

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.	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 4/2001

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.	Sklyarov (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 Šůvy - 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.	Mikolášská 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