CONTENTS

SPIES—CODES AND CIPHERS

The practice of sending secret messages is known as "steganography," Greek for "concealed writing." The problem with hiding a message in the lining of a coat or tattooed on the scalp is that anyone can read it. It makes a lot of sense to practice "cryptography," as well, Greek for "hidden writing." Cryptography is the art of writing or breaking codes and ciphers.

The words "code" and "cipher" are sometimes used as if they mean the same thing. They do not. A code is a substitution, such as the following sentence: "The Big Cheese lands at Happy tomorrow." We do not know who the Big Cheese is, or where Happy is. Codes were commonly used between spies in World War II, when groups of numbers could only be translated with the correct codebook. Codes are impossible to break without a key or detailed knowledge of the people involved. If you spied on a group for some months, however, noticing that the president of France landed at Heathrow airport the day after such a message, a pattern might begin to emerge.

Ciphers, on the other hand, are scrambled messages, not a secret language. In a cipher, a plain-text message is concealed by replacing the letters according to a pattern. Even Morse code is, in fact, a cipher. Ciphers are fascinating and even dangerous. More than one person has gone to his grave without giving up the secret of a particular

cipher. Treasures have been lost, along with lives spent searching for them. In time of war, thousands of lives can depend on ciphers being kept—or *deciphered*.

Edgar Allan Poe left behind a cipher that was broken in the year 2000. The composer Edward Elgar left a message for a young lady that has not yet been fully understood. Treasure codes exist that point the way to huge sums in gold—if only the sequence of symbols can be broken.

At the time of writing, the state-of-the-art cipher is a computer sequence with 2,048 figures, each of which can be a number, letter, or symbol. The combinations are in trillions of trillions, and it is estimated that even the fastest computers in the world couldn't break it in less than thirty billion years. Oddly enough, it was created by a seventeen-year-old boy in Kent, named Peter Parkinson. He is quite pleased with it. To put it in perspective, it is illegal in America to export an encryption program with more than *forty* digits without providing a key. It takes three days to break a fifty-six-bit encryption.

Combinations to computer locks are one thing. This chapter contains some classic ciphers—starting with the one used by Julius Caesar to send messages to his generals.

1. **The Caesar Shift Cipher.** This is a simple alphabet cipher, but tricky to break without the key. Each letter is moved along by a number—say four. A becomes E, J becomes N, Z becomes D, and so on. The number is the key to the cipher here. Caesar could agree on the number with his generals in private and then send encrypted

messages knowing they could not be read without that crucial extra piece of information.

"The dog is sick" becomes "WKH GRJ LV VLFN," with the number three as the key.

As a first cipher it works well, but the problem is that there are only twenty-five possible number choices (twenty-six would take you back to the letter you started with). As a result, someone who really wanted to break the code could simply plod their way through all twenty-five combinations. Admittedly, they would first have to recognize the code as a Caesar cipher, but this one only gets one star for difficulty—it is more than two thousand years old, after all.

2. **Numbers.** A=1, B=2, C=3, etc., all the way to Z=26. Messages can be written using those numbers. This cipher is probably too simple to use on its own; however, if you combine it with a Caesar code number, it can suddenly become very tricky indeed.

   In the basic method, "The dog is better" would be "20 8 5–4 15 7–9 19–2 5 20 20 5 18," which looks difficult but isn't. Add a Caesar cipher of 3, however, and the message becomes "3 23 11 8–7 18 10–12 22–5 8 23 23 8 21," which should overheat the brain of younger brothers or sisters trying to break the encryption. Note that we have included the key number at the beginning. It could be agreed beforehand in private to make this even harder to break. (With the Caesar combination, a difficulty of two stars.)

3. **Alphabet Ciphers.** There are any number of these. Most of them depend on the way the alphabet is written out—agreed on beforehand between the spies.

   A B C D E F G H I J K L M

   N O P Q R S T U V W X Y Z

   With this sequence, "How are you?" would become "UBJ NER LBH?"

   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

   Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

   In this one, "How are you?" would become "SLD ZIV BLF?" It's worth remembering that even simple ciphers are not obvious at first glance. Basic alphabet ciphers may be enough to protect a diary, and they have the benefit of being easy to use and remember.

4. Most famous of the alphabet variations is a **code stick**—another one used by the Romans. Begin with a strip of paper and wind it around a stick. It is important that the sender and the receiver both have the same type of stick. Two bits from the same broom handle would be perfect, but most people end up trying this on a pencil (see picture).

Here the word "Heathrow" is written down the length of the pencil, with a couple of letters per turn of the strip. (You'll need to hold the paper steady with tape.) When the tape is unwound, the same pen is used to fill in the spaces between the letters. The tape should now look like gibberish. The idea is that when it is wound back on to a similar stick, the message will be clear. It is a cipher that requires a bit of forethought, but can be quite satisfying. For a matter of life and death, however, you may need the next method.

5. **Codeword Alphabet Substitution.** You might have noticed a pattern developing here. To make a decent cipher, it is a good idea to agree on the key beforehand. It could be a number, a date, the title of a book, a word, or even a kind of stick. It's the sort of added complexity that can make even a simple encryption quite fiendish.

   Back to one of our earlier examples:

   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

   Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

   If we added the word "window," we would get the next sequence. Note that no letters are repeated, so there are still twenty-six in the bottom sequence and the second "W" of "window" is not used.

   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

   W I N D O A B C E F G H J K L M P Q R S T U V X Y Z