Computing Reviews

Association for Computing Machinery

ThinkLoud

TODAY'S ISSUE | HOT TOPICS | SEARCH | BROWSE | RECOMMENDED | MY ACCOUNT | LOGOUT

REVIEW | ?

Search

Review

RC4 stream cipher and its variants

Paul G., Maitra S., CRC Press, Inc., Boca Raton, FL, 2011. 311 pp. Type: Book (978-1-439831-35-9)

Date Reviewed: Jun 7 2012

Full Text

Recommendations

Reviewer Selected

Featured Reviewer

Related Topics

Browse Alerts

Data Encryption (E.3) Add

Number-Theoretic Computations (F.2.1 ...) Add

Manage Alerts More Alerts

Cryptography is a hot topic these days due to its use in securing communications. Ciphers used in cryptography are generally classified as block ciphers and stream ciphers. Block ciphers operate on blocks of data, while stream ciphers operate on bits of plaintext. Stream ciphers generally operate much faster than block ciphers. To this day, no one stream cipher is a de facto standard. This book discusses the widely used RC4 stream cipher and its variants. It has been published under the "Discrete Mathematics and Its Applications" series, and is the first book that deals exclusively with RC4. It is meant for use as a reference text for graduate and advanced undergraduate students. Familiarity with combinatorics, data structures, algorithms, and probability and statistics is expected of the readers.

In the first of ten chapters, the authors introduce cryptology and acquaint the reader with some commonly used terminology. The introduction is very brief at just ten pages. Stream ciphers and RC4 are then presented. Attack models for cryptanalysis of stream ciphers are discussed, along with hardware and software stream ciphers. The key scheduling algorithm of RC4 is then analyzed, followed by an examination of biases of permutation toward secret key bytes. The authors show that the permutation bytes are not random, although the key-scheduling algorithm of RC4 does try to randomize permutations. The authors then touch upon key recovery from state information, and describe various algorithms for recovering the secret key of RC4 from state information. Key stream generation in RC4 is then analyzed. In practice, true random number generators are hard to use. The alternative is a pseudorandom number generator. A stream cipher can be regarded as a pseudorandom generator with the secret key as a seed. If by studying the cipher, one can show a bias in the probability of some key stream-based event happening, then we have what is known as a distinguishing attack on the cipher. The authors study distinguishing attacks and introduce a theoretical framework of distinguishing attacks.

Wired equivalent privacy (WEP) is a security protocol for IEEE 802.11 wireless networks. WEP has numerous flaws and has been deprecated in favor of newer standards such as Wi-Fi protected access 2 (WPA2) (which makes use of the block cipher advanced encryption standard (AES) for encryption). WEP incorporates RC4 for encrypting the network traffic. The authors look at different types of attacks on WEP and WPA. In practice, various types of faults may occur in cryptographic devices that may enable attackers to make use of the vulnerabilities of the cipher. The authors discuss some fault attacks on RC4. They then talk about some variants of RC4 and the stream cipher HC-128. There is a short concluding chapter that mentions the safe use of RC4.

The authors must be acknowledged for bringing out the first book on the RC4 stream cipher, which is widely used and worth studying. The allocation of the material in the book into ten homogeneous topics is appreciated. However, the book is very heavy on mathematical aspects and is very prosaic, which makes for difficult reading. The numerous lemmas, theorems, and proofs make the book very dull and tiresome, though mathematically concise. The saving grace is the research problems section at the end of each chapter. The inclusion of questions and exercises (mathematically oriented as well as programming-based) would have helped to overcome the monotony of the book. The authors should have touched upon the factors that enabled the success of RC4, and mentioned protocols and products that employ it. A list of acronyms would have helped minimize the effort required of the reader to find their meanings. The authors should have touched upon implementation issues in both software and hardware, and could have provided more programming assistance. The references are adequate and current. The brief, one-page concluding chapter of the book is very disappointing. It touches upon the safe use of RC4 in just a few words. The authors have done some considerable work on RC4, but I feel they could have produced a more readable book. Nonetheless, I recommend this book as a reference book for computer security professionals and researchers.

Reviewer: S. V. Nagaraj Review #: CR140247

SHARE

Would you recommend this review? ○ yes ○ no Enter

Other reviews under "**Data Encryption**":

	Date
Interoperable digital rights management based on the MPEG Extensible Middleware Rodr&#237;guez Doncel V., Delgado J., Chiariglione F., Preda M., Timmerer C. Multimedia Tools and Applications 53(1): 303-318, 2011. Type: Article	Feb 16 2012
Practical signcryption Dent A., Zheng Y., Springer-Verlag New York, Inc., New York, NY, 2010. 274 pp. Type: Book (978-3-540894-09-4)	Jul 22 2011
Encryption for digital content Kiayias A., Pehlivanoglu S., Springer-Verlag New York, Inc., New York, NY, 2010. 209 pp. Type: Book (978-1-441900-43-2)	May 25 2011

more...

E-Mail This Printer-Friendly

REVIEWER'S AREA | MASTHEAD | SUBSCRIBE | PRESS | TIPS | HELP | CONTACT US

Select Language ▼ Powered by Google Translate