1

MAKING PAPER CRYPTOGRAPHY TOOLS

"The encryption genie is out of the bottle."
—Jan Koum, WhatsApp founder

Before we start writing cipher programs, let's look at the process of encrypting and decrypting with just pencil and paper. This will help you understand how ciphers work and the math that goes into producing their secret messages. In this chapter, you'll learn what we mean by cryptography and how codes are different from ciphers. Then you'll use a simple cipher called the Caesar cipher to encrypt and decrypt messages using paper and pencil.

TOPICS COVERED IN THIS CHAPTER

- What is cryptography?
- Codes and ciphers
- The Caesar cipher
- Cipher wheels
- Doing cryptography with arithmetic
- Double encryption

What Is Cryptography?

Historically, anyone who has needed to share secrets with others, such as spies, soldiers, hackers, pirates, merchants, tyrants, and political activists, has relied on cryptography to make sure their secrets stay secret. *Cryptography* is the science of using secret codes. To understand what cryptography looks like, look at the following two pieces of text:

nyr N.vNwz5uNz5Ns6620Nz0N3z2v
N yvNwz9vNz5N6!9Nyvr9
y0QNnvNwv tyNz
Nw964N6!9N5vzxys690,N.vN2z5u-
3vNz Nr Ny64v,N.vNt644!5ztr vNz
N 6N6 yv90,Nr5uNz Nsvt64v0N
yvN7967v9 BN6wNr33Q N-m63 rz9v

!NN2 Nuwv,N9,vNN!vNrBN3zyN4vN
N6 Qvv0z6nvN.7N0yv4N 4 zzvNN
vyN,NN99z0zz6wz0y3vv26 9
w296vyNNrrNyQst.560N94Nu5y
rN5nz5vv5t6v63zNr5.
N75sz6966NNvw6 zu0 wtNxs6t
49NrN3Ny9Nvzy!

The text on the left is a secret message that has been *encrypted*, or turned into a secret code. It's completely unreadable to anyone who doesn't know how to *decrypt* it, or turn it back into the original English message. The message on the right is random gibberish with no hidden meaning. Encryption keeps a message secret from other people who can't decipher it, even if they get their hands on the encrypted message. *An encrypted message looks exactly like random nonsense.*

A *cryptographer* uses and studies secret codes. Of course, these secret messages don't always remain secret. A *cryptanalyst*, also called a *code breaker* or *hacker*, can hack secret codes and read other people's encrypted messages. This book teaches you how to encrypt and decrypt messages using various techniques. But unfortunately (or fortunately), the type of hacking you'll learn in this book isn't dangerous enough to get you in trouble with the law.

Codes vs. Ciphers

Unlike ciphers, *codes* are made to be understandable and publicly available. Codes substitute messages with symbols that anyone should be able to look up to translate into a message.

In the early 19th century, one well-known code came from the development of the electric telegraph, which allowed for near-instant communication across continents through wires. Sending messages by telegraph was much faster than the previous alternative of sending a horseback rider carrying a bag of letters. However, the telegraph couldn't directly send written letters drawn on paper. Instead, it could send only two types of electric pulses: a short pulse called a "dot" and a long pulse called a "dash."

To convert letters of the alphabet into these dots and dashes, you need an encoding system to translate English to electric pulses. The process of converting English into dots and dashes to send over a telegraph is called *encoding*, and the process of translating electric pulses to English when a message is received is called *decoding*. The code used to encode and decode messages over telegraphs (and later, radio) was called *Morse code*, as shown in Table 1-1. Morse code was developed by Samuel Morse and Alfred Vail.

Table 1-1: International Morse Code Encoding

Letter	Encoding	Letter	Encoding	Number	Encoding
A	•—	N	—•	1	•————
B	—•••	O	———	2	••———
C	—•—•	P	•——•	3	•••——
D	—••	Q	——•—	4	••••—
E	•	R	•—•	5	•••••
F	••—•	S	•••	6	—••••
G	——•	T	—	7	——•••
H	••••	U	••—	8	———••
I	••	V	•••—	9	————•
J	•———	W	•——	0	—————
K	—•—	X	—••—		
L	•—••	Y	—•——		
M	——	Z	——••		

By tapping dots and dashes with a one-button telegraph, a telegraph operator could communicate an English message to someone on the other side of the world almost instantly! (To learn more about Morse code, visit *https://www.nostarch.com/crackingcodes/*.)

In contrast with codes, a *cipher* is a specific type of code meant to keep messages secret. You can use a cipher to turn understandable English text, called *plaintext*, into gibberish that hides a secret message, called the *ciphertext*. A cipher is a set of rules for converting between plaintext and ciphertext. These rules often use a secret key to encrypt or decrypt that only the communicators know. In this book, you'll learn several ciphers and write programs to use these ciphers to encrypt and decrypt text. But first, let's encrypt messages by hand using simple paper tools.

The Caesar Cipher

The first cipher you'll learn is the Caesar cipher, which is named after Julius Caesar who used it 2000 years ago. The good news is that it's simple and easy to learn. The bad news is that because it's so simple, it's also easy for a cryptanalyst to break. However, it's still a useful learning exercise.

The Caesar cipher works by substituting each letter of a message with a new letter after shifting the alphabet over. For example, Julius Caesar substituted letters in his messages by shifting the letters in the alphabet down by three, and then replacing every letter with the letters in his shifted alphabet.

For example, every A in the message would be replaced by a D, every B would be an E, and so on. When Caesar needed to shift letters at the end of the alphabet, such as Y, he would wrap around to the beginning of the alphabet and shift three places to B. In this section, we'll encrypt a message by hand using the Caesar cipher.

The Cipher Wheel

To make converting plaintext to ciphertext using the Caesar cipher easier, we'll use a *cipher wheel*, also called a *cipher disk*. The cipher wheel consists of two rings of letters; each ring is split up into 26 slots (for a 26-letter alphabet). The outer ring represents the plaintext alphabet, and the inner ring represents the corresponding letters in the ciphertext. The inner ring also numbers the letters from 0 to 25. These numbers represent the *encryption key*, which in this case is the number of letters required to shift from A to the corresponding letter on the inner ring. Because the shift is circular, shifting with a key greater than 25 makes the alphabets wrap around, so shifting by 26 would be the same as shifting by 0, shifting by 27 would be the same as shifting by 1, and so on.

You can access a virtual cipher wheel online at *https://www.nostarch.com/crackingcodes/*. Figure 1-1 shows what it looks like. To spin the wheel, click it and then move the mouse cursor around until the configuration you want is in place. Then click the mouse again to stop the wheel from spinning.

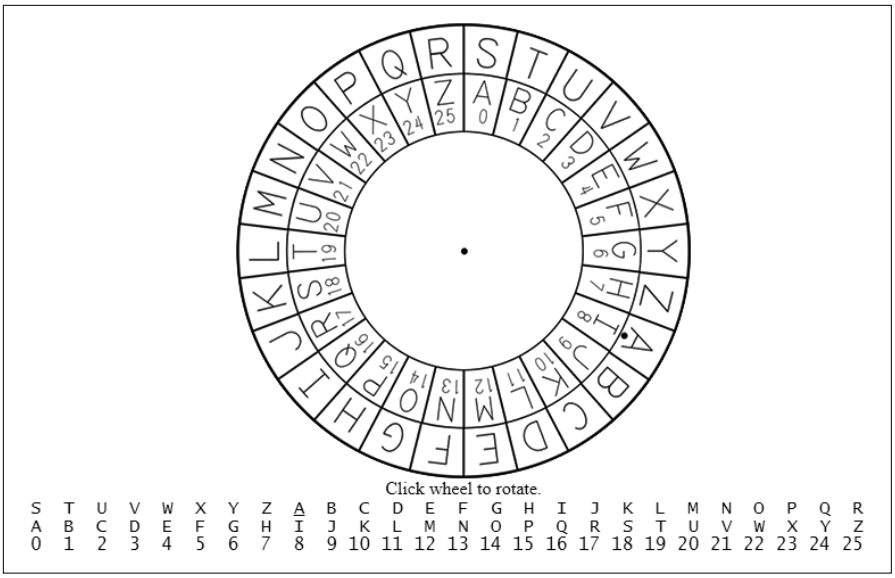

Figure 1-1: The online cipher wheel

A printable paper cipher wheel is also available from the book's website. Cut out the two circles and lay them on top of each other, placing the smaller one in the middle of the larger one. Insert a pin or brad through the center of both circles so you can spin them around in place.

Using either the paper or the virtual wheel, you can encrypt secret messages by hand.

Encrypting with the Cipher Wheel

To begin encrypting, write your message in English on a piece of paper. For this example, we'll encrypt the message THE SECRET PASSWORD IS ROSEBUD. Next, spin the inner wheel of the cipher wheel until its slots match up with slots in the outer wheel. Notice the dot next to the letter A in the outer wheel. Take note of the number in the inner wheel next to this dot. This is the encryption key.

For example, in Figure 1-1, the outer circle's A is over the inner circle's number 8. We'll use this encryption key to encrypt the message in our example, as shown in Figure 1-2.

T	H	E		S	E	C	R	E	T		P	A	S	S	W	O	R	D		I	S		R	O	S	E	B	U	D
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B	P	M		A	M	K	Z	M	B		X	I	A	A	E	W	Z	L		Q	A		Z	W	A	M	J	C	L

Figure 1-2: Encrypting a message with a Caesar cipher key of 8

For each letter in the message, find it in the outer circle and replace it with the corresponding letter in the inner circle. In this example, the first letter in the message is T (the first T in "THE SECRET…"), so find the

letter T in the outer circle and then find the corresponding letter in the inner circle, which is the letter B. So the secret message always replaces a T with a B. (If you were using a different encryption key, each T in the plaintext would be replaced with a different letter.) The next letter in the message is H, which turns into P. The letter E turns into M. Each letter on the outer wheel always encrypts to the same letter on the inner wheel. To save time, after you look up the first T in "THE SECRET…" and see that it encrypts to B, you can replace every T in the message with B, so you only need to look up a letter once.

After you encrypt the entire message, the original message, THE SECRET PASSWORD IS ROSEBUD, becomes BPM AMKZMB XIAAEWZL QA ZWAMJCL. Notice that non-letter characters, such as the spaces, are not changed.

Now you can send this encrypted message to someone (or keep it for yourself), and nobody will be able to read it unless you tell them the secret encryption key. Be sure to keep the encryption key a secret; the ciphertext can be read by anyone who knows that the message was encrypted with key 8.

Decrypting with the Cipher Wheel

To decrypt a ciphertext, start from the inner circle of the cipher wheel and then move to the outer circle. For example, let's say you receive the ciphertext IWT CTL EPHHLDGS XH HLDGSUXHW. You wouldn't be able to decrypt the message unless you knew the key (or unless you were a clever hacker). Luckily, your friend has already told you that they use the key 15 for their messages. The cipher wheel for this key is shown in Figure 1-3.

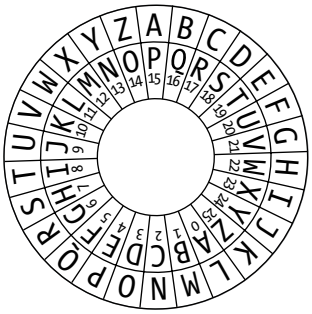

Figure 1-3: A cipher wheel set to key 15

Now you can line up the letter A on the outer circle (the one with the dot below it) over the letter on the inner circle that has the number 15 (which is the letter P). Then, find the first letter in the secret message on the inner circle, which is I, and look at the corresponding letter on the outer circle, which is T. The second letter in the ciphertext, W, decrypts to the letter H. Decrypt the rest of the letters in the ciphertext back to the plaintext, and you'll get the message THE NEW PASSWORD IS SWORDFISH, as shown in Figure 1-4.

I	W	T		C	T	L		E	P	H	H	L	D	G	S		X	H		H	L	D	G	S	U	X	H	W
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
T	H	E		N	E	W		P	A	S	S	W	O	R	D		I	S		S	W	O	R	D	F	I	S	H

Figure 1-4: Decrypting a message with a Caesar cipher key of 15

If you used an incorrect key, like 16, the decrypted message would be SGD MDV OZRRVNQC HR RVNQCEHRG, which is unreadable. Unless the correct key is used, the decrypted message won't be understandable.

Encrypting and Decrypting with Arithmetic

The cipher wheel is a convenient tool for encrypting and decrypting with the Caesar cipher, but you can also encrypt and decrypt using arithmetic. To do so, write the letters of the alphabet from A to Z with the numbers from 0 to 25 under each letter. Begin with 0 under the A, 1 under the B, and so on until 25 is under the Z. Figure 1-5 shows what it should look like.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 1-5: Numbering the alphabet from 0 to 25

You can use this letters-to-numbers code to represent letters. This is a powerful concept, because it allows you to do math on letters. For example, if you represent the letters CAT as the numbers 2, 0, and 19, you can add 3 to get the numbers 5, 3, and 22. These new numbers represent the letters FDW, as shown in Figure 1-5. You have just "added" 3 to the word *cat*! Later, we'll be able to program a computer to do this math for us.

To use arithmetic to encrypt with the Caesar cipher, find the number under the letter you want to encrypt and add the key number to it. The resulting sum is the number under the encrypted letter. For example, let's encrypt HELLO. HOW ARE YOU? using the key 13. (You can use any number from 1 to 25 for the key.) First, find the number under H, which is 7. Then add 13 to this number: 7 + 13 = 20. Because the number 20 is under the letter U, the letter H encrypts to U.

Similarly, to encrypt the letter E (4), add 4 + 13 = 17. The number above 17 is R, so E gets encrypted to R, and so on.

This process works fine until the letter O. The number under O is 14. But 14 plus 13 is 27, and the list of numbers only goes up to 25. If the sum of the letter's number and the key is 26 or more, you need to subtract 26 from it. In this case, 27 – 26 = 1. The letter above the number 1 is B, so O encrypts to B using the key 13. When you encrypt each letter in the message, the ciphertext will be URYYB. UBJ NER LBH?

To decrypt the ciphertext, subtract the key instead of adding it. The number of the ciphertext letter B is 1. Subtract 13 from 1 to get –12. Like our "subtract 26" rule for encrypting, when the result is less than 0 when decrypting, we need to add 26. Because –12 + 26 = 14, the ciphertext letter B decrypts to O.

NOTE *If you don't know how to add and subtract with negative numbers, you can read about it at* https://www.nostarch.com/crackingcodes/.

As you can see, you don't need a cipher wheel to use the Caesar cipher. All you need is a pencil, a piece of paper, and some simple arithmetic!

Why Double Encryption Doesn't Work

You might think encrypting a message twice using two different keys would double the strength of the encryption. But this isn't the case with the Caesar cipher (and most other ciphers). In fact, the result of double encryption is the same as what you would get after one normal encryption. Let's try double encrypting a message to see why.

For example, if you encrypt the word KITTEN using the key 3, you're adding 3 to the plaintext letter's number, and the resulting ciphertext would be NLWWHQ. If you then encrypt NLWWHQ, this time using the key 4, the resulting ciphertext would be RPAALU because you're adding 4 to the plaintext letter's number. But this is the same as encrypting the word KITTEN once with a key of 7.

For most ciphers, encrypting more than once doesn't provide additional strength. In fact, if you encrypt some plaintext with two keys that add up to 26, the resulting ciphertext will be the same as the original plaintext!

Summary

The Caesar cipher and other ciphers like it were used to encrypt secret information for several centuries. But if you wanted to encrypt a long message—say, an entire book—it could take days or weeks to encrypt it all by hand. This is where programming can help. A computer can encrypt and decrypt a large amount of text in less than a second!

To use a computer for encryption, you need to learn how to *program*, or instruct, the computer to do the same steps we just did using a language the computer can understand. Fortunately, learning a programming language like Python isn't nearly as difficult as learning a foreign language like Japanese or Spanish. You also don't need to know much math besides addition, subtraction, and multiplication. All you need is a computer and this book!

Let's move on to Chapter 2, where we'll learn how to use Python's interactive shell to explore code one line at a time.

PRACTICE QUESTIONS

Answers to the practice questions can be found on the book's website at *https://www.nostarch.com/crackingcodes/*.

1. Encrypt the following entries from Ambrose Bierce's *The Devil's Dictionary* with the given keys:
   a. With key 4: "AMBIDEXTROUS: Able to pick with equal skill a right-hand pocket or a left."
   b. With key 17: "GUILLOTINE: A machine which makes a Frenchman shrug his shoulders with good reason."
   c. With key 21: "IMPIETY: Your irreverence toward my deity."
2. Decrypt the following ciphertexts with the given keys:
   a. With key 15: "ZXAI: P RDHIJBT HDBTIXBTH LDGC QN HRDIRWBTC XC PBTGXRP PCS PBTGXRPCH XC HRDIAPCS."
   b. With key 4: "MQTSWXSV: E VMZEP EWTMVERX XS TYFPMG LSRSVW."
3. Encrypt the following sentence with the key 0: "This is a silly example."
4. Here are some words and their encryptions. Which key was used for each word?
   a. ROSEBUD – LIMYVOX
   b. YAMAMOTO – PRDRDFKF
   c. ASTRONOMY – HZAYVUVTF
5. What does this sentence encrypted with key 8 decrypt to with key 9? "UMMSVMAA: Cvkwuuwv xibqmvkm qv xtivvqvo i zmdmvom bpib qa ewzbp epqtm."