Contents

Introduction

Cryptography is an important but difficult topic. A great many professions require some level of use of cryptography. This includes programmers, network administrators, and cybersecurity professionals. However, such people often are not provided adequate training in cryptography. There are a number of excellent cryptography books available, but most assume some level of mathematical sophistication on the part of the reader. This renders them inaccessible to a substantial number of potential readers.

The entire purpose of this book is to bridge this gap. If you are a mathematician or cryptographer, this book is not intended for you. In fact, you might feel frustrated that certain mathematical details are not fully explored. As one glaring example, there are no mathematical proofs in this book. This book is aimed at the person who wants or needs a better understanding of cryptography, but may not have a background in number theory, linear algebra, and other similar topics. When needed, just enough math is provided for you to follow along, and no more detail than is necessary. As a consequence, this book is meant to be accessible to a broad audience. However, that also means that should you master every topic in this book, you would not be a cryptographer. You will, however, be an intelligent consumer of cryptography. You will know the questions to ask vendors, and be able to understand and evaluate their responses.

There are a great many practical questions this book will prepare you to analyze. Should you use elliptic curve or RSA? If you wish to use RSA, what is the appropriate key size? What makes a good cryptographic hashing algorithm? Why is an HMAC better than a hash? Why should you always use CBC mode with symmetric ciphers? What impact will quantum computing have on the current cryptography? These are just a few of the questions you will gain answers to in this book.

Furthermore, this book should provide you a solid foundation should you later wish to delve into more mathematically rigorous cryptography books. Having

studied this book, you will be able to venture into deeper waters. There are some excellent books from Springer that go deeper into the mathematics. *Understanding Cryptography* by Paar and Pelsl is one such book. For readers who really want to dive into the math, *An Introduction to Mathematical Cryptography* by Hoffstein, Pipher, and Silverman is an excellent choice.