PART I

SECRET KEY CRYPTOGRAPHY

In 1977, two innovations in computer cryptography forever changed 3,500 years of message disguise engineering and brought cryptography closer to being a tool everyone would need and use. Part I, “Secret Key,” explains the concepts used to develop one of these innovations—Data Encryption Standard (DES)—and leads into the second innovation, public key cryptography, discussed in Part II.

Part I describes the current state of secret key computer cryptography. The first five chapters explain two important concepts:

- Secret key cryptography offers secure ways to store secrets.
- The attacker’s most feasible attack against these secure methods is to try each possible key.

To prove these two concepts, Chapters 1 through 5 quickly proceed from ancient to modern cryptographic methods. If you’re familiar with these two concepts, you may choose to skip to Chapter 6. That said, we believe the first five chapters offer a quick and instructive overview that will help you understand secret key cryptographic protective devices.

Chapter 6 shows how cryptography evolved into a mathematical science.

Chapter 7 describes protections and assurances available with secret key cryptography.

Chapter 8 explains why secret key cryptography, by itself, is not sufficient to protect communications on the Internet. The bulk of the book and appendixes explain public key cryptography and demonstrate why the Internet needs it.