Chapter 1

Locks and Keys

We begin our explanation of cryptographic concepts with the help of two people you'll get to know well in this book: Alice and Bob, a fictitious pair often used for illustration in cryptography books. Alice and Bob's first task is to illustrate the difference between *method* and *key*.

Locks and Combinations

One lock design used to make many locks

Imagine that a master locksmith has designed a combination lock and published the entire inner workings—the nuts and bolts of every mechanism in the lock. Alice buys a lock and changes the combination. The design is so secure that no one, not even the locksmith, can figure out the new combination. Of course, this means that if Alice forgets the combination, no one can open the lock without trying every combination or breaking the lock.

Further imagine that this one lock design is used to make many locks. Suppose Bob also buys a lock and changes the combination. Just like the locksmith who designed the lock, Alice has no clue how to figure out the combination on Bob's or anyone else's lock. So Alice can't open Bob's lock, and Bob can't open Alice's lock (see Figure 1-1).

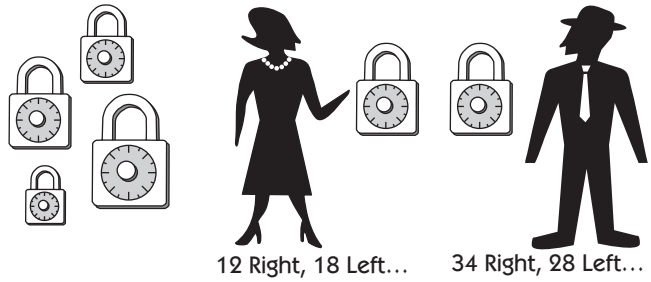
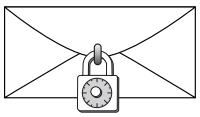


Figure 1-1 Alice's and Bob's individual locks are only two of many instances of the identical lock design.

Alice checks that her lock is secure against the force she believes an opponent might use to open it and checks that the lock can't be opened by merely pulling on the handle. She also wants to have confidence that it would take an intruder a long time to try all the possible combinations. How long Alice wants someone to have to try different combinations determines the kind of lock she buys. If Alice's only concern is to protect her luggage against a nosy baggage attendant, she needs a lock to stop someone for only a few minutes. She might buy a lock with only a few possible combinations. On the other hand, if Bob wants to protect his valuables at an athletic club, he needs a lock with more possible combinations (see Figure 1-2).



Let's use the lock and key analogy to see how Alice could protect her electronic possessions. Imagine that Alice has an envelope containing a secret message and that her lock seals the envelope to keep others from opening it. The message inside the envelope is readable if the correct combination opens the lock. The message is unreadable if the lock is opened any other way, such as breaking it with a hammer or a crowbar.

Cryptography is both the lock and the combination (or key). Just as there are a variety of locks, there are a variety of cryptographic methods and keys (see Figure 1-3). The joining of the method and the key determines how secure Alice's secret message is from an opponent who doesn't know the combination.

Strength of lock and number of possible combinations (keys)

Bob can use a lock with the same design as Alice's lock; many people know that the method is to turn right to number 1, left to number 2, and finally right again to number 3. But it's Bob's individual lock combination (his personal numbers 1, 2, and 3) that enables his lock to secure his personal belongings and keeps Alice, or anyone else without the lock combination, out. What matters most in securing Bob's personal belongings is the strength of the lock and the number of possible combinations or keys.

In the same way, the lock strength and the number of possible keys are critical to securing Bob's and Alice's electronic communications. Alice and Bob can use a cryptographic method or lock with the same design (as long as it's a strong method) and still securely hide their personal messages from a savvy opponent,

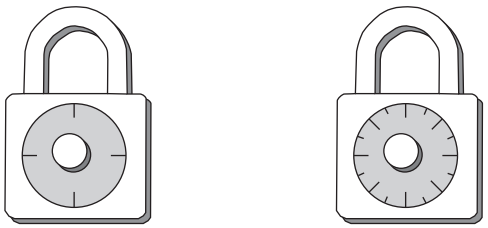


Figure 1-2 Some locks have very few possible combinations; others have many possible combinations.

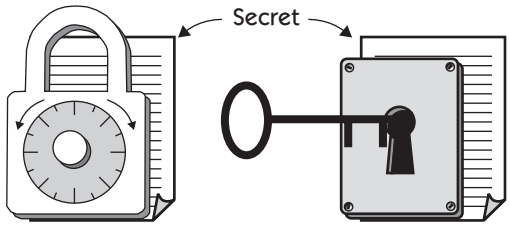


Figure 1-3 Cryptography is both a lock and a key.

or each other, *because their individual cryptographic keys are different*. As long as there are enough possible keys to keep an opponent busy trying them for a long time, Bob and Alice can feel somewhat secure that the secrets in their messages won't fall into the wrong hands.

Why is the number of possible secret keys one of the most important factors about a secret key cryptographic method? It's obvious that a physical lock with 10,000 possible combinations is much more secure than a lock with only 10 possible combinations. In cryptography, this has not always been true. In the following chapters, you'll learn why.

Defining Cryptographic Terms

Definitions: cryptography, cryptographer, cryptanalyst, cryptology

Cryptography is both the lock and the combination (key) that protects a secret message from anyone who doesn't know the key. *Cryptographers* are the people who create a disguise to hide the meaning. A key that will reclaim the meaning is given only to those for whom the message is intended.

Cryptanalysts are mathematical and linguistic analysts who remove the disguise created by cryptographers. Because they haven't been given a key, they attempt to pick the lock to meaning using statistical analysis. *Cryptology* is the study of both cryptography and cryptanalysis.

Hiding Writing

Cryptography is like building a crypt, where people have traditionally buried valuables for safekeeping on the way to the afterlife. It comes from the Greek word *kryptos,* meaning "hidden" or "covered," the Old Norse *hreysar,* meaning "heap of stones," and the Lithuanian *krauti,* meaning "to pile up." It's a way to hide writing ("-graphy") but retain a way to find it again, like piling stones on a gravesite to which you want to return.

Making and Solving Puzzles

For as long as people have been communicating, the Bobs and Alices of the world have looked for secure ways to share and hide meaning. When people began using written language to reveal meaning, fields such as cryptography and cryptanalysis were created by the clever mathematical and linguistic minds among us. These people like to make and solve puzzles and often spend lifetimes doing it. Some make a living at it, whereas others only dabble; many contribute to the field. Over time, many good ideas and systems have been created but not fully understood, recognized, or used until much later.

To stay one step ahead of cryptanalysts, cryptographers have invented various ingenious ways to hide meaning. Although computers have made many older methods obsolete, technology has put cryptographic minds to work in new ways.

If you want to lay a good foundation for looking at computerized disguising techniques, the first step is to understand how complexity affects a cryptographic system. So before we clarify how today's computer methods work, let's take a brief look at the history of the cryptographic craft, starting with simple methods and leading up to the more complex. In the next two chapters we'll discuss the two major components of ancient and modern secret key cryptography: substitution and transposition.

The Father of American Cryptography

Thomas Jefferson earned the title "Father of American Cryptography" for a device he called a wheel cipher. It remained undiscovered for nearly a century until two others—a Frenchman and an American—independently created the same device. Although the wheel cipher was a good method for its time, Jefferson put it aside and apparently forgot about it. In 1922, the year the device was discovered in the Library of Congress among Jefferson's papers, the U.S. Army adopted an almost identical cipher mechanism others had developed.

Review

If you're connected to or transmit data over an electronic network, your data is vulnerable to attack by anyone else who is connected to that network.

Cryptography is both the lock and the combination (or key) that can be used to help protect your data. There are a variety of cryptographic methods and keys. Together, the method and the key determine cryptographic security.