Chapter 10
Basic Cryptography

YORK: Then, York, be still awhile, till time do serve:
Watch thou and wake when others be asleep,
To pry into the secrets of the state;
— *The Second Part of King Henry the Sixth*, I, i, 249–260.

Cryptography is a deep mathematical subject. Because this book focuses on system security, we consider cryptography as a supporting tool. Viewed in this context, the reader needs only a brief overview of the major points of cryptography relevant to that use. This chapter provides such an overview.

Cryptographic protocols provide a cornerstone for secure communication. These protocols are built on ideas presented in this chapter and are discussed at length in later chapters.

10.1 Cryptography

The word *cryptography* comes from two Greek words meaning "secret writing" and is the art and science of concealing meaning. *Cryptanalysis* is the breaking of codes. The basic component of cryptography is a *cryptosystem*.

Definition 10–1. A *cryptosystem* is a 5-tuple $(\mathcal{E}, \mathcal{D}, \mathcal{M}, \mathcal{K}, \mathcal{C})$, where $\mathcal{M}$ is the set of *plaintexts*, $\mathcal{K}$ the set of *keys*, $\mathcal{C}$ is the set of *ciphertexts*, $\mathcal{E} : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{C}$ is the set of *enciphering functions*, and $\mathcal{D} : \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{M}$ is the set of *deciphering functions*.

EXAMPLE: In the latter days of the Roman Republic, Julius Caesar was preparing to invade Italy. His confidential communications with his secret allies in Rome were enciphered using a cipher in which the letters are shifted by 3 (so this type of cipher is called a *shift cipher* or a *Caesar cipher*). For example, the letter "A" becomes "D," "B" becomes "E," and so forth, ending with "Z" becoming "C."

So the word "HELLO" is enciphered as "KHOOR." Informally, this cipher is a cryptosystem with

$$\begin{aligned}\mathcal{M} &= \{\text{all sequences of Roman letters}\}\\ \mathcal{K} &= \{i \mid i \text{ an integer such that } 0 \leq i \leq 25\}\\ \mathcal{E} &= \{E_k \mid k \in \mathcal{K} \text{ and } \forall(m = m_1 \ldots m_n \in \mathcal{M})[E_k(m_i) = (m_i + k) \bmod 26]\}\end{aligned}$$

Representing each letter by its position in the alphabet (with "A" in position 0), "HELLO" is 7 4 11 11 14; if $k = 3$, the ciphertext is 10 7 14 14 17, or "KHOOR."

$$\mathcal{D} = \{D_k \mid k \in \mathcal{K} \text{ and } \forall(c = c_1 \ldots c_n \in \mathcal{C})[D_k(c_i) = (26 + c_l - k) \bmod 26]\}$$

Each D_k simply inverts the corresponding E_k. We also have

$$\mathcal{C} = \mathcal{M}$$

because $\mathcal{E}$ is clearly a set of onto functions.

The primary goal of cryptography is to keep enciphered information secret, thereby countering the threat of disclosure (see Section 1.2). Cryptography can also be used to provide integrity of both data and origin, thereby countering the threats of modification and masquerading. It can also provide nonrepudiation, countering the threat of repudiation of origin. Thus, it is a remarkably powerful mechanism that computer security techniques rely on heavily.

Cryptosystems are based on two types of transformations [1725]. The first, *onfusion*, replaces parts of the plaintext message with other data, to hide the original content. The second, *diffusion*, scrambles the plaintext message so that the original content is spread throughout the message. These increase the difficulty of uncovering the original plaintext message.

10.1.1 Overview of Cryptanalysis

Cryptanalysis is the analysis of cryptosystems in order to decipher the messages. *Kerckhoff's Principle* says that the security of a cryptosystem cannot rely on an adversary's not knowing the algorithms for encryption and decryption [1826]. Thus, standard cryptographic practice is to assume that she knows the algorithms used to encipher and decipher, and the set of possible keys, but not the specific cryptographic key (in other words, she knows $\mathcal{K}$, $\mathcal{D}$, and $\mathcal{E}$).

An adversary may use three types of attacks:

- In a *ciphertext only* attack, the adversary has only the ciphertext. Her goal is to find the corresponding plaintext. If possible, she may try to find the key, too.