CryptoBytes Index of Articles

Cryptobytes is in Adobe Acrobat (PDF) format. Be sure to download the Acrobat Reader for your web browser.

Volume 4, No. 2 - Winter 1998 (pdf, 332k) (Zipped PostScript - 1.12mb)

- Breaking DES
- First Advanced Encryption Standard (AES) Candidate Conference
- Attacking Elliptic Curve Cryptosystems Using the Parallel Pollard rho Method

Volume 4, No. 1 - Summer 1998 (pdf, 470k) (Zipped PostScript - 1.47mb)

- Performance Comparison of Public-Key Cryptosystems
- Smart Card Crypto-Coprocessors for Public-Key Cryptography
- Chaffing and Winnowing: Confidentiality without Encryption
- DES, Triple-DES and AES
- DES-II Challenges Solved

Volume 3, No. 2 - Autumn 1997 (pdf, 301k) (Zipped PostScript - 974k)

- On the Foundations of Modern Cryptography
- Efficient DES Key Search An Update
- The RSA Data Security DES Challenge II
- The Cryptographic Hash Function RIPEMD-160
- PKCS: The Next Generation, Chapter 2

Volume 3, No. 1 - Spring 1997 (pdf, 285k) (Zipped PostScript - 1.06mb)

- Proactive Security: Long-term Protection Against Break-ins
- Fast Generation of Random, Strong RSA Primes
- Algorithms Update, Standards Update, Announcements

Volume 2, No. 3 - Winter 1997 (pdf, 405k)

- How Exhausting is Exhaustive search?
- An Introduction to Threshold Cryptography
- The RC5 Encryption Algorithm: Two Years On

Volume 2, No. 2 - Summer 1996 (pdf, 357k)

- The Status of MD5 After a Recent Attack
- RSA-130 Factored
- The Security of DESX
- At the Newton Institute: Coding Theory, Cryptology, and Computer Security

Volume 2, No. 1 - Spring 1996 (pdf, 210k)

- Asymmetric Encryption: Evolution and Enhancements
- Payword and Micromint: Two Simple Micropayment Schemes
- Message Authentication Using Hash Functions: the HMAC Construction

Volume 1, No. 3 - Autumn 1995 (pdf, 320k)

- RSA for Paranoids
- The Secure Use of RSA
- How Do Digital Time-Stamps Support Digital Signatures

Volume 1, No. 2 - Summer 1995 (pdf, 390k)

- Elliptic Curve Cryptosystems
- The Future of Integer Factorization
- On the Security of the RC5 Encryption Algorithm

Volume 1, No. 1 - Spring 1995 (pdf, 365k) (HTML)

- The Impending Demise of RSA?
- Message Authentication with MD5
- The RC5 Encryption Algorithm

RSA Laboratories | CryptoBytes | Article Index | Subscribe

Contact RSA Laboratories at: rsa-labs@rsasecurity.com
Website feedback: webmaster@rsasecurity.com
Labs Home | Contact RSA Labs | Search | Site Map | Legal Disclaimer