Review of the book

A Classical Introduction to Cryptography:

Applications for Communications Security

by Serge Vaudenay

Springer 2006

ISBN: 978-0-387-25464-1

Jothi Rangasamy
Queensland University of Technology

01-01-2010

1 Overview of the book:

The book is aimed at bridging the gap between cryptography and its standard applications. From my point of view, it has achieved its goal. This book presents basic tools of cryptography with applications in communication and information security. This book is a compilation of author's lecture notes that he used for teaching cryptography to undergraduate students.

Though this book is titled like any other introductory books on cryptography, this is actually an advanced level textbook covering prehistory of cryptography; symmetric key cryptography; public key cryptography; mathematical topics like algorithmic algebra and number theory for cryptologists and other cryptographic protocols. This book differs significantly from other introductory books, since it covers some topics that other books did not. For example, RSA exponent problem and its equivalence to factorization problem is covered in this book. Also some topics from cryptanalysis of both symmetric and asymmetric primitives are well presented, though it is a book on cryptography.

The most important point is that every concept is discussed intuitively with rigorous mathematics. A reader can find how beautiful is cryptography when it joins hand with mathematics. But at the same time too much mathematics will be too boring for some readers and they may find this book difficult to read. This book will answer two questions once it is read. First question is how important is cryptography in todays world and the second question is how fun is cryptography with mathematics. All complexity theory and mathematical preliminaries needed are covered in separate chapters of the book. This means a reader with no mathematical background could directly start reading this book. But a better insight into several discussion points requires additional reading.

2 Book Summary

This book has 12 chapters, totally. But they can be grouped accordingly as five major parts:

Part 1 This part covers the prehistory of cryptography. It begins with the details of some important historical ciphers such as substitution ciphers, transposition ciphers and the Vernam cipher amongst others. Then assumptions of modern cryptography and adversarial models are discussed as roots of modern cryptography. Finally, the Shannon theory of secrecy is presented in detail.

Part 2 This part is all about symmetric key cryptography, also known as conventional cryptography. This part consists of four chapters from two to five. In these chapters, almost all state of the art and important block ciphers like DES and its successor AES are discussed in detail

with their applications. From stream ciphers, GSM mobile encryption (A5/1) and bluetooth encryption (E0) are discussed. In addition, some brute force attacks like dictionary attack and time-memory tradeoff attacks on symmetric key primitives are also considered. Moreover, one full chapter is dedicated to cryptographic primitives such as hash functions and cryptographic pseudorandom generators. Rest of the chapters in this part give good reference to cryptanalysis of conventional cryptosystems.

Part 3 All the background materials needed to understand crtyptography are provided in this part. So anyone can directly start reading this book without any pre-requisite knowledge. To avoid too much of mathematics here, algorithmic algebra, algorithmic number theory and the elements of complexity are the only materials covered in this part. Chapters from six to eight come under this part.

Part 4 This part is dedicated to public key cryptography where i am most impressed with. The reason is that many topics covered here are relatively new and can not be seen on other books. I saw the equivalence of RSA multiple exponent problem and factoring of integers only on this book. The author himself tried to include many new algorithms and topics as the well-known ones can be seen anywhere. This section gives the state of the art knowledge on public-key algorithms, especially the RSA problems. The way each topic is linked is quite impressive. This section also provides security proofs for important encryption schemes, identification schemes and DSA-like signature schemes. Digital signatures, an important application of public-key cryptography are detailed in a separate chapter. Chapters nine and ten come under this part.

Part 5 This part presents cryptographic protocols and their applications in communication security. Cryptographic protocols such as secret sharing, zero-knowledge proofs and special purpose signature schemes are included. Some important standards like SSH2 and security in bluetooth are also discussed. This part consists of the last two chapters 11 and 12.

3 Comments and Recommendations

This book, A Classical Introduction to Cryptography: Applications for Communications Security presents fundamentals of cryptography with more mathematical flavor. It covers a lot of basic material on cryptography and hence it is very helpful for students and teachers. Also each chapter ends with some significant number of exercises which are very intuitive. Moreover the book is presented by following a chronological order. This makes it easy for a reader to follow the development of new security definitions and schemes.

Most of the sections are rich in theory and hence, from my point of view, this is more suitable for research than for industry purposes. For graduate level students in computer science and engineering, this is good source to learn mathematical cryptography. At the same time, the book will help students in mathematics to know how important is mathematics for cryptography. This would encourage and welcome them to take cryptography as their research area in future. For researchers, this could be a very handy reference book. More references and materials are given under the section called Further Readings.

I would strongly recommend this book for any research student in cryptography irrespective of their background. The goal of the book is teaching cryptography, I think that this goal is achieved.

The reviewer is a Ph.D. student at Queensland University of Technology, Brisbane, Australia.

2004. A classical introduction to cryptography: Applications for communications security. S Vaudenay. Springer Science & Business Media, 2006. 194. 2006. Decorrelation: a theory for block cipher security. S Vaudenay. Journal of Cryptology 16 (4), 249-286, 2003. 182. 2003. Mutual authentication in RFID: security and privacy. RI Paise, S Vaudenay. Proceedings of the 2008 ACM symposium on Information, computer and â€¦, 2008. 178. 2008. Provable security for block ciphers by decorrelation. S Vaudenay. Annual Symposium on Theoretical Aspects of Computer Science, 249-275, 1998.