Review of the book

"Understanding Cryptography"

by Christof Paar and Jan Pelzl

Springer, 2010

ISBN: 978-3-642-04100-6

Luigi Lo Iacono

1 What the book is about

Yet another introductory book on cryptography!? This is what most people from the community might think, when they first glimpse at the present book by Christof Paar and Jan Pelzl. And that is what the book entitled Understanding Cryptography really is about. It is a textbook mainly targeted to undergraduate students as a very first course in cryptography. Still, when having a closer second look at the book, the unique and distinguishing character appears.

The book is organized into thirteen chapters as follows: It kicks-off in chapter 1 by characterizing the field of cryptology. The fundamental counterparts of cryptography as the science of secret writing and cryptanalysis as the science of breaking cryptography are introduced. Cryptography is further divided into its major areas including symmetric and asymmetric cryptographic primitives as well as protocols. The same is done for Cryptanalysis. It is subdivided into its fields social engineering, implementation attacks and the classical cryptanalysis which is further splitted-up into brute-force attacks and mathematical analysis. All of these mentioned domains and concepts are illustrated and explained by making use of historical ciphers.
Chapter 2 is devoted to stream ciphers. Before diving into this topic, the two basic types of symmetric ciphers—block ciphers and stream ciphers—are introduced and the main differences between these approaches are explained. Hereafter, the essential ingredient required in each and every stream cipher is described: the XOR operation. Based on this foundation, the next consequent step is to discuss about key streams and their randomness. The book continues on this path and explains the distinct techniques to generate random numbers ranging from true random number generators to pseudo-random number generators. After a short stop at the only known cryptosystem which provides unconditional security, the One-Time-Pad, the rest of chapter 2 focusses on more practical stream ciphers by introducing the generation of key streams based on linear feedback shift register and by using one particular algorithm as an example: Trivium.
Block ciphers are focussed in the following two chapters, starting with the data encryption standard (DES) in chapter 3. By making use of the most popular block cipher, the authors explain basic design ideas of block ciphers, which are still fundamental building blocks of all modern ciphers, such as confusion and diffusion. Then the DES specifics are explained in high detail. Since DES has been the first standardized block cipher it was widely deployed. For this reason, DES also received a lot of attention from the cryptanalytic side. Analytic attacks including differential and linear cryptanalysis have been evolved from this and are the subject of the following sections. This chapter closes by mentioning some DES alternatives including triple DES, the lightweight cipher PRESENT and very briefly the DES successor AES which takes the centre stage in the following chapter 4.
Before going into the details of the advanced encryption standard (AES), chapter 4 describes the remarkable procedure of selecting the AES and lists the five finalists from which the Rijndael algorithm at the end was nominated the AES. To understand the AES and its internal structure, the required mathematical prerequisites in terms of basic facts on Galois fields are laid. This chapter closes by commenting on the efficiency of software and hardware implementations.

Chapter 5 goes on with block cipher related aspects. Different modes of operations for block ciphers are presented in detail along with considerations on their usage in order to prevent common security pitfalls. The discussed modes focus on the classical ones, namely ECB, CBC, OFB and CFB as well as more recent alternatives, here CTR and GCM. Other targeted aspects in this chapter include mechanisms to increase the security of block ciphers. The meet-in-the-middle attack is pointed out and used to explain, why a two-times usage of a cipher is not enough to increase the resistance against exhaustive key search attacks. That is why a double DES does not exist but a triple DES does. Finally, key whitening techniques are introduced.
Chapter 6 leaves the symmetric cryptographic primitives and introduces the concept and foundations of public key cryptography. The basic principles of public key cryptography are illustrated by using the analogy of a safe. The demand for public key cryptography is motivated by the key distribution problem and missing security services such as non-repudiation. The remainder of this chapter is then dedicated to the mathematical background required to understand the asymmetric cryptosystems discussed in the following chapters.
After all this ground building, the most popular and widely used asymmetric crypto algorithm takes the centre stage of chapter 7. Named after its inventors Rivest, Shamir and Adleman, the RSA scheme is based on the problem of factorizing large integer numbers. Chapter 7 shows how RSA works also by giving examples based on artificially small as well as practical RSA parameters. Further aspects discussed in this chapter include the computation of parameters, the fast exponentiation using the square-and-multiply algorithm, other speed-up techniques, schemes to find large primes, padding to avoid certain weaknesses and other known attacks.
Chapter 8 continues with asymmetric algorithms which are based on the discrete logarithm problem (DLP). The Diffie-Hellman key exchange (DHKE) is explained first. By this rather simple protocol, the grass roots in terms of group-based algebra are introduced, which are essential for understanding DLP-based algorithms. Building on that, this chapter closes by describing The ElGamal encryption algorithm which has practical relevance and is an extension of the DHKE protocol.
The newest member in the family of established public-key cryptosystems are elliptic curves. Based on the generalized DLP, elliptic curve cryptosystems are addressed in their own chapter. As in the previous chapters, also chapter 9 introduces the basic mathematical background required to understand elliptic curve cryptography first. Backed by the knowledge on what an elliptic curve is and how a group and group operations such as point addition and point doubling can be constructed on such curves, the reader learns how the DLP can be build with elliptic curves. On this ground, the DHKE is constructed with elliptic curves.
Chapter 10 addresses a cryptographic tool, which is grown from asymmetric cryptography: digital signatures. The principles behind digital signatures are covered first and it is explained, why symmetric cryptography is not sufficient to provide security services such as non-repudiation. Four schemes to compute digital signatures are discussed in more detail: RSA, ElGamal, digital signature algorithm (DSA) and elliptic curve DSA (ECDSA).
An important prerequisite for calculating digital signatures are hash functions. Chapter 11 takes on this topic by first motivating that hash functions are required in digital signature schemes when it comes to signing long messages. Then it discusses security requirements of hash functions and describes the birthday attack. This chapter closes by giving an overview of hash functions. This includes common construction principles based on block ciphers and constructions specifically dedicated for hash functions. SHA-1 has been selected for a more in depth analysis, since it is the most widely used hash function and the SHA-2 family shows a similar internal structure.
Chapter 12 gives an overview of message authentication codes (MAC). The principles and properties of MACs are introduced and the two main approaches to build MAC schemes are addressed. First, the construction based on hash functions is derived from the secret prefix MAC and the secret suffix MAC (both having security weaknesses) to the HMAC. Second, block cipher based MACs are pointed out with the most popular construction relying on the CBC mode of operation.
The last chapter deals with cryptographic protocols and more specifically with key establishment. The main flow starts with introducing key establishment using symmetric cryptosystems and includes the Kerberos protocol as a practical example. By discussing the limitations of the symmetric schemes, key establishment using asymmetric cryptosystems is discussed subsequently. Issues in regard to the authenticity of public keys are derived and used to finally explain concepts such as certificates, public key infrastructure (PKI), certificate authority (CA), certificate chains, certificate revocation list (CRL), etc.

2 What is the book like

Mainly targeting undergraduate students, the book gives a good understandable introduction to cryptography. Most importantly, this book does not make any assumptions on prior knowledge in neither mathematics nor computer science. It is therefore not only suited for undergraduate students in mathematics or in the computer science field, but rather also for students from other domains requiring crypto skills such as legal people for example.
Its strength is really its ability to explain the complex content in an easy understandable but yet accurate manner. It does so by giving a lot of examples—often based on artificially small numbers—and by including a multitude of exercises at the end of each chapter. By this, the book can be used for self-studies or practical hands-on training as well as reference for a course or lecture respectively. In fact, the authors themselves have developed the book for and used it in their own lectures and courses.
Another very useful measure is that each chapter includes a sort of guidance for the reader. Each chapter starts with a bullet list of items which will be taught and ends with a section listing the lessons learnd as well as a section containing a discussion on further readings for readers interested in going deeper into the particular topic.
Last but not least, the authors provide a rich book-companioning service. Additional ressources can be downloaded from the book's Web site `www.crypto-textbook.com` such as slides (in PDF format), links to related sites and test vectors. Moreover, the slides can be requested in PowerPoint format from the authors as well as a hardcopy version of the solutions manual for the exercises which will be delivered via postal mail free of charge. In both cases, it is sufficient to request these materials by simply contacting the authors via email.

The book is written in a clear and fluent way. The general style is concise and to the point. The structure is well-organized and although the chapters build on each other, the authors managed to write them in a way that also allows to read them selectively.

It is really hard to find negativ points or disadvantages of the present book. When being forced to name some, the following remarks could be made. Every now and then the book gets a tendency towards hardware-oriented cryptography. This is not serious and is surely an influence coming from the authors' field of expertise. From a content viewpoint, two aspects are missing or have only been targeted marginally. Padding schemes which are required for some modes of operations and which go beyond the simple ones-or-zeros padding such as ciphertext-stealing and ANSI X.923 are missing as well as elliptic curve based encryption.

3 Recommendation

I would certainly recommend this book for the audience it is targeting. It provides a good starting point, regardless of whether being in the computer science field or for any other discipline in which cryptography knowledge is required. Since cryptography is a complex matter, it is very important to practice a lot in order to gain understanding. With the numerous examples and exercises included in the book the authors respect exactly this requirement and support the reader with a large amount of material for hands-on training. Henceforth, this book is not only a valuable source for undergraduate students but also for lecturers who can benefit from this book as a reference for their courses.

Overall, I really hope to see an equivalent book in the future, which targets more advanced topics in the field of cryptography in the same way this book does for the introductory subjects.

The reviewer is a lecturer at the European University of Applied Sciences.