

CHAPTER 1

Introduction

According to legend, Julius Caesar sent encrypted communications to Cicero because he did not trust the messengers delivering his messages. His scheme, which is extremely simple, is based on elementary mathematics. More than 2,050 years later, computer scientists at the Massachusetts Institute for Technology (MIT) developed an encryption method in which the enciphering details are made public and yet the message remains secure! This scheme uses the same mathematics as Caesar's scheme, albeit in a more sophisticated way.

A cipher is a scheme for obscuring a message in order to exchange information securely. The purpose of using a cipher is to keep a message concealed from all except the intended receiver. Privacy is something we value, even when the content of a message is not particularly significant. That is why we use envelopes, instead of postcards, for all but the most trivial of our written communications. In this current "information age," we send many different types of messages, including e-mail, bank transactions, and on-line shopping. Banks, stores, and libraries all hold a tremendous amount of information about us. The need for privacy is greater than ever.

The use of ciphers is probably as old as writing itself. One of the earliest recorded instances occurs in the book of Jeremiah in the Hebrew Bible. Throughout history, a variety of ingenious techniques have been used to obscure or hide messages. These include writing with invisible ink, employing coding machines, and hiding the real message inside a larger one. As an example of the latter technique, consider the message:

- (1) A TRICKY TIGER ALWAYS COMES KNOWINGLY.
 A THREATENED DEER ALWAYS WALKS NEARBY.

Can you find the real message? If you write down the first letter of each word in (1), you will find the hidden message:

ATTACK AT DAWN.

This scheme is, of course, not particularly secure.

Dedicated coding machines provide more security than the scheme illustrated in (1). They have the additional advantage of enabling the sender and receiver to code and decode messages quickly. Thomas Jefferson invented one of the oldest known coding machines; it is on display at Monticello in Virginia. In World War II, the Germans used the ENIGMA machine. A turning point in the war occurred when the allies built their own copy of

this machine; from that point on, they were able to read German communications created by ENIGMA.

Computers have significantly changed the way in which coded messages are created. With the increase of computer speed, it is now possible to implement encryption schemes that were impractical just a few years ago. On the other hand, faster computers also mean that intercepted messages can be more quickly analyzed by unintended receivers. So schemes that might have been secure before can now be broken easily.

The widespread use of technology has increased the necessity for encryption. Until recently, the need for secret codes was limited to government and perhaps some businesses. Computers and the Internet have changed that forever. Today, many people have their paychecks deposited directly into their checking accounts. To do this, the employer's and the employees' bank account numbers must be transmitted electronically. Likewise, ordering merchandise on-line requires sending a credit card number out into cyberspace. And, we all expect that our e-mail messages are private.

We will begin our study of encryption with the system used by Julius Caesar. Building on that simple system, we will then consider more complicated schemes. All of these different ciphers will build toward the cipher developed by the MIT computer scientists, which is called the RSA Cipher. It is one of the ciphers that is used to provide security for the Internet.

This introductory chapter covers some basic terminology. The original message is known as the *plaintext*, while the coded message is called the *ciphertext*. The process of converting from plaintext to ciphertext is known as *enciphering* or *encryption*; restoring the plaintext from the ciphertext is *deciphering* or *decryption*. The many schemes used for enciphering constitute the area of study known as *cryptography*. Such a scheme is known as a *cryptographic system* or a *cipher*. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of *cryptanalysis*. Cryptanalysis is what the layperson calls "breaking the code." The areas of cryptography and cryptanalysis together are called *cryptology*.

When devising an enciphering scheme, it is important that there be a corresponding deciphering scheme. It is useless to encipher a message if it is impossible to recover the plaintext. Thus, for each system that we develop, we will describe both the enciphering and deciphering processes. We will also use each system as an opportunity to discuss different aspects of cryptanalysis. For the first few cryptographic schemes, we will consider the following question. If we did not know the enciphering details, how might we go about discovering the plaintext message?

Here is a ciphertext that we will analyze in a later chapter:

ZK YRJ FECP SVVE ZE KYV CRJK WVN UVTRUVJ KYRK
TIPGKFXIRGYVIJ YRMV LJVU DRKY KF UVJZXE TZGYVIJ

Can you decipher it?