-3
B.	Voynichův rukopis (Wikipedia)	4-7
C.	Záhadný Dr. Rafael (J.Hurych)	8-12
D.	Z dějin československé kryptografie, část VI., Československé šifrovací stroje z období 1955 – 1960. Šifrovací stroj ŠD – 2 (2. díl) (K.Šklíba)	13-22
E.	O čem jsme psali v březnu 2000-2007	23-24
F.	Závěrečné informace	25

Crypto-World 4/2008

A.	Hakin9 - jak se bránit ? (P.Vondruška)	2 - 4
B.	MIME formát a NBÚ formát ZEP(ZIP) pre uľahčenie splnenia požiadavky WYSIWYS pri QES (P.Rybár)	5 - 6
C.	Trusted Computing (P.Sušil)	7 - 10
D.	Ještě o Dr. Rafaelovi (Jan B. Hurych)	11-17
E.	O čem jsme psali v dubnu 2000-2007	18-19
F.	Závěrečné informace	20

Crypto-World 5/2008

A.	Příklad útoku na podpisovaný dokument, ktorého typ nie je chránený samotným podpisom (P.Rybar)	2
B.	Speciální bloková šifra - Nová hešovacích funkce. (P.Sušil)	3 – 9
C.	Z dějin československé kryptografie, část VI., Československé šifrovací stroje z období 1960– 1970. Šifrovací stroj ŠD – 3 (K.Šklíba)	10-14
D.	Mikulášská kryptobesídka, Call for Papers	15-17
E.	O čem jsme psali v květnu 2000-2007	18-19
F.	Závěrečné informace	20

Příloha:

- 1) Mikulášská kryptobesídka (4.-5.12.2008): CFP_MKB2008_May.pdf
- 2) Příloha k článku „Příklad útoku na podepsaný dokument ...“ : prikklad.bmp

Crypto-World 6/2008

A.	RFID: Co to vlastně máme v kapse? (M.Hlaváč, T.Rosa)	2 - 17
B.	Bezpečnost PHP aplikací (J.Vrána)	18 - 22
C.	Popis šifrovacího algoritmu Serpent (J.Jeřábek)	24 - 29
D.	O čem jsme psali v červnu 2000-2007	30 – 31
E.	Závěrečné informace	32

Crypto-World 78/2008

A.	Současná kryptologie v praxi (V.Klíma)	2-10
B.	Zabezpečení souborů v kanceláři (L.Caha)	11-17
C.	Z dějin československé kryptografie, část VIII., Trofejní šifrovací stroje používané v Československu v letech 1945 - 1955. Šifrátory ENIGMA, ANNA a STANDARD (K.Šklíba)	18-24
D.	Nové knihy (Biometrie a identita člověka, Autentizace elektronických transakcí a autorizace dat i uživatelů)	25
E.	O čem jsme psali v létě 2000-2007	26-27
F.	Závěrečné informace	28

Crypto-World 9/2008

A.	Podzimní Soutěž v luštění 2008, úvodní informace (P.Vondruška)	2-3
B.	John Wellington (prolog Soutěže 2008) (P.Vondruška)	4-6
C.	Autentizace pomocí Zero-Knowledge protokolů (J.Hajný)	7-13
D.	Recenze knihy: Matyáš, V., Krhovják, J. a kol.: Autorizace elektronických transakcí a autentizace dat i uživatelů (V.J.Jákl)	14-15
E.	O čem jsme psali v září 1999-2007	16-17
F.	Závěrečné informace	18

Crypto-World 10/2008

A.	Podzimní Soutěž v luštění 2008 začíná (P.Vondruška)	2
B.	John Wellington vzpomíná, pokračování příběhu (P.Vondruška)	3-5
C.	Příběh šifrovacího stroje Lorenz SZ (P.Veselý)	6-17
D.	Hašovací funkce COMP128 (P. Sušil)	18-26
E.	O čem jsme psali v říjnu 1999-2007	27-28
F.	Závěrečné informace	29

Příloha: simulátor historického šifrátoru Lorenz SZ 40- lorenz.zip

Crypto-World 11/2008

A.	Podzimní Soutěž v luštění 2008 skončila! (P. Vondruška)	2-4
B.	KYBERNETICKÉ ÚTOKY: RUSKO? – GRUZIE a SVĚT (T.Sekera)	5-11
C.	Kvantový šumátor ve Společné laboratoři optiky UP a Fyzikálního ústavu AV ČR (J. Hrubý)	12-17
D.	Mikulášská kryptobesídka 2008 / SantaCrypt 2008	18-19
E.	O čem jsme psali v listopadu 1999-2007	20-21
F.	Závěrečné informace	22

Crypto-World 12/2008

A.	Závěr soutěže 2008, úlohy, použité systémy, řešení, komentáře řešitelů (P.Vondruška, řešitelé)	2-24
B.	Příběhy Johna Wellingtona (P.Vondruška)	25-33
C.	O čem jsme psali v únoru 2000-2007	34-35
D.	Závěrečné informace	36

Příloha:

- 1) simulátor šifrátoru Lorenz SZ40 <http://soutez2008.crypto-world.info/pribeh/lorenz.zip>
- 2) nastavení pro řešení soutěžních úloh 07,14,15,01: set.zip

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 2000-2008 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 2000-2008 20-21
- E. Závěrečné informace 22

Crypto-World 3/2009

- A. Prvá konference SHA-3 kandidátů (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

2010

Crypto-World 1/2010

A.	Analýza Blue Midnight Wish – útok na vzor (V.Klíma, D. Gligoroski)	2-11
B.	Tajné písmo Martina Kukučina (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.	Dílčí diferenciální vlastnosti zobrazení $A_2(A_1(M))$ 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 finíše (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 Crypt 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

2011

Crypto-World 1/2011

A.	Seriál Československé šifry z obdobia 2. svetovej vojny (J.Kollár)	2
B.	Československé šifry z obdobia 2. svetovej vojny, Diel 1., Šifra TTS (J.Kollár)	3-11
C.	Nové užitečné statistické testy (V.Klíma)	12-13
D.	Československý šifrátor MAGDA – dodatek k popisu v e-zinu Crypto-World 5/2007 (K.Šklíba)	14-15
E.	Báječný svet elektronického podpisu J.Peterky	16
F.	Poslední výzva k príspevku na mezinárodni konferenci Security and Protection of Information konanou 10.– 12. května v Brně (J.Dočkal)	17-18
G.	Problematika infrastruktury veřejných klíčů (PKI), dvoudenní kurz Akademie CZ.NIC (P.Vondruška)	19-20
H.	O čem jsme psali v lednu 1999-2010	21-22
I.	Závěrečné informace	23

Crypto-World 2/2011

A.	Československé šifry z obdobia 2. svetovej vojny Diel 2., Šifra „Rímska dva“ (J.Kollár)	2 - 11
B.	Pár poznámek k šifre použité v deníku Karla Hynka Máchy (P.Vondruška)	12 - 20
C.	O čem jsme psali v únoru 1999-2010	21 - 22
D.	Závěrečné informace	23

Crypto-World 3/2011

A.	Československé šifry z obdobia 2. svetovej vojny Diel 3., Šifra „Rímska osem“ (J.Kollár)	2 - 12
B.	Blinkry blikají aneb komentář ke zprávě NISTu o výběru finalistů SHA-3 (V.Klíma)	13 - 16
C.	Charakteristiky Booleovských funkcí osmi proměnných (P.Tesař)	17 – 22
D.	Odborná skupina kryptologie při JČMF (J.Hrubý)	23 - 24
E.	O čem jsme psali v březnu 2000-2010	25 - 26
F.	Závěrečné informace	27

Crypto-World 4/2011

A.	Československé šifry z obdobia 2. svetovej vojny Diel 4., Šifra „Rímska devät“ (J.Kollár)	2 - 16
B.	Rotorový šifrátor Fialka M-125, Úvod k seriálu (E.Antal, M.Jókay)	17
C.	Rotorový šifrátor Fialka M-125, Diel 1., Popis šifrátoru (E.Antal, M.Jókay)	18 – 27
D.	Problematika infrastruktury veřejných klíčů (PKI), dvoudenní kurz Akademie CZ.NIC (P.Vondruška)	28 - 29
E.	O čem jsme psali v dubnu 2000 – 2010	30 – 31
F.	Závěrečné informace	32

Crypto-World 5/2011

A.	Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 5., Šifra „Rímska desať“ (J.Kollár)	2 - 13
B.	Vzpomínky a poznámky čtenáře k tématu Fialka M-125 (J.Knížek)	14
C.	Rotorový šifrátor Fialka M-125, Diel 2., Porovnanie s viacerimi rotorovými šifratormi (E.Antal, M.Jókay)	15 – 23
D.	Call for Papers Mikulášská kryptobesídka	24
E.	O čem jsme psali v květnu 2000 – 2010	25 - 26
F.	Závěrečné informace	27

Crypto-World 6/2011

A.	Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 6., Šifra „Rímska trinásť“ (J.Kollár)	2 - 11
B.	Kryptografický softwarový nástroj CipherCAD a kryptoanalýza (V.Klíma, V.Plátěnka)	12 - 22
C.	Rotorový šifrátor Fialka M-125, Diel 3., Vybrané vlastnosti šifry (E.Antal, M.Jókay)	23 – 32
D.	Keymaker – studentská soutěž	33
E.	Konference EUROPEN 2011	34
F.	O čem jsme psali v červnu 2000 – 2010	35 - 36
G.	Závěrečné informace	37

Crypto-World 78/2011

A.	Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 7., Šifra „Eva“ (J.Kollár)	2 - 9
B.	sCrib – Hardwarový správce hesel aneb kapesní Enigma (D.Cvrček)	10 - 13
C.	Problematika infrastruktury veřejných klíčů (PKI), dvoudenní kurz Akademie CZ.NIC (P.Vondruška)	14 - 15
D.	Keymaker – studentská soutěž	16
E.	O čem jsme psali v létě 2000 – 2010	17 - 19
F.	Závěrečné informace	20

Crypto-World 9/2011

A.	Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 8., Šifra „Marta“ (J.Kollár)	2 - 8
B.	Rotorový šifrátor Fialka M-125, Diel 4., Implementácia a možnosti využitia (E.Antal, M.Jókay)	9 – 15
C.	Stále mám přístup k dalším CA, tvrdí útočník na DigiNotar (J.Pinkava)	16 - 22
D.	Soutěž 2011 (P.Vondruška)	23
E.	O čem jsme psali v září 2000 – 2010	24 - 26
F.	Závěrečné informace	27

Crypto-World 10/2011

A.	Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 9., Šifra „Růžena“ (J.Kollár)	2 - 12
B.	Soutěž 2011 (P.Vondruška)	13 -14
C.	CryptoWars I. (P.Vondruška)	16 - 20
D.	O čem jsme psali v zřijnu 2000 – 2010	21 - 22
E.	Závěrečné informace	23

Crypto-World 11/2011

nevyšel

Crypto-World 12/2011

nevyšel

2012

Crypto-World 1/2012

A.	Informace redakce, PF 2012	2
B.	Soutěž 2011 – Kompletní příběh včetně úloh, nápověd a jejich správného řešení	3-29
C.	Soutěž 2011 - Statistika soutěže, úspěšnost, řešitelé	30-31
D.	Soutěž 2011 - Ceny a loga sponzorů	31
E.	Pozvánka na SOOM Hacking & Security konferenci	32
F.	O čem jsme psali v lednu 2000 – 2011	33-34
G.	Závěrečné informace	35

Crypto-World 2/2012

A.	Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 10., Šifra „Utility“ (J.Kollár)	2 - 10
B.	Lehká kryptografie a pár slov k hackingu (V.Klíma)	11 - 24
C.	Pozvánka na SCIENCE Cafe v Hradci Králové	25
D.	O čem jsme psali v únoru 2000 – 2011	26 – 27
E.	Závěrečné informace	28

Crypto-World 3-4/2012

A.	Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 11., Šifra „Palacký“ (J.Kollár)	2 - 12
B.	Má zmysel používať autokľúč? (J.Kollár)	12 - 17
C.	Slabý generátor náhodných čísel umožňuje faktorizovať RSA moduly (O.Mikle, predmluva P.Vondruška)	18 – 21
D.	Call for Papers - Mikulášská kryptobesídka 2012	22
E.	Problematika infrastruktury veřejných klíčů (PKI), dvoudenní kurz Akademie CZ.NIC (P.Vondruška)	23
F.	O čem jsme psali v březnu 2000 – 2011	24 – 25
G.	Závěrečné informace	26

Crypto-World 5-6/2012

A.	HERMANN POKORNY - "zaslužilý umelec" v lúštitel'skom odbore vo víre I. svetovej vojny (J.Krajčovič)	2 - 8
B.	Najstaršia zašifrovaná písomná pamiatka v Čechách (J.Krajčovič)	9 – 10
C.	Nízkoriziková kryptografie (V.Klíma)	11 - 13
D.	Společná novela zákona o elektronickém podpisu (účinná od 1.7.2012) (P.Vondruška)	14 – 18
E.	Call for Papers - Mikulášská kryptobesídka 2012	19
F.	O čem jsme psali v květnu a v červnu 2000 – 2011	20 – 24
G.	Závěrečné informace	25

Crypto-World 7-8/2012

A.	Andreas Figl – Nestor rakúskej školy kryptológie	2 – 13
B.	Kryptologické perličky 1 (K.Šklíba)	14 – 24
C.	Z NISTu unikl interní dokument k SHA-3 (V.Klíma)	25 - 30
D.	Knihy Kryptologie, šifrování a tajná písma rozebrána (P.Vondruška)	31
E.	Problematika infrastruktury veřejných klíčů (PKI), kurz Akademie CZ.NIC (P.Vondruška)	32 – 23
F.	ZPRÁVA - Nechcete být odposloucháváni? (L.Stejskalová)	34
G.	O čem jsme psali v létě 2000 – 2011	35 – 37
H.	Závěrečné informace	38

Příloha: dokument, který měl být odeslán pouze do interní skupiny NISTu pro výběr SHA-3 (více informací viz článek V.Klímy)

Crypto-World 9-10/2012

A.	Pointerová šifra a nízkoriziková náhrada AES (V.Klíma)	2 – 8
B.	Kryptografické zabezpečení prodeje lihovin (R.Palovský)	9 – 13
C.	Kryptologické perličky 2 (K.Šklíba)	14 – 20
D.	Záhada kodexu Rohonczy Codex (E. Antal)	21 – 28
E.	Kaspersky Lab uvádí Kaspersky Internet Security 2013	29 - 31
F.	O čem jsme psali v září a říjnu 1999 – 2011	32 – 35
G.	Závěrečné informace	36

Příloha: neoglyfy.pdf , ukázka ze sešitu Batěk A. S.: Neoglyfy I., str. 4 – str. 13 (<http://crypto-world.info/casop14/neoglyfy.pdf>)

Crypto-World 11-12/2012

A.	SHA-3 a lehká kryptografie (V.Klíma)	2 – 11
B.	Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni , část I. (J.Mírka)	12 – 28
C.	Tip na vánoční dárek - Enigma - bitva o kód (P.Vondruška)	29 – 30
D.	Pracovní příležitost (World Startup Project)	31
E.	O čem jsme psali v listopadu a prosinci 1999 – 2011	32 – 35
F.	Závěrečné informace	36

Příloha: Obrazová příloha k článku B (Mírka, J.) <http://crypto-world.info/casop14/cast1.zip>

2013

Crypto-World 1-2/2013

- | | | |
|----|---|---------|
| A. | Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni, část II. (J.Mírka) | 2 - 12 |
| B. | Lúštitelia historických šifier - A.V. Maloch a Josef Šusta (J. Krajčovič) | 13 - 21 |
| C. | Elektronický podpis v praxi (P.Vondruška, J.Peterka) | 22 |
| D. | SOOM.cz - Hacking & Security konference #2 (R.Kümmel) | 23 |
| E. | Security and Protection of Information 2013
(předběžná infomace) | 24 - 25 |
| F. | O čem jsme psali za posledních 12 měsíců | 26 - 27 |
| G. | Závěrečné informace | 28 |

Příloha: Obrazová příloha k části II. Mírka, J.: Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni

<http://crypto-world.info/casop15/obr2.zip>

Crypto-World 3-4/2013

- | | | |
|----|--|---------|
| A. | Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni, část III. (J.Mírka) | 2 - 14 |
| B. | Andreas Figl – rakúsky dôstojník a kryptológ (J.Kollár) | 15 - 23 |
| C. | Central European Conference on Cryptology 2013 | 24 |
| D. | call for papers - CYBERSPACE 2013 | 25 - 26 |
| E. | O čem jsme psali za posledních 12 měsíců | 27 - 28 |
| F. | Závěrečné informace | 29 |

Příloha: Obrazová příloha k části III. Mírka, J.: Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni

<http://crypto-world.info/casop15/obr3.zip>

Crypto-World 5-6/2013

- | | | |
|----|---|---------|
| A. | Konec aktualit v Crypto-News a Bezpečnostních střípků (J.Pinkava) | 2 |
| B. | Tajomstvo šifrovacieho stroja G. W. Leibniza (J.Krajčovič) | 3 – 11 |
| C. | Kaspersky Lab odhalila novou kyberšpionážní operaci NetTraveler | 12 |
| D. | Reakcia na článok „Andreas Figl – rakúsky dôstojník a kryptológ“
(J.Krajčovič) | 13 – 15 |
| E. | Cvičný CISSP test z kryptografie | 16 – 18 |
| F. | Central European Conference on Cryptology 2013 26.-28. června, Telč | 19 – 20 |
| G. | Call for Papers Mikulášská kryptobesídka | 21 |
| H. | O čem jsme psali za posledních 12 měsíců | 22 |
| I. | Závěrečné informace | 23 |

Crypto-World 7-8/2013

A.	Reino Häyhänen – sovietsky špión (J. Kollár)	2 – 9
B.	Dosud nevyluštěný dopis českého pobělohorského emigranta Karla Rabenhaupta ze Suché z doby třicetileté války. (Soutěž o ceny) (J. Mírka)	10 – 18
C.	Soutěž 2013, luštění originálního šifrového dopisu ze 17. století (P.Vondruška)	19 – 21
D.	Diskrétní logaritmus a metody jeho výpočtu (J. Pulec)	22 – 26
E.	Kaspersky v Praze - Kybernetické zbraně jsou nejhorším vynálezem století	27 – 28
F.	Pozvánka k podzimním kurzům Akademie CZ NIC	29 – 31
G.	O čem jsme psali za posledních 12 měsíců	32 – 33
H.	Závěrečné informace	34

Crypto-World 11-12/2013

A.	Ukládání hesel bezpečně (J.Vrána)	2 - 3
B.	Nomenklátory 17. a 18. století (J.Mírka, P.Vondruška)	4 - 6
C.	Letošní soutěž v luštění skončila – výsledky (P.Vondruška)	7 - 8
D.	Analýza Rabenhauptova zašifrovaného dopisu (E.Antal, P.Zajac)	9 – 17
E.	PF 2013 (P.Vondruška)	18
F.	O čem jsme psali za posledních 12 měsíců	19 – 20
G.	Závěrečné informace	21

Příloha k článku D: http://web.telecom.cz/depotpv/ASD12/priloha_k_D.zip

2014

Crypto-World 1-3/2014

B.	Československá šifra TTS a jej lúštenie (P. Javorka)	2 - 12
B.	Nový (souhrnný) pohled na otázky bezpečnosti eliptické kryptografie (J.Pinkava)	13 - 14
C.	Vyhláška o kybernetické bezpečnosti – výzva k připomínkám	15
D.	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.	Nariadení Evropského parlamentu a Rady o elektronickej identifikácii a dôveryhodných službách pro elektronickej transakcie na vnútornom 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