

## 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. Užahčí 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

### **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. | Hackeři pomozte !   |       |
| 4. | O čem jsme psali v červnu 2000 a 2001   |       |
| F. | Závěrečné informace   |       |

### **Crypto-World 78/2002**

- |    |   |       |
|----|---|-------|
| A. | Hackeři 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)