Review of the book

Complexity and Cryptography: An Introduction

by John Talbot and Dominic Welsh
Cambridge University Press, 2006
ISBN: 978-0-521-61771-0

Sashank Dara
Cisco Systems Pvt ltd

Summary of the review

Complexity and Cryptography An Introduction provides a neat and easily readable introduction to cryptography from a complexity theoretical perspective. This book as the title says, is an introductory book and is clearly not for advanced researchers of the subject. It is suggested for prospective students of two types who want to learn/understand:

- The applications of complexity theory in cryptography,
- The basics of cryptography with complexity theory perspective.

Summary of the book

1. Chapter 1: Basics of Cryptography gives a good introduction to cryptographic models like classic cryptography, public key cryptography and modern cryptography for beginners, which serves as a good appetiser for the rest of the book.
2. Chapter 2: Gives a brief introduction to Complexity Theory. Deterministic Turing machines are explained neatly with examples. Although time complexity is introduced, different ways of measuring time complexity, i.e. the best, worst and average cases, are missing.
3. Chapter 3: This chapter on Non deterministic computation has an introduction to Non deterministic polynomial time. Subsequent sections focus on NP-Completeness, NP-Hardness, and Containment between NP Classes are also made clear.
4. Chapter 4: Probabilistic computation has a good introduction. Then, Probabilistic algorithms for primality testing are covered in detail. Although the recent break through deterministic polynomial time AKS algorithm is mentioned, an informal explanation of the algorithm as an appendix at the end would have helped the reader to learn about it quickly.
5. Chapter 5: Symmetric Key Crypto systems are introduced and the basic idea of perfect secrecy is clearly explained with examples. Two types of approaches exist when discussing security of Crypto systems. One is unconditional security (or perfect secrecy) and the one based on computational security (sometimes called provably secure). The latter approach only provides a proof of security relative to some other problem, not an absolute proof of security.
6. Chapter 6: The basic idea of one way functions, trap doors and their relevance in public key cryptography is explained.

7. Chapter 7: A few important public key Crypto systems are clearly explained along with few problems with trapdoor systems. One of the most important aspect of writing any book is to mention caveats in current systems for beginners to get interest in the subject. This book succeeds in that.
8. Chapter 8: Digital Signatures is another important aspect of cryptography equally important in building security systems. This chapter neatly explains the concept of digital signatures and a few important attacks are also covered. The proof for proposition 8.2 which says the RSA signature scheme is an existentially forge-able under a direct attack is not correct: to form a signature under RSA based signature scheme, one should use their private key, not public key, as stated in section 8.2, but where as the proof says Fred forms a valid signature using public key of Alice which is wrong. RSA based signature scheme is not existentially forge-able unless if Fred some how gets Alice's private key. Correction is required for this proposition.
9. Chapter 9: Most of the books on cryptography mention Diffie-Hellman key exchange but often do not mention Shamir's seminal work, a cult paper written on secret sharing, "*How to share a secret*?", this book explains clearly and briefly about the work done by Shamir in that paper which needs special pat.
10. Chapter 10: Pseudo Random Generators are important building blocks for many Crypto systems, this chapter explains their details in an easy readable way.
11. Chapter 11: Identification schemes based on interactive proofs and zero knowledge schemes are explained. The example 11.7 *The gold prospector* given to elucidate zero knowledge proof's is not intuitive and convincing for first time reader.

What is the book like (style) ?

This book is styled in a way that students get a bird's eye view of the fascinating and interesting world of cryptographic concepts from a complexity theory perspective. Each chapter gives the basic definitions, theorems and algorithms required for learning certain concepts. It is thoroughly complimented and backed up with further notes, exercises and appendices for further reference and learning.

In general students often want to see links between theory and practice, but often textbooks are written in a theoretical way ignoring the corresponding practical real world systems built around them. This book mentions RSA which is used extensively in real world, however, examples of systems build upon them could be mentioned. In similar lines the key distribution chapter can mention small paragraph on Kerberos for students to know real world implications and further study it.

Although the authors mention in the preface the reasons for not including quantum cryptography, it is a very important topic, especially when dealing with the subject of this book: cryptography from a complexity theory perspective. As quantum computing techniques become mature and quantum computers become reality, cryptographic primitives based on algorithms that have no polynomial time solutions would become obsolete.

Would you recommend this book?

This book can act as supplement but not a textbook on its own for Cryptography, as the authors mention in the preface. The reasons are that they have purposefully omitted a few (important) topics like cryptanalysis, quantum cryptography, Elgamal Crypto system etc.

I can recommend this book for: a) beginners who want to study cryptography and applications of complexity theory; b) researchers who want to get a complexity theoretic perspective of cryptography. This book might help advanced researchers to refresh their knowledge, but not beyond that. Professors, Teachers and Teaching assistants can make use of the huge number of exercises in this book for conducting exams, tests and quizzes.

Sashank Dara is currently a Senior Engineer working on Secure Technologies at Cisco Systems Private limited.