

2003

Crypto-World 1/2003

A.	Ceské technické normy a svet (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 svetem	18 - 20
E.	Závěrečné informace	21

Príloha : Crypto_p1.pdf
CEN Workshop Agreements (dokumenty vztahující se k elektronickému podpisu)

Crypto-World 2/2003

A.	Ceské technické normy a svet, 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 svetem - Kurs "kryptologie" na MFF UK Praha - Za použití šifrování do vedení - Hoax jdbgmgr.exe - Interview - AEC uvedla do provozu certifikační autoritu TrustPort - 6. ročník konference - Information Systems Implementation and Modelling ISIM'03 - O cem jsme psali v únoru 2000 - 2002	17-21
F.	Závěrečné informace	22

Príloha : Crypto_p2.pdf
Přehled dokumentu ETSI, které se zabývají elektronickým podpisem (ETSI - European Telecommunication Standards Institute)

10 stran

Crypto-World 3/2003

A.	Ceské technické normy a svet, III.část (Národní normalizační proces) (P.Vondruška)	2 - 6
B.	Přehled norem v oblasti bezpečnosti informacních 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 svetem	20-23
F.	Závěrečné informace	24

Príloha : 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.	Zacátek roku 2003 protokolu SSL nepreje.... (P.Vondruška)	8 - 9
D.	Eliptická kryptografie a kvantové počítače (J.Pinkava)	10 - 11
E.	Digitální certifikáty. IETF-PKIX část 11. Archivace elektronických dokumentu (J.Pinkava)	12-18
F.	Letem šifrovým svetem - Mobilní telefon s vestaveným utajovacem TopSec GSM - SIM karty lze klonovat za sedm minut - Danová priznání s elektronickým podpisem Pozvánky (vstup zdarma): - 16.4.2003 – Cesty k unitární teorii z pohledu astrofyziky (RNDr. Jirí Grygar, CSc.) - 17.4.2003 - seminár "Broadband Visions 2003" - 24.4.2003 - seminár "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 informacních systému - FIPS PUB 199 (P.Vondruška)	14 - 16
F.	Smernice OECD pro bezpečnost informacních systému a sítí: smerem ke kulture bezpečnosti (P.Vondruška)	17 - 18
G.	Letem šifrovým svetem	19 - 23
H.	Závěrečné informace	24

Crypto-World 6/2003

A.	Nebezpečí internetových řešení (M.Kuchar)	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 svetem	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 sdelení prostřednictvím Internetu, zejména pak jeho elektronické pošty, část I. (J.Matejka)	15-20
E.	TWIRL a délka klícu algoritmu RSA (J.Pinkava)	21
F.	Postranní kanály v Cryptobytes (J.Pinkava)	22
G.	Podarilo se dokázat, že P není rovno NP? (J.Pinkava)	23-24
H.	Letem šifrovým svetem (P.Vondruška)	25-28
I.	Závěrečné informace	29

Príloha: "zábavná steganografie" (steganografie.doc)

Crypto-World 9/2003

A.	Soutež 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 certifikátu, část 1. (J.Pinkava)	8 - 11
D.	K problematice šíření nevyžádaných a obtěžujících sdelení 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 svetem	25-26
H.	Závěrečné informace	27

Crypto-World 10/2003

A.	Soutež 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
C.	Jednoduchá a automatická aktualizace (D.Doležal)	20-21
D.	Recenze knihy "Řízení rizik" autoru V. Smejkal a K. Raise (A. Katolický)	22-24
E.	Letem šifrovým svetem	25-26
F.	Závěrečné informace	27

Crypto-World 11/2003

A.	Soutež 2003 - prubežná zpráva (P.Vondruška)	2
B.	Mikulášská kryptobesídka - Program	3
C.	Cesta kryptologie do nového tisíciletí IV. (Od NESSIE ke kvantovému počítání) (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 procesu a normy v EU (J.Hrubý)	17-27
G.	Letem šifrovým světlem (P.Vondruška)	27-29
I.	Vláda schválila novelu zákona o elektronickém podpisu	
II.	Přednášky z informační bezpečnosti IS na MFF UK	
III.	Nová RFC pro PKI	
IV.	Normální je fakturovat elektronicky	
V.	O čem jsme psali v listopadu 1999 - 2002	
H.	Závěrečné informace	30

Crypto-World 12/2003

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

Príloha: pf_2004.jpg