

## 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" svetem                                | 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 svetem                              | 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 kryptosystému ? (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 kun v počítačích                                                                                                         | 5   |
| D. | Matematické principy informací bezpečnosti (Dr. Soucek)                                                                                         | 6   |
| E. | Letem šifrovým svetem                                                                                                                           | 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 informací bezpečnosti (Dr. J. Soucek) | 3   |
| C. | Pod stromeček nové síťové karty (P.Vondruška)              | 3   |
| D. | Konec filatelie (J.Nemejc)                                 | 4   |
| E. | Y2K (Problém roku 2000) (P.Vondruška)                      | 5   |
| F. | Patálie se systémem Mickeysoft fritéza CE (CyberSpace.cz)  | 6   |
| G. | Letem šifrovým svetem                                      | 7-8 |
| H. | Řešení malované křížovky z minulého čísla                  | 9   |
| I. | Spojení                                                    | 9   |