## **Chapter 1**

## Clueing You In about Codes and Cryptograms

#### In This Chapter

- Discovering cryptography through the ages
- Finding out about Masonic codes and ciphers
- Investigating additional resources

n this book, we offer you the challenge of breaking several types of real ciphers and cryptograms, all devised by noted Australian puzzlemaster Denise Sutherland (author of *Word Searches For Dummies* [Wiley]).

In this chapter, we offer a few things to orient you to the secrets of codes and cryptograms, including the world of the cryptogram, the history of ciphers and codes, and the ways in which the time-honored fraternity of the Freemasons has used codes over the centuries. We also tell you about the contemporary world of codes and follow up by giving you some suggestions for further reading.

## Introducing the Cryptographic World

The word *cryptographic* comes from elements that mean "hidden" *(crypto)* and "writing" *(graph)*. The cryptographic world encompasses codes and ciphers (which we distinguish between in Chapter 2), which are used to create *cryptograms* (secret messages).

#### $m{10}$ Part I: Code and Cryptogram Strategies \_\_\_\_\_

Ciphers. Codes. Cryptograms. What do you think about when you hear these words?

You may get an image of dark nights with fog-filled streets. In an attic in wartime London, a nervous man, constantly checking the door with anxious looks over his shoulder, is bent over a static-filled radio, writing down strings of numbers as they come over one particular frequency on the dial. In the street below, people in trench coats trade identical briefcases on street corners after an exchange of passwords. Such is the popular image — and, to some extent, the truth — of espionage, a world where ciphers, codes, and cryptograms are part of everyday reality.

Perhaps you prefer a more ancient or historical slant. Maybe you're thinking of Julius Caesar sending messages to his troops in the hostile wilds of Western Europe, in the years before he ruled the Roman Empire. Perhaps you wonder about the secrets encoded on parchment in the Middle Ages and during the Renaissance by people who had quite a lot to lose — like their lives: political plotters, alchemists, and even — gasp! — practitioners of magic and sorcery. And then there are the secret societies of history, some political (the Black Hand of Serbia, the Holy Vehm, the Bavarian Illuminati), some criminal (the Black Hand of Sicily, La Cosa Nostra), some religious (the Rosicrucians), some fraternal (the Freemasons and their affiliated organizations, the York and Scottish Rites).

Then again, you may prefer a more modern and military approach. Military and diplomatic ciphers can make or break a nation in wartime. Just in the relatively short period of American history, ciphers and codes have played prominent roles in the American Revolutionary War and the War Between the States, and afterward. In the world at large, codes and ciphers — which ones were broken and which ones endured — had much to do with determining the outcomes of World Wars I and II, thus affecting the lives of billions of people. Your life may have been very different if the brave geniuses of Britain's Bletchley Park group hadn't broken the German Enigma ciphers.

Of course, today cryptography has gone corporate. You probably send or receive multiple encrypted messages every business day without even knowing it, as you transfer funds from an ATM to your pocket, as you order merchandise over the Internet, even as you communicate through telephone or e-mail. Keeping these communications secure is big business — and big trouble when it fails.

# Considering the History of Codes and Ciphers

The origins of codes and ciphers — like the beginnings of language and writing, and my entire Beatles LP collection — are lost in the sands of time. David Kahn, the master historian of codes and ciphers, wrote that the development of secret writing was inevitable in any literate human culture because of "the multiple human needs and desires that demand privacy among two or more people."

Then again, legends tell of another source of secret writing. In Jewish tradition, the most ancient book was written by God and delivered to Adam in the Garden of Eden by the angel Raziel (a name that means "secrets of God"). The first published edition of the *Book of Raziel the Angel* appeared in Amsterdam in 1701. One part of that book illustrates divine alphabets that could be used to encode secrets — divine or otherwise.

Parts of the Jewish Talmud (second century AD) reflect the belief that secret messages were encoded within the text of the Bible. These messages could be decoded according to specific rules, such as *gematria* (the use of the numerical equivalents of the Hebrew letters, where the first letter has the numerical value "1," and so on). The use of *gematria* and other methods to detect secret messages in the Bible appears today in the study of *Kabbalah*, one approach to Jewish mysticism. (If you're interested in discovering more about this topic, check out *Kabbalah For Dummies* by Arthur Kurzweil [Wiley].)

Whether you accept a human or a divine origin of codes and ciphers — or both! — the following sections offer you some tantalizing references to what *could* be codes and ciphers in ancient literature of a very early date.

## Early ciphers

Homer's *lliad* — thought to date between the sixth and eighth centuries BC — has exactly one reference to writing. It comes up in the story-within-a-story of Bellerophon, who was sent off by an angry monarch with folded and sealed "tablets on which he [the monarch] had traced a number of devices with a deadly meaning," tablets that Bellerophon was to give to another king, who was supposed to kill Bellerophon after reading the message. To this day, a message that instructs the recipient to kill the messenger is called a "bellerophontic" message. Is Homer's wording a fancy way to talk about normal writing — or does it indicate the use of a code or cipher? We don't know.

The earliest use of a cipher for military purposes involved the fifth century BC Spartans of Greece. They used the device called the *scytale*, a baton. A strip of paper or leather was wrapped around the baton, and the message was written straight across the different "columns" of the paper or leather. The recipient of the message would wrap the leather or paper around a baton of the same dimensions and then read the message off the material wound about the baton.

The second century BC Greek historian Polybius devised a ciphering system that has been used for centuries. Polybius put the letters of the alphabet in a 5 x 5 array like a short checkerboard. In Polybius's system, each letter is described in terms of the column and row in which it appears. Thus, "A" is ciphered as "1-1," "B" as "1-2," all the way to "Z" as "5-5." (In this scheme, "I" and "J" are given the same code.)

Julius Caesar, the first century BC Roman statesman, used at least two ciphering systems during the years when he was a general of the Roman armies. These systems are the Caesar Shift and the Caesar Box Codes (we describe both in Chapter 2, and you can try your hand at them in Chapters 7 and 11). After the fall of the Roman Empire in the West (about 476 AD), we know little of the making of codes and ciphers in the West for many centuries.

However, in other parts of the world, cryptography thrived. The rise of Islamic civilization, from the seventh century AD onward, saw the first books written on *cryptanalysis*, that is, the organized effort to *break* codes and ciphers. In Eastern Asia, the use of *idiograms* (picture writing) in such languages as Chinese made it impractical to use *ciphers* (substitutes for letters). However, real codes were sometimes used. For example, in 11th century AD China, one military code was based on the 30 words of a particular poem. Each word corresponded to a brief message, like "need more bows and arrows." A single word of the poem would be sent as the message from one commander to his superior.

The rebirth of learning during the Renaissance, which continued in the Enlightenment, saw a great increase in the use of codes and ciphers in the Western world. The emergence of the central text of Kabbalah, the Zohar, in about 1300, led many Christian scholars to look into the use of gematria to detect secret meanings in sacred writ. The publication of Agrippa's Three Books of Occult Philosophy in 1531 did a great deal to spread the use of special alphabets to conceal secret religious writings because Agrippa was the first to publish together in tabular form the magical alphabets called "Celestial," "Malachim" (Hebrew for "angels"), and the enigmatically named "Passing the River." These magical alphabets were republished centuries later in Francis Barrett's popular work, The Magus (1801), through which these alphabets became a permanent part of the landscape of esoteric and magical studies. (You can try some of these magical alphabets in Chapters 6 and 8.)

But it is the worlds of politics and military actions that have seen an explosion of activity in the area of secret writing over the last 600 years. The destinies of nations have hung on the making and breaking of codes. For example, the attempt by Mary Queen of Scots to take the British throne from Elizabeth I of England in 1585 collapsed when the cipher used by her conspirators, led by Anthony Babington, was broken by Elizabeth's agents.

As cryptography made and unmade nations in Europe, it did the same in the New World. For example, in the American Revolutionary War, a wide variety of cryptographic techniques (including ciphers, code books, and invisible inks) was used on both sides. The same is true of the use of cryptography during the American War Between the States, or Civil War.

## Cryptography and the Great Wars

During the wars of the 20th century, cryptography came to determine the destiny, not just of nations, but of the globe.

We offer you three examples, one from the First World War and two from the Second. Both wars began in Europe, with the entry of the United States following sometime afterward.

#### The Zimmerman telegram

By early 1917, the First World War had been raging on the continent of Europe for two and a half years, but the U.S. was officially neutral. The question on everyone's mind was whether the U.S. would enter the war, and if so, when. On January 16, 1917, the German Foreign Secretary (equivalent to the American Secretary of State), Arthur Zimmerman, sent a ciphered telegram to the German ambassador to Mexico. The British intelligence services intercepted the telegram, which consisted of hundreds of groups of digits, each group up to 5 digits long ("13042 13401 8501 115" and so forth). The British had captured some German code books that described an earlier version of the cipher and so were able to decode the message.

The Zimmerman telegram described a plot in which the Germans would begin "unrestricted submarine warfare" on February 1. If America entered the war, Germany proposed to help Mexico reconquer territories in Texas, New Mexico, and Arizona from the U.S.! A way was found to leak this telegram to the U.S. government without revealing that the British had broken the German cipher. The telegram's message was printed in American newspapers on March 1, 1917, and the U.S. entered the war just over a month later. The entry of the U.S. decisively tipped the balance of power in the war away from Germany. The deciphering of the Zimmerman telegram thus changed the course of history.

#### The Enigma code

In the Second World War, German U-boats were destroying a large fraction of the Allied shipping in the Atlantic Ocean. The Germans used a coding machine, code-named the Enigma, which used a collection of cipher wheels and switches to apply a different cipher to *every single letter of a message*. The British applied an immense amount of effort to breaking this code, which they finally did. The breaking of the Enigma code turned the tide of the war in the Atlantic and made the D-Day invasion that much more possible.

### The future of cryptography

Beginning in the 1960s, cryptographers used higher mathematics to make more and more complicated ciphers. These ciphers involve the use of enormously long prime numbers to create ciphers of such complexity that they can only be broken, if at all, with immensely powerful computers. We don't use those ciphers in this book. However, if you're interested in cryptography, you should know that this is where a large part of the future of cryptography is headed. If you're still in school and interested in cryptography, work hard at those math courses!

#### The Navajo code talkers

In the Pacific theatre of the Second World War, the American armed forces used Native American speakers of the Navajo language. The Navajo code talkers used words from the natural world to represent military objects: different types of birds were different types of aircraft, different types of fish were different types of ships, and so on. The Navajo code talkers were used to communicate among different American military units, with great success. After the war, it was revealed that the Japanese had broken several American codes but had made no progress with breaking Navajo. Much of the American success in the Pacific theatre can be attributed to the contribution of the Navajo code talkers.

## Uncovering Masonic Codes and Ciphers

Not everyone who uses codes and ciphers is involved in military or political activity. Groups with a spiritual orientation have long used ciphers and codes to conceal their teachings. This isn't so much for fear of their being discovered (although sometimes this has been a concern, when persecution is an issue). Rather, the issue is to keep certain types of spiritual knowledge or teachings from those who aren't ready or aren't qualified to receive them. The Freemasons (or Masons), a fraternal organization that has been public about its existence since 1717, has long used codes of different sorts. The primary purpose of using codes has been to keep the Masonic ceremonies of initiation secure. These ceremonies are complex and must be performed from memory. Masons put hours of study into the effort to learn their ceremonies. In some areas, Masons possess small books with the text of these ceremonies. To keep the ceremonies confidential even if the books fall into the wrong hands, the books are written in an *initial-letter cipher*, that is, a code in which each word of the text is represented by its initial letter. This code allows someone who already knows the ceremony to use the cipher to practice the ceremony until the person memorizes it to perfection.

In earlier generations, Freemasons sometimes used symbols instead of letters to encipher their ceremonies. Coauthor Mark has in his possession a couple of book lover's treasures, small old ritual books with ceremonies enciphered by symbol, a sort of American hieroglyphic extravaganza. If you come upon any of these books in an old bookstore or yard sale, treasure them — they become rarer every year.

Masons have also made great use of the *Pigpen Cipher*, so called because, to people of an earlier age, its tic-tac-toeboard structure resembled the layout of pigpens. The Pigpen Cipher has many versions and has come to be known as the Freemasons' Cipher. The version in this book isn't "the" correct one because a single correct version doesn't exist. Masons in different areas learned different versions. However, the version we present in Chapter 8 shows the exotic, mysterious character of the cipher, where letters are represented by a few angular symbols and dots.

On the continent of Europe, where Freemasonry developed in ways that were a bit different from English Masonry, there was more of an interest in exotic ciphers. You can find some of those ciphers in Chapter 8, as well. They're elaborate symbolic inventions dating from the 18th and 19th centuries. In that era, all ciphers had to be written out by hand, so it didn't matter that the ciphers used unique symbols that can't easily be represented in computer-readable form.



Enjoy these ciphers as a glimpse into a different age, when the creation of cryptograms was a bit more leisurely than it is today.

## Continuing Your Crypto Education

In this section, we include some reading suggestions for those of you who are hooked on codes, cryptograms, and conspiracies!

Consider these additional resources if you seek to solve more puzzles:

- ✓ Word Searches For Dummies by Denise Sutherland (Wiley): This book, by one of the authors of the book you hold in your hands, shows you how to approach word search puzzles of different types and levels of difficulty. The book includes 250 puzzles to solve, with hints and answers.
- ✓ The Mammoth Book of Secret Codes and Cryptograms by Elonka Dunin (Running Press): This book includes a huge collection of codes and ciphers, as well as real-life unsolved codes and undeciphered scripts.

If you want to gain additional knowledge about codes, ciphers, and cryptography, give these books a try:

- Codebreaker: The History of Codes and Ciphers by Stephen Pinnock (Walker & Company): This brief and lavishly illustrated book may be the best place to go next if you want to dive further into the subject, especially from a historical point of view.
- ✓ The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography by Simon Singh (Doubleday): As the subtitle indicates, the focus in this book is on the last four centuries or so. You can find extensive examples of different ciphers in this fascinating book.
- ✓ The Codebreakers: The Story of Secret Writing by David Kahn (Macmillan): This is the big daddy of all books on cryptography, a highly readable yet comprehensive description of the entire history of the field. It gives a great deal of emphasis to the period of World War II and the Cold War, but it also includes much about codemaking and codebreaking during earlier periods of history.

Kahn on Codes: Secrets of the New Cryptology by David Kahn (Macmillan): For the true crypto fan, this is a collection of essays, largely focused on the World War II period and thereafter.

If you want more information about codes in the Kabbalah, we suggest *Kabbalah* by Gershom Scholem (Meridian/Penguin). For cryptographers, the chapter on *gematria* is particularly interesting!

If you want information on cryptography and its use in the American Revolutionary War and the Civil War, turn to these texts:

- ✓ George Washington, Spymaster: How the Americans Outspied the British and Won the Revolutionary War by Thomas B. Allen (National Geographic): This book for young adults has a great deal about true codes and other secret writing techniques used during the Revolutionary War. For example, the book reproduces the nine-page codebook created by Major Benjamin Tallmadge, who was General Washington's spy chief — and who appears as a character in our first conspiracy story (see Chapter 3).
- ✓ Washington's Spies: The Story of America's First Spy Ring by Alexander Rose (Bantam): This groundbreaking history of the subject has a lot to say about ciphers and codes.
- Secret Missions of the Civil War: First-Hand Accounts by Men and Women Who Risked Their Lives in Underground Activities for the North and the South by Philip Van Doren Stern (Bonanza Books): The final chapter of this book includes info on codes and ciphers in the Civil War.

And if you're looking for information about Freemasonry and its ciphers, consider the following:

✓ Freemasons For Dummies by Christopher Hodapp (Wiley): This book is an excellent introduction to the general subject of Freemasonry. It tells you how Freemasonry operates, what the Masonic "degrees" or rituals of initiation are like, and how to tell the difference between truth and fantasy in the many stories you can read about Freemasonry in literature and on the Internet.

- ✓ Freemasonry: An Introduction, by Mark Koltko-Rivera (LVX Publishing): This book, by one of the authors of the book you hold in your hands, describes the ideals and values of Freemasonry, its relationship to ancient systems of initiation, and why men choose to become Freemasons in the first place.
- ✓ Scottish Rite Ritual Monitor and Guide, 2nd Edition, by Arturo de Hoyos (Washington, DC: The Supreme Council of the Scottish Rite, 33°, Southern Jurisdiction): If you're a real fan of Masonic ciphers, this book gives you traditional Scottish Rite alphabets and ciphers, including the *Cypher of the Rose Croix* devised by Albert Pike, and several other cryptographic treats. (This is the source of the 19th century Masonic Ciphers we use in this book.) For more info, check out www.scottishrite.org.
- Committed to the Flames: The History and Rituals of a Secret Masonic Rite by Arturo de Hoyos and S. Brent Morris (Lewis Masonic): This book describes the effort that successfully deciphered a custom Masonic Cipher that resisted all efforts to break it for over a century. The result revealed a secret set of ceremonies that were used by a small Masonic group in New York.

## 20 Part I: Code and Cryptogram Strategies \_\_\_\_\_