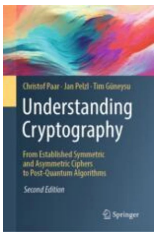
Review of [1]

Understanding Cryptography

From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms

Second Edition



Christof Paar, **Jan Pelzl**, and **Tim Güneysu**

Springer, 2024
543 pages, $79.99 Hardcover, $64.99 Ebook

Review by
Shiva Houshmand
Department of Mathematics and Computer Science
Santa Clara University

1 Overview

Today, almost every part of modern life relies on digital systems, which makes cybersecurity more important than ever. Technologies such as social networking platforms, medical devices, and emerging systems like autonomous vehicles all depend on strong security mechanisms to function safely. Cryptography is a foundational pillar of modern computer security and a primary tool for building secure systems. This book offers clear explanations of the cryptographic mechanisms most commonly used in real-world systems, with a strong emphasis on practical relevance.

Designing, implementing, and using cryptographic mechanisms correctly is subtle and critical, and even small misunderstandings can lead to serious security failures. Aimed at both students and practitioners, the book helps readers develop a solid conceptual understanding of cryptographic schemes, protocols, and implementation issues, including how they withstand known attacks and how to choose appropriate key lengths. Mathematical foundations are introduced when needed, without going deeply into formal proofs or provable-security frameworks. Overall, the book gives readers a clear picture of how cryptographic systems are built, why they are considered secure, and under what assumptions that security might no longer hold.

2 Summary of Contents

The organization of the book follows a structure that is typical of introductory cryptography texts, beginning with an overview of the field of cryptography.

Chapter 1 introduces symmetric encryption using historical ciphers to motivate fundamental concepts such as message secrecy and key space. It also briefly discusses basic cryptanalysis techniques and introduces modular arithmetic, which provides the mathematical background needed for later chapters.

Chapter 2 is about stream ciphers (a family of symmetric encryption). Since randomness plays a major role in stream ciphers, the chapter presents pseudorandom number generators and explains

how keystreams are derived from cryptographically secure pseudorandom number generators. It concludes with a discussion of modern stream ciphers currently in practical use.

The next three chapters focus on block ciphers (another family of symmetric encryption scheme). **Chapter 3** covers DES, one of the earliest modern encryption algorithms, which is now considered obsolete. The chapter explains DES's internal structure, including Feistel networks and S-boxes, and introduces core block cipher design principles such as diffusion and confusion. These concepts remain central to the design of modern block ciphers.

Chapter 4 is dedicated to AES, the most widely used block cipher today. It walks through the design process behind AES and explains its internal structure in detail.

Chapter 5 then explores how block ciphers can be used as building blocks for other cryptographic mechanisms, including stream ciphers, pseudorandom number generators, hash functions, and message authentication codes, discussed in the context of their modes of operation.

Chapter 6 introduces asymmetric-key cryptography (aka public-key cryptography) along with the number theory concepts that are essential for understanding public-key algorithms.

Chapter 7 focuses on RSA, one of the earliest public-key encryption schemes that remains widely used in practice. The chapter explains the core RSA algorithm and then discusses its practical weaknesses, emphasizing the need for proper padding schemes in real-world implementations.

Chapter 8 continues the discussion of public-key cryptography by presenting algorithms based on the discrete logarithm problem, including Diffie–Hellman and ElGamal.

Chapter 9 introduces elliptic curve cryptography, a third family of public-key algorithms that has become increasingly popular in practice due to its performance advantages and shorter key lengths.

Chapter 10 introduces digital signatures, a fundamental tool based on public-key cryptography that provides integrity and authentication. The chapter covers RSA- and ElGamal-based signature schemes, along with its widely used extensions, including the Digital Signature Algorithm (DSA) and the Elliptic Curve Digital Signature Algorithm (ECDSA).

Chapter 11 focuses on hash functions, a core cryptographic primitive used across a wide range of protocols and systems. Hash functions produce a short, fixed-length, and unique representation of a message and play a central role in applications such as digital signatures, message authentication codes, cryptocurrencies, password security, and post-quantum cryptographic constructions.

Chapter 12 introduces post-quantum cryptography by explaining the threat that quantum computers pose to widely deployed public-key schemes. It presents the basic ideas behind post-quantum approaches—such as lattice-based, hash-based, and code-based cryptography—at a high level. This chapter reinforces a central theme of the book: cryptographic security depends on underlying assumptions, and those assumptions must be revisited as technology evolves.

Chapter 13 focuses on message authentication codes (MACs), which provide message integrity and authentication using symmetric-key techniques. While they serve a purpose similar to digital signatures, MACs are widely used in practice due to their efficiency and role in many security protocols.

The final chapter, **Chapter 14**, addresses practical deployment and key management issues, covering the mechanisms used to securely generate, store, and distribute the secret keys that are essential to most of the cryptographic algorithms discussed in the book.

3 Opinion

This book would work very well as a textbook for undergraduate and graduate courses in applied cryptography, and it is also a good fit for practitioners with a solid technical background. It assumes some familiarity with programming and basic mathematics, but it does not expect the reader to have prior experience with cryptography. One thing I particularly appreciate is that the book intentionally avoids heavy mathematical formalism. This is a thoughtful choice that keeps the focus on practical understanding and correct application of cryptographic techniques without getting lost in formal proofs.

A major strength of the book is how each chapter is structured. Each chapter explains the core ideas behind each cryptographic algorithm, while also discussing known attacks, relevant NIST recommendations, and practical implementation issues in software and hardware when appropriate. Having all of this information brought together in a single chapter is especially valuable for readers who want to understand how these schemes are actually used in practice.

Each chapter also points readers to additional resources for those who want to dive deeper into the mathematical details or specific attacks, and the chapter concludes with a concise summary of the key takeaways. Another aspect I found valuable is the explicit discussion of cryptography in the presence of quantum computing. The authors explain how known quantum algorithms affect existing cryptographic schemes and why this forces us to rethink long-standing security assumptions. In this edition, the new chapter on post-quantum cryptography gives readers a clear picture of which types of algorithms are expected to remain secure and which are not once powerful quantum computers become available, along with an overview of the main post-quantum approaches.

Naturally, some chapters, especially Chapter 9 on elliptic curve cryptography and Chapter 12 on post-quantum cryptography, are more mathematically demanding than earlier ones. Even so, the presentation remains approachable, with an emphasis on intuition and high-level structure.