

2000

Crypto-World 1/2000

A.	Slovo úvodem (P.Vondruška)	2
B.	Zeme vstoupila do roku 19100 (P.Vondruška)	3 - 4
C.	Nový zákon o ochraně osobních údajů (P.Vondruška)	4 - 5
D.	Soukromí uživatelu GSM ohroženo (P.Vondruška)	6
E.	Letem šifrovým svetem	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 ? (Soucek, Hrubý, Beneš, Vondruška)	6-8
F.	Letem šifrovým svetem	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 - POZMĚNOVACÍ NÁVRHY K ZÁKONU O ELEKTRONICKÉM PODPISU BUDE PROJEDNÁVAT HOSPODÁRSKÝ VÝBOR PARLAMENTU	6
E.	Digital Signature Standard (DSS)	7-8
F.	Matematické principy informační bezpečnosti	9
G.	Letem šifrovým svetem	9-10
H.	Závěrečné informace	11

Crypto-World 4/2000

A.	Prohlášení odborné skupiny pro zpracování pozmenovacích návrhu k predložení zákona o elektronickém podpisu	2 - 3
B.	Fermatova čísla (P.Vondruška)	4 - 6
C.	Lekce pro tajné agenty - c.1 : "Neztrácejte své laptopy "	6
D.	Opet 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 svetem	11 - 12
H.	Závěrečné informace	13

Crypto-World 5/2000

A.	Statistický rozbor prvního známého megaprvočísla (P.Tesar, P.Vondruška)	2-3
B.	Mersennova prvočísla (P.Vondruška)	4-7
C.	Quantum Random Number Generator (J. Hruby)	8
D.	Sdružení pro bezpečnost informacních technologií a informacních systému (BITIS)	9
E.	Code Talkers (II.díl) , (P.Vondruška)	10-11
F.	Letem šifrovým svetem	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.	Fermatuv test primality, Carmichaelova čísla, bezctvercová čísla (P.Vondruška)	3 -5
C.	Cerv 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 svetem	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.	Fermatuv test primality, Carmichaelova čísla, bezctvercová čísla (P.Vondruška)	7-9
D.	Počátky kryptografie veřejných klíčů (J.Janecko)	10-14
E.	Prehled některých českých zdrojů - téma : kryptologie	15-16
F.	Letem šifrovým svetem	17-18
G.	Závěrečné informace	19

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

Crypto-World 9/2000

A.	Soutěž ! Část I. - Zaczínáme steganografií	2 - 5
B.	Prehled standardu 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 svetem	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.- Zaczínáme steganografií" , str.10) .

Crypto-World 10/2000

A.	Soutež ! Část II. - Jednoduchá záměna	2 - 4
B.	Král DES je mrtev - at 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

Príloha : ZoEP.htm

Dnešní užitečnou přílohou je plné znění zákona c.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.	Soutež ! 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.	Soutež (průběžný stav, informace o 1.ceně) (P.Vondruška)	2 - 3
B.	Substituce složitá - periodické heslo, srovnaná abeceda (P.Tesar)	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

Príloha : 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.	Soutež - 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