

This article was downloaded by: [Institute of Messologi]

On: 29 April 2014, At: 01:07

Publisher: Taylor & Francis

Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Information Security Journal: A Global Perspective

Publication details, including instructions for authors and subscription information:

<http://www.tandfonline.com/loi/uiss20>

Stallings, W. Cryptography and Network Security: Principles and Practice

Nicolas Sklavos

Published online: 24 Apr 2014.

To cite this article: Nicolas Sklavos (2014): Stallings, W. Cryptography and Network Security: Principles and Practice, Information Security Journal: A Global Perspective, DOI: [10.1080/19393555.2014.900834](https://doi.org/10.1080/19393555.2014.900834)

To link to this article: <http://dx.doi.org/10.1080/19393555.2014.900834>

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at <http://www.tandfonline.com/page/terms-and-conditions>

Book Review

Stallings, W. *Cryptography and Network Security: Principles and Practice*, 6th ed. Upper Saddle River, NJ: Prentice Hall, 2013, 752p., \$142.40. ISBN: 13: 978-0133354690.

Cryptography and Network Security: Principles and Practice is the revised sixth edition by William Stallings. The prolific and exquisite writer presents an up-to-date book related to computer security and essentials of cryptology. The book is divided in seven major sections, and through the 20 chapters, Dr. Stallings succeeds in covering all the aspects of cryptography. From the very start of the book, before the numbering of the chapters begins, the author explains to readers the improvements that have been made in the sixth edition while referring to the noteworthy changes. The material of the book is organized into four basic topics: symmetric/asymmetric encryption and cryptographic hash functions, matters of authentication and mutual trust in communication, cryptographic algorithms in network security, and computer security concerning threats and malicious attacks. The reader is informed from the start about the most important standards of organizations developed in network security and cryptography. In chapter 1, the author makes an introduction to the meanings of computer security and gives definitions of significant objectives such as confidentiality, authentication, and accountability, as well as the security attacks and the mechanisms. In the first part of the book, starting from chapter 2 up to chapter 7, the author introduces the reader to the techniques of encryption in the classical and the advanced modus, the operation of block ciphers, and the basic concepts in number theory. In chapters 8–10, he explains the asymmetric ciphers, the RSA algorithm, and various public-key cryptosystems. In section 3, Dr. Stallings continues with algorithms related to data integrity in cryptography, describing the different signature schemes and the codes functioned in terms of message authentication. In section 4, the author talks about the matters of trust managing different keys and user authentication and verification. The last section is dedicated to the issues of network and Web security, either in electronic communication or in Web exchanges. At the end of the book, the author offers projects and case studies, laboratory exercises, and sage examples in specific chapters of the book. The sixth and the seventh chapters, documents, audiovisual material, supplemental papers, and homework problems with their solutions are provided online in the so-called Premium Content via a unique access code in the inner side of the front cover of the book. *Cryptography and Network Security: Principles and Practice* is a comprehensive, organized, and detailed book, with an important educational use. The book is addressed not only to simple learners or students but also to professionals and academics who need an analytical and complete book in subjects of cryptography and network security, both in content and in supporting material of PDF files, slides, problems, and solutions and projects. The pedagogical characteristic of the book is enhanced by the fact

that each chapter is enriched with learning objectives, figures, tables, recommended reading books and papers, key terms, review questions, and problems. This revised version of the book contains the topics of the courses recom-

mended by the Information Assurance Security, according to the ACM/ IEEE Computer Science Curricula 2013.

*Reviewed by Nicolas Sklavos
nslavos@ieee.org*