PART II
PUBLIC KEY CRYPTOGRAPHY

If all you need is to encrypt your disk, you don't need anything more than secret key cryptography. Unlike secret key cryptography, public key cryptography provides a feasible way to distribute encryption keys publicly while keeping decryption keys secret.

The chapters in Part II explain public/private key cryptography—often referred to simply as "public key"—the most important advance in cryptography in several thousand years. Although public key solves the secret key delivery problem for our global digital marketplace, it creates others that must be considered, such as how Bob can be certain he is using Alice's authentic public key, a problem we discuss in Part III, "Distribution of Public Keys."

From the beginning of human history to about 20 years ago, secret key cryptography satisfied all our needs for secure communications. That's because most people didn't need cryptographic communications, and those who did need it spent money and time to distribute and maintain secret keys. As illustrated in Chapter 8, setting up and maintaining a system of thousands of secret keys is all but impossible. Key distribution centers (KDCs) worked well with secret keys because, with few exceptions, KDCs were never required to maintain thousands of keys.

Chapter 9 introduces the concepts behind public key systems with an early innovation by Ralph Merkle, one of the pioneers of public key cryptography. In the 1970s, Merkle demonstrated a clever method to exchange secret keys over a public line without a KDC. Merkle's ideas capture the benefits that a public key system provides its users and the problems it forces on potential adversaries.

Chapter 10 explains how encrypting with a public key ensures confidentiality.

Chapter 11 shows a simple example of a math trick used in public key cryptography that is the basis for confidentiality. If you'd rather eat liver than do math,[1] rest assured that understanding the rest of the book is not contingent on understanding the math tricks in this chapter.

1. We wish we'd come up with this analogy, but the full quote is from Bill Neugent: "The protection provided by encryption is based on the fact that most people would rather eat liver than do mathematics."

Chapter 12 explains how encrypting with a private key provides assurances other than confidentiality: authentication, integrity, and nonrepudiation. Nonrepudiation, which ensures that Alice and Bob cannot deny sending any messages they transmit, is an added benefit of public key that secret key can't provide.

Chapters 13 shows how message digests speed the encryption process and provide even more security.

Chapter 14 describes technicalities that cryptographers have built into message digests to defeat attacks. These details are not essential to understanding how public key cryptography operates, so if you're interested only in the big picture, you can safely skip this chapter.

Chapter 15 compares secret key, public key, and message digests to help you better understand why all three cryptographic tools are used in the real-world systems discussed in Part IV.