7. The Whisper Network

Standard: 2-NI-06: Use encryption to secure data for transmission

You settle down to watch the newly gated moss device that you created in Chapter 6, "Securing the Moss," to see if any visitors are able to enter the correct password to gain entrance. You're happy to notice that a line has formed, made up of small black ants, who seem to need to get to the moss. They seem to know the password and gain entrance quickly. What are they up to? And how did they manage to get the password so quickly, given that you just implemented the system?

Being aware of security, break-ins, and hacks, you comment to the Guide, "These ants are up to something suspicious!" "I don't think so," the Guide says with a smile. "Listen!"

You listen attentively and notice a low undercurrent of what can only be described as whispered words and numbers. What on Earth could that be? Bending down, you observe two ants chatting to each other in tiny voices. "What are they saying?" you ask, puzzled. "It's not a language I've ever heard!"

"It's encrypted," replies the Guide. "These ants have developed a sophisticated way to transmit information among the members of their community. No other creature understands what they say, but they seem to be able to tell each other important things such as the gate's password and, most important, the locations of the different patches of this type of moss throughout the forest. They may be an ancient race of creatures, but they use modern encryption to communicate secrets that only they must know. They are the keepers of the moss, you know." You didn't know, actually.

It appears that the moss depends on these ants. The ants help the moss propagate by carrying its spores to new areas of the forest. They are all part of the ecosystem that ensures the moss's survival. "If you could discover what they use to encrypt their messages, you'd be doing me a service," states the Guide. She lifts an ant into her hand and asks it, "Friend, where can we find another

patch of moss?" The ant readily tells her, "Xli qsww mw mr xli gezi ex 86.705589 pexmxyhi erh -a5.d9adb7 psrkmxyhi."

Can you crack the ant's code?

> **Definition**
>
> *Encryption* is the process of converting data into a form that is unreadable by people who do not possess a key to decipher it.

Do Some Research

Since you're learning about encryption, this is a golden opportunity to dive into this rich field of inquiry. People have been trying to keep their messages to each other safe from prying eyes since the dawn of history. One very early example of encrypted communication is the smoke signal, which was used millennia ago, on the Great Wall of China, to send alerts from one turret to another, often using colored smoke.

Ancient Greeks used a method of arranging torches in patterns to signal messages alphabetically. The arrangement of torches represented a number that was converted to a part of the Greek alphabet.

> **Definition**
>
> *Cryptography* is the study of all the various techniques used to protect messages.

More and more sophisticated ways of encrypting messages have evolved over time. In the information age, powerful computers are available to decrypt

and read these encrypted messages. There is always a balance between how sophisticated the encryption is and how quickly the intended user can decrypt and use the message. There is a need to ensure that the messages cannot be decrypted easily by unintended interceptors.

In this chapter, you'll work with an early encryption strategy, the Caesar cipher. There are many more strategies, including the following, which are presented in chronological order, starting with the oldest:

The Caesar Cipher A cipher that involves shifting letters along a given number of spaces in the alphabet, such that in a Caesar cipher of "shift 2," the letter *a* becomes *c*, and *c* becomes *e*.

The Vigenère Cipher While a Caesar cipher involves shifting letters along a given number of spaces in the alphabet, a Vigenère cipher is more complex, including several Caesar ciphers with different shift values in a sequence. Rather than a one-line shift along the alphabet, this cipher is represented as a table.

Affine Cipher This type of cipher is a substitution cipher like the Caesar cipher, except that letters are mapped to corresponding numbers and encrypted with a mathematical function.

M-94 and the Enigma Machine These were machines used in World Wars I and II to encrypt messages. The M-94 was a cylinder that could be manipulated to create secret messages that were formed and encrypted by aligning letters horizontally. The Enigma machine was used in World War II by the Axis powers. In a more sophisticated version of the M-94, its scrambled letters changed each day, with the order only known to the senders. This made the window for decryption short.

RSA Named for its inventors, Rivest, Shami, and Adleman, RSA is a modern public-key system in which a public key, used for encryption, is different from a private key, used for decryption. The public key is created by using two large numbers, which are kept secret. Messages can be decoded only by someone with access to both of those numbers. The larger the key, the harder it is to crack the system.

Steganography This is a completely different way of encoding messages. Steganography refers to hiding messages in common formats such as audio, images, or video. Messages can be found when playing audio at a certain volume or video at a certain speed, or by looking at only certain pixels of images. Try an online steganography tool to hide messages in images. These tools allow you to hide a message in an image, save it, and decode it. They do so by subtly attaching extra data to the image's pixels.

> **Definition**
>
> While text can be encrypted using either the *public* or the *private* key, the other key must be used to decrypt the message. Public keys are made available to the public, but only a recipient of a message should have access to and use a private key to decrypt. Learn more about keys at `www.cloudflare.com/learning/ssl/what-is-a-cryptographic-key`.

Do some research on other ways that messages can be encoded and decoded.

Think Like a Computer Scientist: Encryption and Keys

You might wonder how you can put into use a basic cipher such as the one used by Julius Caesar over 2,000 years ago. This cipher is a simple method of encrypting text by shifting each letter by a certain number of places, as shown in Figure 7.1. To decode a message, the reader needs to know that the alphabet order is shifted a given number of places—that's the "key" to decode the message.

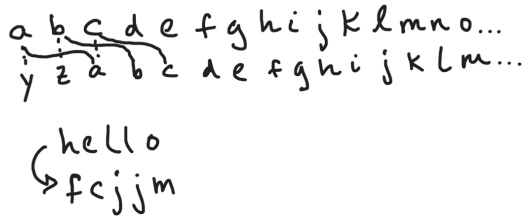

FIGURE 7.1: A letter-shifted cipher

> **Note**
>
> You'll be able to create a Caesar cipher of your own later in this chapter. Even if it's a simple cipher, it's not so simple to decode it if you don't have a key!

> **Definition**
>
> A *key*, as used for encryption, is a series of numbers used to encrypt or decrypt data. If a key is long and complex, it is more difficult to guess it and thus break an encrypted code. Without a key, it becomes necessary to use various techniques, from "brute-force" guessing to more complex methods, to decrypt a message. Learn more about keys here: `https://phemex.com/academy/what-is-symmetric-key-encryption`.

There are two types of encryption: symmetric encryption and asymmetric encryption. The difference is in their use of keys.

Symmetric encryption relies on a shared secret key to both encrypt and decrypt data. Say, for example, that the key to decrypting a given word is the fact

that it is spelled backward. If you know this fact, and the person receiving the encrypted word knows this fact, then the recipient of the word can decode it much faster. There are several different algorithms, some more secure than others and some faster than others, to encrypt data so that a key can help decrypt it efficiently.

Definition

In this context, an *algorithm* is a mathematical formula that converts plain-text messages to encrypted text, also called cyphertext. Learn more about algorithms in cryptography at `https://docs.aws.amazon.com/crypto/latest/userguide/concepts-algorithms.html`.

Asymmetric encryption is the process of encrypting data with a public key and decrypting it with a private key. The public key is shared with the recipient of the data, and the private key is kept secret. The recipient of the data can decrypt the data with the private key but cannot decrypt the data with the public key.

An example of a key would be the Letter + 2 key in the Caesar cipher depicted in Figure 7.1. A more complicated key is depicted in Figure 7.2, where text is encrypted using a Letter + 7 key, such that letters are shifted forward by 7.

While encryption is a useful way to encode messages to protect them, these techniques are not enough to ensure a message's security. There are several elements that need to be considered to enhance security:

- The path from user to server needs to be protected to prevent interception.
- Once data is decrypted, or deciphered for use on a server, other processes need to come into play to continue to protect its integrity.
- The storage of the message on a server needs to also be protected to prevent tampering.

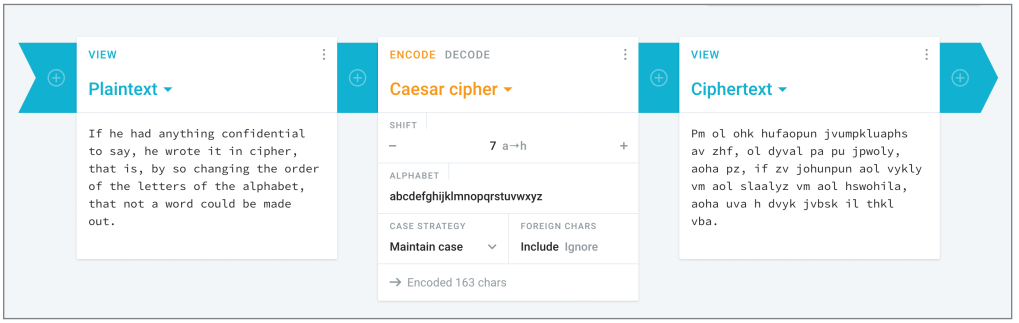

FIGURE 7.2: A Caesar cipher as depicted on `criptii.com`

Your Challenge

What are the ants telling each other? It's some sort of code, but you don't understand any of it, and neither does your Guide. Your job: determine what kind of encryption they are using and decrypt their message by using a key.

Sketch It Out

Practice both decoding a sample message and then encoding one of your own. Start with the first task. You have a message that you need to decode for the Guide so that she can continue in her role as caretaker of the entire forest. Here is the ant's message again: "Xli qsww mw mr xli gezi ex 86.705589 pexmxyhi erh -a5.d9adb7 psrkmxyhi."

Assume that this is a Caesar cipher, which is characterized by a letter shift. This letter shift value is the key, and your job is to determine the key's value and decode the message. Sketch out the message, the alphabet and numbers you think are included in the code, and a possible letter shift, as can be seen in Figure 7.3. If it's helpful, create two strips of paper and copy the alphabet sequence onto each. You can keep one strip stable and move the other strip to try different letter shifts to determine the key that was used to encrypt the message.

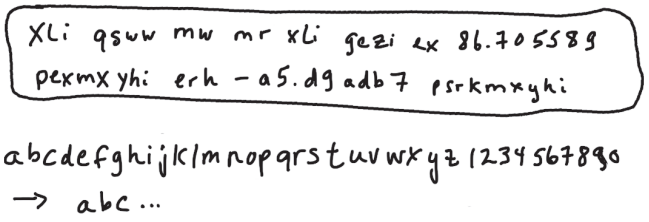

FIGURE 7.3: A cipher to decrypt

Project Recipe

You have two tasks before you. First is to decrypt a message for which you have no key, and second, for practice, to encrypt a message with a key and challenge someone to decrypt it. Start by tackling the first, because there are a few ways to approach the problem.

Step 1: Brute Force

Since there are only 26 letters to try, plus the numbers 1,2,3,4,5,6,7,8,9 and 0, and the letters are in the right order, this encrypted message is susceptible to being decoded by what is called brute force. Brute force decryption involves trying one method after another to try to guess an encrypted code's key. In this case, make guesses that start with a presumed key of 1, meaning that A has been shifted to B.

Your first guess might be that the key is 1+. So, A is shifted to B, B to C, and so on. Try the first few letters to see if they make sense. Consider Xli, the first three characters of the code. If the key is 1+, the first letters, decoded, will be wkh. If the key is 2+, it's vjg. If 3+, it's uif. Keep going until the first word makes some sense in English. Does it seem to be using the same shift key if you decode a second word?

> **Note**
>
> If you need to, use the strips of paper from your earlier sketch to create a sort of "decoder ring" for yourself so that you can visualize the letter shifts more easily.

Step 2: Frequency Analysis

Try a different strategy to crack the code that's slightly better than brute force: frequency analysis. Since this code has breaks between words and the code is presumed to be in English, you can try to see if you can determine patterns based on common words in English that have repeated letters. Think about "is," "the," "an," and "in." Circle repeated letters and try to decipher a pattern as shown in Figure 7.4. Does the word "Xli" correspond in theory to any common three-letter word in English? Is the repeated "i" character a good clue to pursue to figure out other words? Which letters, in English, tend to be repeated often, and which don't? Can that help you rule out some letters, like x and z?

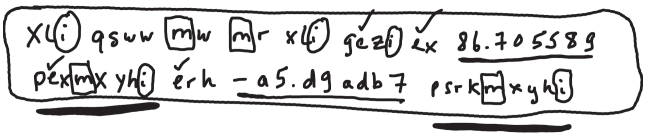

FIGURE 7.4: Attempting to decrypt a cipher

In addition, this code has a peculiarity in that it also includes numbers: 86.705589 and the strange-looking cipher –a5.d9adb7. There is a pattern in these numbers that you might be able to visualize if you break up the words:

```
86.705589 pexmxyhi
erh
-a5.d9adb7 psrkmxyhi
```

Context can help, too! What topic do you think the ants are discussing? Could it have anything to do with moss? Do you see any word in the code that might represent the word "moss"?

Finally, consider how English sentences often begin. What is a common three-letter word that might fit here? The answer to this code is at the end of this chapter, but try to figure it out by yourself!

Step 3: Encrypt a Message

Now it's your turn to encrypt a message. You can continue with a Caesar cipher, or find something more difficult to crack, perhaps a Vigenère or Affine cipher. You can use the tools available for encrypting messages on `https://cryptii.com` or do the encryption by hand.

Try a Vigenère cipher. In this method, the letter shift is done using a key as well as a Vigenère square, or "tabula recta," shown in Figure 7.5.

To do the encryption, imagine you are encrypting the phrase "Preservetheforest." Select a key word such as "guide." Build up the keyword to match the character count of the phrase: "guideguideguidegu."

Use the table to match the phrase horizontally with the first letter of the keyword. So, the first letter, P, matched with G vertically, correlates to V. The next letter, R, matches with U, so the correlation in ciphertext is L. The ciphertext is thus "vlmvixpmwlkzwuiyn." You can see how this cipher is harder to crack, because you now need the table and key to make any sense of it!

Extend Your Knowledge

The history of encryption and cryptography is fascinating and dates back thousands of years. Visit the Bletchley Park website at `https://bletchleypark.org.uk` to learn more about the history of cryptography, in particular during World War II. Bletchley was the location where Alan Turing worked to create machines used to decrypt the German Enigma cipher during World War II. Learn more about Turing and advances in the field of cryptography at the museum website.

	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
a	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
b	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	a
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	z	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

FIGURE 7.5: A Vigenère square

Vocabulary Review

In your own words, describe:

- Cryptography
- Encryption
- Steganography

Quiz

Select the best answer for each of the following:

Q1: Steganography allows you to hide a message in an audio or image file.

a. True

b. False

Q2: Symmetric encryption is a method of encrypting data using:

a. A public key
b. An NFT
c. A shared secret key

Q3: Asymmetric encryption is a method of encrypting data using:

a. Two keys
b. One private key
c. One shared key

Assignment: Let's Encrypt

In this chapter, you learned about different methods of encryption used to protect data. Practice your knowledge by converting a message using an encryption technique of your choice and challenging others to decipher it. Research and try:

- A Caesar cipher
- A Vigenère cipher
- Any encryption technique of your choice

The message, encoded, is "The moss is in the cave at 42.361145 latitude and –71.057083 longitude" and the shift is 4+. Did you figure it out?