Chapter 2

SUBSTITUTION AND CAESAR'S CIPHER

If your mission is to win a war, maintaining secrecy is mission-critical. Ancient warrior Julius Caesar was extremely eager to disguise written messages, and he came up with Caesar's cipher, a simple system that is not particularly secure once the method is known.

Caesar's cipher example: FIVE AM encrypts to GJWF BN

Here's a slightly simplified version of how it works. Say Caesar wants to send a written message, FIVE AM, to his generals, instructing them to attack at that time. In the emperor's system, each letter in the message FIVE AM is advanced one place in the alphabet. F becomes G, I becomes J, V becomes W, and so on. The generals receive GJWF BN, and, knowing that the procedure to reclaim the message meaning is "subtract 1," they convert G back to F, J to I, and so on until the message makes sense.

To aid decoding, Caesar may have given his generals the helpful chart shown in Figure 2-1.

To encrypt (disguise) a message, you convert each letter of the message to the letter directly underneath it in the chart. A is converted to B and so on. Mathematically, this method can be described as follows: message letter + 1 place = encrypted (disguised) letter. Z, the last letter, is converted to A.

Definitions: cipher, plaintext, ciphertext, encryption, decryption, encipher, encrypt, decipher, decrypt

A *cipher* is a method that encrypts or disguises text. The undisguised text is called *plaintext*, and the disguised text is called *ciphertext***.** The process of transforming plaintext to ciphertext is called *encryption*. The reverse is called *decryption*. *Encipher* and *encrypt* mean the same thing: to confuse or hide meaning. Similarly, *decipher* and *decrypt* both mean to remove disguise and reclaim meaning. See Figure 2-2 for some helpful pictures.

Plain	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
Ciphered	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

Figure 2-1 This chart helps in decoding Caesar's messages.

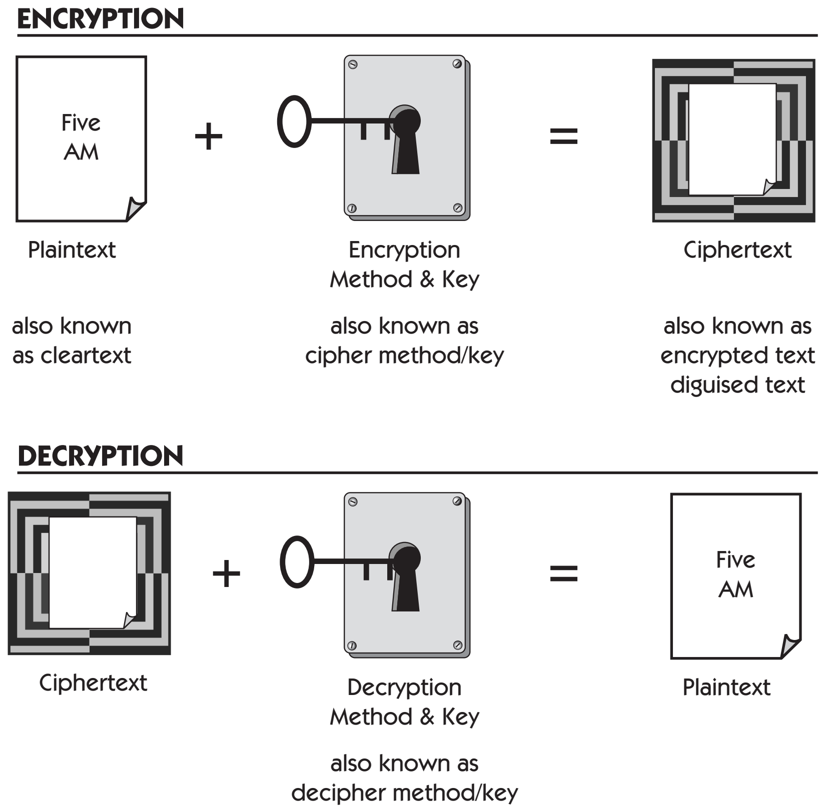


Figure 2-2 Encryption and decryption.

Note that even though it's called "plaintext," it could as well be "plain pictures" or "plain audio" or "plain video."

Definition: substitution cipher algorithm

In Figure 2-1 we used the labels "Plain" and "Ciphered" because Caesar's cipher transforms a plain alphabet into a ciphered alphabet. Each letter of ciphertext substitutes for a letter of plaintext. This is called a *substitution* cipher.[1]

Caesar's cipher combines a method—called, in mathematics, an *algorithm*—and a key. The method is "add," and the key (how many times to do it) is 1. Julius Caesar's cipher was actually slightly more complex; he rotated the cipher alphabet three places. If you understand "F + 1 = G," it follows that "F + 2 = H" and "F + 3 = I," assuming that your cipher alphabet is in alphabetical order. The `F` in `FIVE` becomes `I`, so `FIVE AM` translates to `ILYH DP` (see Figure 2-3).

[1] Purists prefer to categorize this as a *shift* cipher or *rotational* cipher, a special kind of substitution.

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
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

Figure 2-3 Caesar's cipher variation: rotating each letter three places.

Advancing three letters, instead of one, shows what happens when you add levels of complexity to a key. An adversary trying to understand your disguised message must work a little harder to reclaim plaintext from an enciphered message that rotates the alphabetic code by three letters (Figure 2-3) than with a ciphered message that rotates the alphabetic code by one letter (Figure 2-1).

Number of possible keys dictates number of possible encryptions.

Julius Caesar used the ciphered alphabet in Figure 2-3. His nephew, Augustus Caesar, said to be less able than his uncle, used the ciphered alphabet in Figure 2-1. Figures 2-1 and 2-3 show the results of using two Caesar's cipher keys—1 and 3, respectively—of 25 possible keys; that is, there are 25 different ways to disguise letters of the alphabet using a Caesar cipher method.

The concentric alphabet circles in Figure 2-4 can be used to picture any possible key. The outer ring is fixed and does not rotate. It's the plaintext alphabet that is used to write the message. The inner, or cipher, circle is the cipher alphabet used to create the disguised text. Each movement of the inner cipher circle creates a new cipher alphabet. The diamond shapes in key 1 point to the letters `FIVE AM`.

In Figure 2-4, one of the four keys—1, 2, 24, or 25—is displayed inside each circle. The inner wheel rotates the "key" number of positions: 1, 2, 24, or 25. After 25, the cipher alphabet has turned full circle and the key returns to 0. In other words, at "key" 0 the message and ciphertext are the same—oops, not a disguise!

The key tells how far to move the inner circle alphabet from the initial position where the `A'`s in both alphabet circles match—remember, that's key 0.

The Origin of Cipher

The Arabic *sifr* is the root from which we get our words *cipher* and *zero.* After the thirteenth century, Europeans began using Arabic numerals rather than Roman numerals because decimals and zeroes made European medieval mathematicians very happy. But the concept of zero confused common people in the Middle Ages; so when they referred to something that wasn't quite clear, they compared it to something they considered a mystery: the cipher. Eventually the word *cipher* evolved to describe concealment of clear meaning.

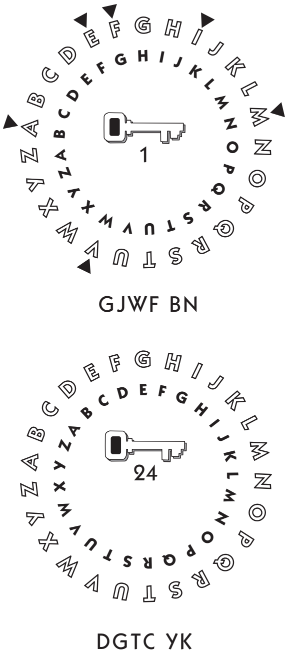


Figure 2-4 Four Caesar cipher keys—1, 2, 24, and 25—encrypting `FIVE AM`.

The four different cipher combinations for the plaintext message `FIVE AM` are shown below each cipher circle. Because all the inner cipher circles are in alphabetical order, the differing ciphertext is *due only to the key*, which tells how many places to rotate the cipher alphabet in relation to the message alphabet.

Cryptanalysis of Caesar's Cipher

Caesar's cipher: only 25 possible keys. Much too few.

Caesar's cipher is a little bit confusing if you've never seen it, but the confusion is easy to overcome. To cryptanalyze a message using this cipher, you simply put the encrypted text on the top row and repeatedly increase each letter one alphabetic position (see Figure 2-5). For example, you replace *I* with *J*, then *K*, then *L*, and so on. Most trials produce gibberish. When you are successful, the English plaintext jumps out upon inspection.

It's important to understand that Caesar's cipher has only 25 possible keys. Next, you'll see other methods with many more possible keys.

More keys means more work for your adversary.

Throughout this book the "key" concept is the same. Like Caesar and his generals, you and your confidant share a key. The object is to make your adversary work a long time trying many, many keys. Hopefully, by the time an

	I	L	Y	H	D	P
+1	J	M	Z	I	E	Q
+2	K	N	A	J	F	R
+3	L	O	B	K	G	S
+4	M	P	C	L	H	T
. . .						
+17	Z	D	P	Y	U	G
+18	A	E	Q	Z	V	H
+19	B	F	R	A	W	I
+20	C	H	S	B	X	J
+21	D	G	T	C	Y	K
+22	E	H	U	D	Z	L
+23	F	I	V	E	A	M
+24	G	J	W	F	B	N
+25	H	K	X	G	C	O
+26	I	L	Y	H	D	P

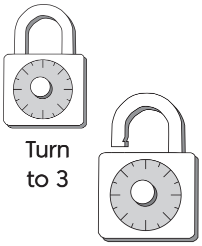
Figure 2-5 Caesar's cipher cryptanalysis: Meaningful text appears after 23 tries.

adversary finds the correct decrypting key, the encrypted message has little value. At 5:01, the value of a `FIVE AM` attack message is greatly reduced. We'll see cryptographic methods that put your adversary to work for thousands of years, just in case unforeseen technological advances permit your adversary to do in hours what used to take years.

Empowering the Masses

After Gutenberg invented the printing press, more people learned to read. With more people knowing the reading code, encryption systems such as Caesar's cipher were subjected to increasingly educated scrutiny. Secure hiding demanded increasingly elaborate encrypting.

Anyone who can read can quickly try all 25 keys. Also, if you figure out just one letter of ciphertext that corresponds to plaintext, you've got the key. For example, knowing that `E` is encrypted as `K` (see Figure 2-6) lets you determine all the letters in the inside cipher circle by simply filling in the remaining alphabet in alphabetical order. Well, what to do, what to do? Don't teach them to read! Although it may not be ethical or particularly democratic, this approach worked for quite a long time. Major institutions supported it for centuries (and based on the reading scores of many American children, perhaps some of them still do).



If you want to keep important secrets hidden from the reading masses, using 25 alphabetically ordered alphabets does not provide enough complexity. It's like using a combination lock that has only 26 numbers on the face—and a one-number combination key (say, turn to 3) opens the lock.

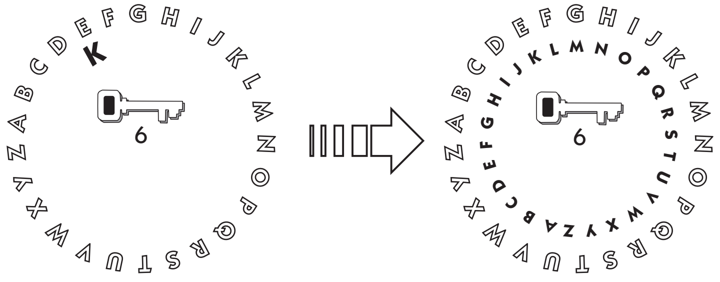


Figure 2-6 Cryptanalysis of one letter determines the entire cipher alphabet.

Messages Inside and Out

Even though ideography, the written form of Chinese, is very old, cryptography wasn't used in China in ancient times. The ancient Chinese didn't have a great need to disguise their writing because few people knew how to read. Also, ideographic writing doesn't lend itself to cryptography as well as an alphabetic language does, so the Chinese found other ways to hide meaning. Diplomatic and military messages were memorized or hidden on or in the messenger.

Using cipher circles, the key is the number of positions to move the inner cipher circle. Caesar's generals simply moved the inner cipher circle to the position indicated by the key number. Based on probability, Caesar's adversaries must try about half the keys (about 12), on average, until they stumble on the correct key and decrypt the message.

The Importance of Separating the Method and the Key

Review: method and key

Before we add a huge number of keys to befuddle hound-dog cryptanalysts, let's reinforce the concepts of method and key. The method in a Caesar cipher type of encryption system is to rotate the alphabetic ordering of the ciphertext 1 to 25 places in relation to the plaintext. Caesar's adversaries, as well as generals, can know the method, but they need the key to quickly decrypt the message.

The method is not secret. The key is secret.

The important concept is that anyone can have the cryptographic method. The method "shift the letters in the alphabet" can be written on the walls of the Roman Coliseum, published on the front page of *The New York Times*, or posted to an Internet site. You may share many secrets, but all your secrets are built on the fact that you and your confidant share a *secret key*. Your secrets are only as secure as your secret key. Even though an adversary may know your encryption method, it is the joining of the encryption method with your unique secret key that secures messages for anyone who doesn't have the secret key.

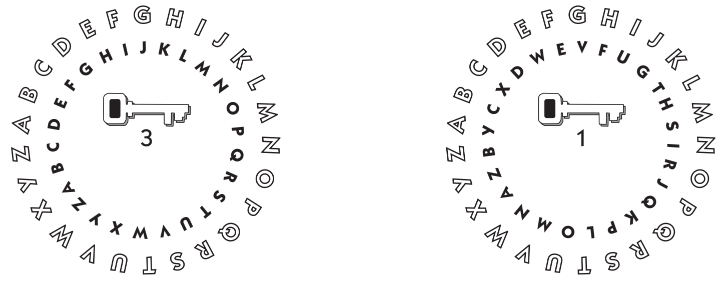
Adding Keys

There are ways to make an adversary try many more keys than discussed so far to find the correct decrypted message. Suppose Alice gives Bob two different cipher circles (see Figure 2-7).

Both cipher circles have an outer, alphabetically ordered plaintext ring, but each cipher circle has a different inner ring. Cipher circle 1 is Caesar's cipher, but the inner ring of the cipher circle 2 is different: We've altered the normal ordered sequence of the alphabet.

This system allows Alice to increase complexity by doubling the number of possible cipher alphabets. Now Bob will need a two-part secret key. Part 1 of the secret key identifies which cipher circle—the first or the second—to use; part 2 of the secret key is just like Caesar's cipher key: the number of positions to rotate the chosen ring.

Now Alice has 50 possible encrypted alphabets: 25 from each cipher circle. Cipher circle 2 disguises plaintext better than cipher circle 1 because the inner cipher alphabet ring is not in alphabetic order. This means that knowing a single letter on the inner ring does not immediately allow an adversary to fill in the rest of the cipher letters.


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
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
3
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
X D W E V F U G T H S I R J Q K P L O M N A Z B Y C
1

Cipher circle 1

Cipher circle 2

Figure 2-7 Two cipher circles with different inner cipher alphabets.

Cipher circle 2's inner ring is just one of about 400 million-billion-billion possible inner rings. This is much more than a 400 million + a billion + a billion. It is a 400 million times a billion times a billion—much too large a number for anyone to imagine.

A Weakness of Caesar's Ciphers: The Failure to Hide Linguistic Patterns

Given the high number of possible inner rings, you might think that every Alice could simply make some unordered rings and thereby ensure safe encrypted messages forever. Not so—it's still easy to break or cryptanalyze.

Let's see why. Suppose the plaintext message is `EVERYONE MUST ATTACK BEFORE FIVE AM`. It doesn't matter which cipher ring or key Caesar uses to encrypt the message. To illustrate our point, let's use the cipher alphabet shown in Figure 2-8.

Merely using a large number of potential keys is not a secure method.

The encrypted message certainly looks like gibberish—but not to a cryptanalyst, who would instantly see that there are six `H`s and three `C`s. Because `E` is the most used letter in English, the cryptanalyst would substitute `E` for all the `H`s and then substitute `T`, the second most used letter, for all the `C`s. The decryption is well under way even though the cryptanalyst isn't using the secret cipher circles and doesn't know the key.

The billions and billions of possible keys don't necessarily slow a cryptanalyst very much. That's because the Caesar's cipher method does not disguise the linguistic patterns of letter and word frequency in the encrypted message. In this type of encryption, those patterns are the same as in the plaintext message. This aspect of the Caesar cipher method gives a good cryptanalyst enough information to very quickly recover plaintext.

Definition: monoalphabetic

So far we've looked at one-alphabet, or *monoalphabetic*, ciphers, and we've seen how using alphabetic and nonalphabetic order affects complexity. In Figure 2-8, every plaintext `A` is replaced by ciphertext `Z`, every plaintext `B` is replaced by ciphertext `P`, and so on. Using a single alphabet to substitute letters in a message is not secure enough to stop a cryptanalyst.

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

EVERYONE MUST ATTACK BEFORE FIVE AM

HEHSDVOH YKJC ZCCZXF PHMVSH MREH ZY

Figure 2.8 A substitution cipher. The plaintext (normal) alphabet is on the top row; the cipher alphabet is on the bottom row.

Letter and Word Frequency

Facts about letter and word usage in languages have helped cryptologists encrypt and decrypt messages ever since Arab linguists started doing statistical analysis on Arabic languages more than a thousand years ago. Here's a look at letter and word frequency and letter combination statistics from the English language.

- *E* is the letter used most often, followed by *t*, *o*, *a*, and *n*.
- *T* is the most common letter at the beginning of a word. *E* is the most common letter at the end of a word.
- *A* and *I* are the only single-letter words in English. The words *of*, *to*, and *in* are the most frequent two-letter words; *the* and *and*, the most frequent three-letter words; *that*, the most frequent four-letter word.
- The most common double letters are *ll*, *ee*, *oo*, *tt*, *ff*, *rr*, *nn*, *pp*, and *cc*. *Th*, *he*, *an*, *re*, *er*, and *in* are the most frequent two-letter combinations. *The*, *ing*, *and*, *ion*, and *ent* are the most frequent three-letter combinations.
- *N* is the consonant that most often follows a vowel.

More Work, More Money

Edgar Allan Poe amazed nineteenth-century readers with his amateur facility in solving monoalphabetic ciphers. But he decided to focus on his more lucrative writing after winning a $100 prize for "The Gold-Bug," a story based on cryptography. Poe wrote to a friend that cracking ciphers took too much of his time.

Unlike Poe, the best cryptanalysts found cipher cracking lucrative. France's Antoine Rossignol and England's John Wallis, seventeenth-century cryptanalysts, could spend months cracking ciphers; but for such pros the time was well spent because those in power paid them well.

More Complex Substitution: Vigenére's Cipher

Confusing the cryptanalyst: a more complex encryption method and longer keys

Now let's look at a way to make the cryptanalyst do a lot more work. Cryptographers added complexity to Caesar's cipher, naming the method Vigenére's cipher for Blaise de Vigenére, a French cryptographer of the 1500s.

Everything's a Cipher

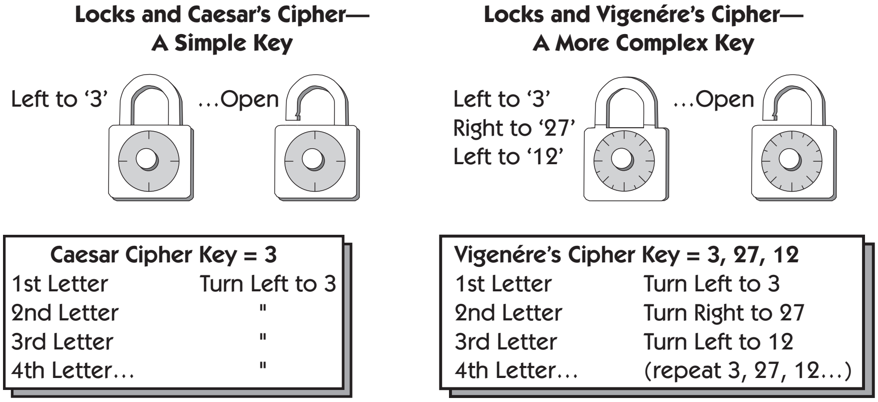
In 1586, Vigenére published a book in which he seemed to lump cryptography with everything. He wrote, "All nature is merely a cipher and a secret writing. The great name and essence of God and his wonders, the very deeds, projects, words, actions, and demeanor of mankind—what are they for the most part but a cipher?"

Like Caesar's cipher, Vigenére's method can be compared to a combination lock (see Figure 2-9). Caesar's cipher is like the lock on the left. The combination is a single number: Turn left to 3, and the lock opens. It was a breakthrough in security—2,500 years ago. Vigenére's cipher, on the other hand, is like the lock on the right; the combination is more complex. It was a breakthrough in security 400 years ago. (It's instructive to see how Vigenére confuses the cryptanalyst, but don't get bogged down trying to understand the details. Instead, focus on how Vigenére enhanced Caesar's method, as explained in a moment. Although substitution is a key tool in modern cryptographic methods, both Caesar's and Vigenére's ciphers are obsolete and insecure.)

Figure 2-10 shows how Vigenére used a longer key and many alphabets to confuse the relationship between ciphertext and the secret key. In our example, the secret key first transforms an `E` to an `F`, and then it transforms an `E` to an `M`!

Definition:
polyalphabetic

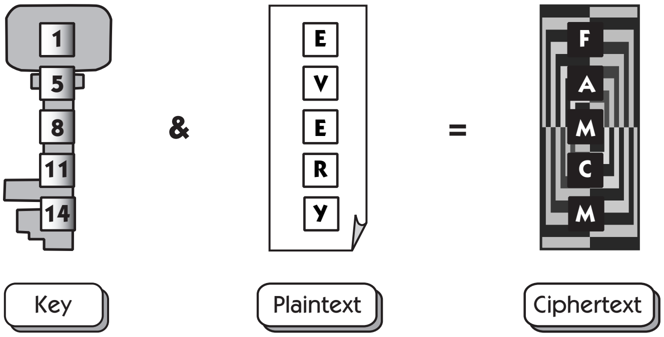
The Vigenére cipher looks like Caesar's cipher, but instead of one cipher alphabet, there are 26—a *polyalphabetic* cipher. This kind of cipher adds a twist to Caesar's cipher, and that makes the disguise more effective. The *key length*, combined with all the cipher alphabets, makes this system much better at hiding meaning than Caesar's cipher.



Caesar Cipher Key = 3	
1st Letter	Turn Left to 3
2nd Letter	"
3rd Letter	"
4th Letter...	"

Vigenére's Cipher Key = 3, 27, 12	
1st Letter	Turn Left to 3
2nd Letter	Turn Right to 27
3rd Letter	Turn Left to 12
4th Letter...	(repeat 3, 27, 12...)

Figure 2-9 Comparing the Caesar and Vigenére methods.



	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	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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 2-10 The Vigenére cipher is a polyalphabetic cipher.

At the top of the Vigenére table is the plaintext alphabet in alphabetical order. Along the side are numbers, and any combination of those numbers could be the key. For our example, we've picked 1-5-8-11-14 as the key.

Suppose an early seventeenth-century Alice wants to send Bob the encrypted message `EVERY ONE UP AT FIVE AM`. Let's encrypt plaintext `EVERY` to ciphertext `FAMCM`. Notice that the first alphabet at key 0 in the Vigenére table in Figure 2-10 is the same as the plaintext alphabet at the top of the table. So just as in Caesar's cipher, key 0 does not disguise the message.

Confuse the relationship between plaintext and secret key.

Using 1, the first number in the key 1-5-8-11-14, plaintext `E` encrypts to ciphertext `F`. If you follow `E` along the top of the table to its intersection with row 1 along the side of the table, you'll find the cipher letter `F`.

The next number in the key is 5, and the next letter to encrypt is `V`. Plaintext `V` encrypts to ciphertext `A`—the intersection of `V` along the top of the table with row 5 along the side.

The word `EVERY` in our message now contains a second `E`. Here's where this system is much better than Caesar's cipher. Can you see that this more complex key combined with multiple alphabets allows the second `E` in our message to be encrypted differently from the first `E`? This is an important advance because it makes the encrypted message resistant to statistical analysis (e.g., identifying the most commonly used letters such as `E` and `T`).

Following this pattern, you should be able to look at the table now and easily understand how `R` and `Y` must be encrypted. Because the key contains only five numbers, 1-5-8-11-14 is used again and again to encrypt each five-letter chunk of plaintext.

The entire message, `EVERY ONE UP AT FIVE AM`, encrypts to `FAMCM PSK FD BY NTJF FU`—if we got it right. It's easy for humans to make enciphering errors, even using an encryption table. Although cryptanalysis of a Vigenére's cipher is a tough problem for most people, it's easy for a well-designed computer program.

Adding key length causes a little more work encrypting plaintext, but it makes the cryptanalyst do much more work.

In public key cryptography, key lengths grow to 200 or more digits. How big a number is that? Try picturing all the atoms in the known universe. Well, that's not enough because there are many fewer atoms in the universe than "1 followed by 100 zeroes." If you can't imagine how big a 200-digit number is, imagine how such a number complicates the task of determined cryptanalysts. That's the idea behind long keys.

Vigenére's cipher is just like Caesar's cipher in that the method is public knowledge but the key is secret. Vigenére's method was a major conceptual breakthrough because identical plaintext letters seldom encrypt to the identical ciphertext letters. Although your adversary can have a copy of the table you and your confidant use to encrypt and decrypt messages, it still takes a long time to decrypt the ciphertext without the secret key. Vigenére's cipher disguises simple linguistic patterns.

Methods, Keys, and Error

Look what happens when the method is not secure and there are not enough keys. For hundreds of years, the Vigenére cipher created in the 1500s was mistakenly thought by some people to be invincible. During the U.S. Civil War in the 1860s , the Confederate Army was among those that invested too much trust in this legend. Confederate cryptographers used a Vigenére cipher, usually combined with three keys. Mistakes were frequent, and having to turn the cipher into Morse code added to the difficulty. As a result, telegraph transmission sometimes was so troublesome that Southern soldiers would gallop over to the sender to get the message firsthand.

Dutch cryptologist Auguste Kerckhoffs—the first to distinguish between the cryptographic method and the specific key used with it—would not have approved of the South's method and keys. In 1883 Kerckhoffs wrote that wartime cryptography needed to be efficient, portable, and easy to understand. It should also have a key that was easy to change and should lend itself to telegraphic transmission, Kerckhoffs argued.

Review

Caesar's cipher uses a simple cryptographic method (lock): Substitute each letter in the message with a letter from a ciphered alphabet. The key determines which ciphered alphabet to use for this monoalphabetic substitution. Cryptanalysis of this centuries-old substitution method is simple and can be done more than one way. For example, because there are only 25 possible keys, an adversary can try each one until something emerges that looks like a message. Another approach, frequency analysis, is to look for the most frequently appearing letter; in English, that letter is *e*.

Other substitution ciphers, such as the Vigenére cipher, are polyalphabetic and use a similar lock and key. The lock is the Vigenére cipher table. Even assuming that an adversary has the same Vigenére table used to encrypt the message, the message's key provides secrecy—if it is not discovered. The use of many possible keys forces the cryptanalyst to work much longer and makes statistical frequency analysis more difficult. This approach is like a lock that requires the user to correctly turn to three numbers in a certain order, making it more difficult than a combination of only one number.

Statistical analysis is a snap for a computer-toting cryptanalyst. By the same token, however, the computer also allows cryptographers to deeply bury the linguistic patterns that help cryptanalysts uncover meaning.