9 Cryptology

Mathematicians are like Frenchmen: whatever you say to them they translate into their own language and forthwith it is something entirely different.

— GOETHE

The great English number theorist Godfrey H. Hardy apparently believed that number theory had no practical applications. In his book *A Mathematician's Apology*, Hardy wrote that Theorem 2.10, which established the infinitude of primes, had only the slightest practical importance. Despite his opinion, ingenious mathematicians over the years, as we saw in Chapter 5, have discovered many practical as well as interesting applications of number theory.

We will now study several useful and charming applications that show that despite Hardy's conservative judgment, human creativity can turn virtually every aspect of mathematical knowledge to some practical use.

One exciting application of number theory is *cryptology*, the study of secrecy systems, which can be traced back to the early Egyptians. A powerful tool in military and diplomatic circles for centuries, cryptology has become an indispensable tool in commerce as well. Governments often want to keep policy decisions secret until an appropriate time; multinational corporations protect proprietary research and development, and marketing strategies.

In 1917, at the height of World War I, Germany cabled the Mexican government that it would commence submarine warfare, and promised Arizona, New Mexico, and Texas to Mexico if it would join the Axis against the United States, if the United States entered the war. The cable was intercepted, the code broken by British intelligence, the message passed on to President Woodrow Wilson, and the rest is history.

***Godfrey Harold Hardy** (1877–1947), an eminent English number theorist, was born in Cranleigh, England. Even as a child, he showed a precocious interest in mathematics. At the age of thirteen, he left Cranleigh School where his father was a master, and moved to Winchester College. In 1896, he entered Trinity College, Cambridge, and was elected a fellow four years later. Ten years later, Hardy became a lecturer at Cambridge University, a position he held until 1919. He plunged into research, wrote many papers in analysis, and completed his well-known book* A Course of Pure Mathematics *(1908). The text, designed for undergraduates, provided the first rigorous exposition of analysis, and transformed mathematics teaching forever.*

In 1919, Hardy left Cambridge to become Savilian professor of geometry at Oxford University, where also he was an active researcher. He was succeeded at Cambridge by John E. Littlewood (1885–1977). Eleven years later, Hardy returned to Cambridge, where he remained until his retirement in 1942. They had the most remarkable and productive partnership in the history of mathematics; they coauthored about 100 papers.

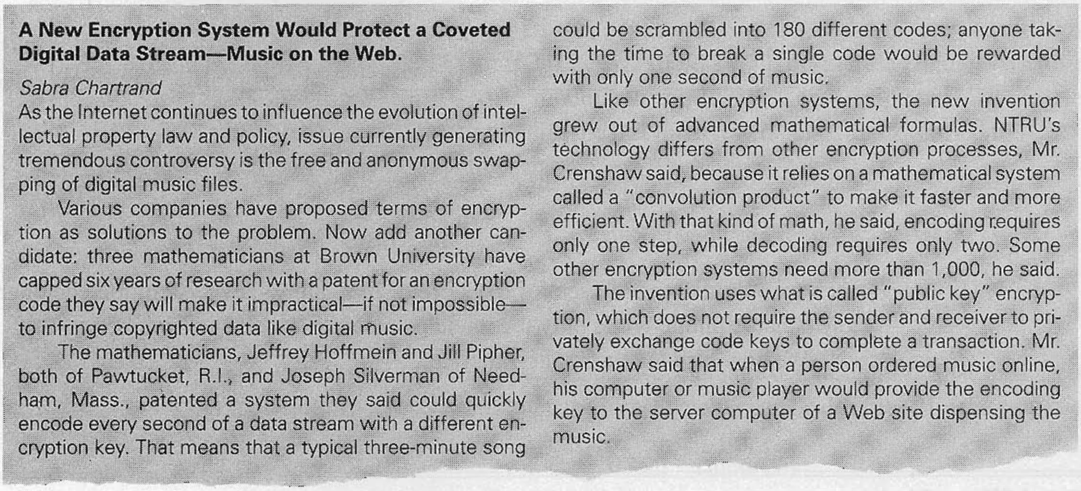
Hardy's most spectacular contribution to the mathematical community is generally considered to be his 1913 discovery of the unsophisticated Indian mathematical genius Srinivasa Ramanujan (1887–1920), whom Hardy brought to England in April, 1914. Their relentless collaboration produced many spectacular discoveries.

Today, electronic banking and computer data banks commonly use encryption for secrecy and security. In 1984 R. Sedgewick of the University of Illinois noted that "a computer user wants to keep his computer files just as private as papers in his file cabinet, and a bank wants electronic funds transfer to be just as secure as funds transfer by armored car."

Recent developments in computer technology and sophisticated techniques in cryptology have revolutionized information security, protecting secret communications over insecure channels such as telephone lines and microwaves from being accessed by unauthorized users. See Figure 9.1.

Cryptography and Cryptanalysis

Cryptology consists of *cryptography* and *cryptanalysis*. The word *cryptography* is derived from the Greek words *kryptos*, meaning *hidden* and *graphein*, meaning *to write*. **Cryptography** is the art and science of concealing the meaning of confidential communications from all except the intended recipients. **Cryptanalysis** deals with breaking secret messages. During World War II, 30,000 people were engaged in cryptographic work. The breaking of Japan's Purple machine code by U.S. cryptanalysts shortly before the attack on Pearl Harbor led to the Allied victory in the Pacific. Today the U.S. government and business employ tens of thousands of people and spend billions annually on cryptology.



A New Encryption System Would Protect a Coveted Digital Data Stream—Music on the Web.

Sabra Chartrand

As the Internet continues to influence the evolution of intellectual property law and policy, issue currently generating tremendous controversy is the free and anonymous swapping of digital music files.

Various companies have proposed terms of encryption as solutions to the problem. Now add another candidate: three mathematicians at Brown University have capped six years of research with a patent for an encryption code they say will make it impractical—if not impossible—to infringe copyrighted data like digital music.

The mathematicians, Jeffrey Hoffmein and Jill Pipher, both of Pawtucket, R.I., and Joseph Silverman of Needham, Mass., patented a system they said could quickly encode every second of a data stream with a different encryption key. That means that a typical three-minute song could be scrambled into 180 different codes; anyone taking the time to break a single code would be rewarded with only one second of music.

Like other encryption systems, the new invention grew out of advanced mathematical formulas. NTRU's technology differs from other encryption processes, Mr. Crenshaw said, because it relies on a mathematical system called a "convolution product" to make it faster and more efficient. With that kind of math, he said, encoding requires only one step, while decoding requires only two. Some other encryption systems need more than 1,000, he said.

The invention uses what is called "public key" encryption, which does not require the sender and receiver to privately exchange code keys to complete a transaction. Mr. Crenshaw said that when a person ordered music online, his computer or music player would provide the encoding key to the server computer of a Web site dispensing the music.

Figure 9.1

Cryptography is, by no means, the exclusive domain of professionals. Franklin Delano Roosevelt, when he was 21, used a simple code in his diary. American poet Edgar Allan Poe, who was a skilled cryptanalyst, wrote that human ingenuity could invent no unbreakable code that human ingenuity could not crack. Section 9.4, however, will prove otherwise.

Before we turn to some number-theoretic secrecy systems, we must define our terminology. **Plaintext** is the original message that is to be transmitted in secret form. **Ciphertext** is its secret version. A **cipher** is a method of translating a plaintext to ciphertext. The **key** is an explicit formulation of the cipher, so the job of the cryptanalyst is to discover the key and then break the code. The process of converting a plaintext to ciphertext is **enciphering** (or **encrypting**) and the converting device the **encryptor**. The reverse process by the intended recipient who knows the key is **deciphering** (or **decrypting**) and it is accomplished by a **decryptor**. The encryptor and decryptor may be algorithms executed by people or computers. Thus the method used by an unintended receiver to recover the original message is **cryptanalysis**. A **cryptosystem** is a system for encrypting a plaintext to a ciphertext using a key.

This chapter presents five cryptosystems—affine, Hill, exponentiation, RSA, and knapsack—based on modular arithmetic. The first three are **conventional** and the last two are **public-key**. In a **conventional cryptosystem**, pictured in Figure 9.2, the encryption key, from which the decrytion key can be found fairly quickly, is kept

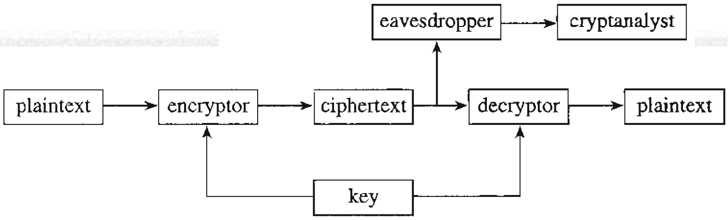


Figure 9.2

secret from unintended users of the system. In a public-key system the enciphering key is made public while only the intended receiver knows the deciphering key.

We now turn to our first cryptosystem.

9.1 Affine Ciphers

We will restrict our discussion to plaintext messages written in capital letters of the English alphabet, and ignore blank spaces and punctuation marks. In all cryptosystems we first translate each letter to a number. A convenient way of doing this is by numbering the letters A through Z by their **ordinal numbers** 00 through 25, respectively, as Table 9.1 shows. Using this scheme, we translate the the plaintext into a numeric message which is then enciphered into a numeric ciphertext. Each number is then replaced by a letter. The recipient of the ciphertext substitutes the ordinal number for each letter and uses the key to decipher the numeric message by substituting letters for the various numbers.

Letter	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
Ordinal Number	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 9.1

Substitution Ciphers

In a **substitution cipher**, we substitute a letter of the alphabet for each letter of the plaintext. It is, in fact, a **permutation cipher**, since each substitution is a permutation of the letters of the alphabet. Since there are 26! permutations of the letters, there is a total of 26! possible substitution ciphers; one of them is the trivial one, where each letter is substituted for itself.

Caesar Cipher

Around 50 B.C. the Roman emperor Julius Caesar (100–44 B.C.) sent encoded messages to his general Marcus T. Cicero (106–43 B.C.) during the Gallic Wars, using a substitution cipher based on modular arithmetic. A **Caesar cipher** shifts each letter by three places to the right, with the last three letters X, Y, and Z shifted to A, B, and C respectively in a cyclic fashion:

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

Let P denote the ordinal number of a plaintext letter and C that of the corresponding ciphertext letter. Then the Caesar cipher can be described by the congruence

$$C \equiv P + 3 \pmod{26} \qquad (1)$$

where $0 \leq P, C \leq 25$.

Ciphertext is often grouped into blocks of five letters to prevent short words from being quickly recognized by cryptanalysts. The following example illustrates the Caesar enciphering algorithm.

EXAMPLE 9.1 Encipher the message HAVE A NICE DAY using the Caesar key.

SOLUTION

step 1 *Using Table 9.1 replace each letter by its ordinal number.*

07 00 21 04 00 13 08 02 04 03 00 24

step 2 *Apply the Caesar transformation* $C \equiv P + 3 \pmod{26}$. The resulting numbers are 10 03 24 07 03 16 11 05 07 06 03 01. For example, when $P = 24$, $C \equiv 24 + 3 \equiv 01 \pmod{26}$.

step 3 *Substitute the letter corresponding to each ordinal number and group them in blocks of five.* The resulting ciphertext message KDYHD QLFHG DB. ■

To decipher such a ciphertext, the recipient simply reverses the steps. From the congruence $C \equiv P + 3 \pmod{26}$, we have the deciphering formula $P \equiv C - 3 \pmod{26}$ which enables us to recover the original plaintext, as the following example demonstrates.

EXAMPLE 9.2 Decipher the ciphertext KDYHD QLFHG DB in Example 9.1.

SOLUTION

step 1 *Using Table 9.1 replace each number with its ordinal number:*

10 03 24 07 03 16 11 05 07 06 03 01

step 2 *Use the deciphering formula* $P \equiv C - 3 \pmod{26}$ *to retrieve the numeric plaintext.* The resulting numeric string is

07 00 21 04 00 13 08 02 04 03 00 24

step 3 *Translate these numbers back to the alphabetic format.* This yields HAVEA NICED AY.

step 4 *Regroup the letters to recover the original message: HAVE A NICE DAY.*

■

Shift Ciphers

Clearly there is nothing sacred about the choice of the **shift factor** 3 in the Caesar cipher. It is one possible choice out of all the **shift ciphers** $C \equiv P + k \pmod{26}$, where k is the shift factor and $0 \leq k \leq 25$. There are 26 possible shift ciphers, one of which is $C \equiv P \pmod{26}$; that is, $C = P$.

A shift cipher is a substitution cipher. By substituting one letter for another, a cryptanalyst can crack a code by using the universally available knowledge of the relative frequency distribution of letters in ordinary text. The most frequently occurring letters in the ciphertext correspond to those in the plaintext. For example, E is the most frequently occurring letter in an arbitrary text, occurring about 12.5% of the time; the next three letters are T, A, and O occurring about 9, 8, and 8% of the time, respectively. Table 9.2 shows the relative frequencies of the various letters in the English alphabet.

The following example illustrates how this table can be used in crytanalysis. However, for short and selective messages the percentages might not be helpful. Consider, for instance, the following well-known passage from President

Letter	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
Relative Frequency in %	8	1.5	3	4	12.5	2	2	5.5	7	.1	.7	4	2.5	7	8	2	.1	6	6.5	9	3	1	2	.2	2	.1

Table 9.2

John F. Kennedy's inaugural address in 1961: ASK NOT WHAT YOUR COUNTRY CAN DO FOR YOU, ASK WHAT YOU CAN DO FOR YOUR COUNTRY. This sentence does not contain a single E, and the most frequent letter in it is O.

EXAMPLE 9.3 Assuming that the following ciphertext was created by the shift cipher $C \equiv P + k$ (mod 26), decipher it:

SLABZ ULCLY ULNVA PHALV BAVMM LHYIB
ASLAB ZULCL YMLHY AVULN VAPHA L

SOLUTION

The given ciphertext can be cracked if we can determine the value of k. To this end, first we construct a frequency table for the letters in the ciphertext, as in Table 9.3. The most frequently occurring letter in the cipher text is L, so our best guess is that it must correspond to the plaintext letter E. Since their ordinal numbers are 11 and 4, this implies $11 \equiv 4 + k$ (mod 26); that is, $k = 7$. Then $C \equiv P + 7$ (mod 26), so $P \equiv C - 7$ (mod 26). Using this congruence, we can now determine the ordinal number of each letter in the plaintext, as Table 9.4 shows. It follows from the table that the plaintext, after regrouping the blocks, is LET US NEVER NEGOTIATE OUT OF FEAR BUT LET US NEVER FEAR TO NEGOTIATE, another passage from President Kennedy's inaugural address.

Letter	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
Frequency	6	4	2	0	0	0	0	2	1	0	0	9	2	1	0	1	0	0	2	0	3	3	0	0	2	2

Table 9.3

Ciphertext Letter	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
	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Plaintext Letter	19	20	21	22	23	24	25	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18
	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

Table 9.4 ■

In Example 9.3, our initial guess did in fact produce an intelligent message. On the other hand, if it had resulted in gobbledygook, then we would continue the preceding procedure with the next frequently occurring letters until we succeeded.

Affine Ciphers

Shift ciphers belong to a large family of **affine ciphers** defined by the formula

$$C \equiv aP + k \pmod{26} \qquad (2)$$

where a is a positive integer ≤ 25 and $(a, 26) = 1$.

The condition that $(a, 26) = 1$ guarantees that as P runs through the least residues modulo 26, so does C; it also ensures that congruence (2) has a unique solution for P, by Corollary 4.8:

$$P \equiv a^{-1}(C - k) \pmod{26} \qquad (3)$$

Since $(a, 26) = 1$, there are $\varphi(26) = 12$ choices for a, so there are $12 \cdot 26 = 312$ affine ciphers. One of them is the identity transformation $C \equiv P \pmod{26}$, corresponding to $a = 1$ and $k = 0$.

When $a = 5$ and $k = 11$, $C \equiv 5P + 11 \pmod{26}$. If $P = 8$, then $C \equiv 5 \cdot 8 + 11 \equiv 25 \pmod{26}$, so under the affine cipher $C \equiv 5P + 11 \pmod{26}$, the letter I is transformed into Z and the letter Q into N. Table 9.5 shows the plaintext letters and the corresponding ciphertext letters created by this affine cipher which shifts A to L and in which each successive letter is paired with every fifth letter.

Plaintext Letter	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
	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Ciphertext Letter	11	16	21	00	05	10	15	20	25	04	09	14	19	24	03	08	13	18	23	02	07	12	17	22	01	06
	L	Q	V	A	F	K	P	U	Z	E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B	G

Table 9.5

The following example illustrates the encrypting procedure for this affine cipher.

EXAMPLE 9.4 Use the affine cipher $C \equiv 5P + 11 \pmod{26}$ to encipher the message THE MOON IS MADE OF CREAM CHEESE.

SOLUTION

Since most of the work has been done in Table 9.5, we group the letters into blocks of length five:

THEMO ONISM ADEOF CREAM CHEES E

Then replace each letter by the corresponding ciphertext letter in the table. The resulting encrypted message is CUFTD DYZXT LAFDK VSFLT VUFFX F. ■

The following example demonstrates how to decrypt a message generated by an affine cipher.

EXAMPLE 9.5 Decipher the ciphertext message OZKFZ XPDDA created by the affine cipher $C \equiv 5P + 11 \pmod{26}$.

SOLUTION

Since $C \equiv 5P + 11 \pmod{26}$, $P \equiv 5^{-1}(C - 11) \equiv 21(C - 11) \equiv 21C + 3 \pmod{26}$. For example, when $C = 14$, $P \equiv 21 \cdot 14 + 3 \equiv 11 \pmod{26}$. Thus the ciphertext letter O is decrypted as L. The other letters can be deciphered in a similar fashion. (We could use Table 9.5 in the reverse order.) This yields the message LIFEI SGOOD. Reassembling the blocks, we find that the original plaintext is LIFE IS GOOD. ■

If a cryptanalyst knows that the enciphered message was generated by an affine cipher, then he or she will be able to break the cipher using the frequency counts of letters in Table 9.2, as the following example shows.

EXAMPLE 9.6 Cryptanalyze the ciphertext BYTUH NCGKN DUBIH UVNYX HUTYP QNGYV IVROH GSU that was generated by an affine cipher.

SOLUTION

Assume the cipher we are searching for is $C \equiv aP + k \pmod{26}$. To make an educated guess which are the most frequently occurring letters in the plaintext, construct a frequency table of letters in the ciphertext, as Table 9.6 shows. According to the table, the most commonly occurring letter in the ciphertext is U, so it is reasonable to assume that it corresponds to the plaintext letter E; that is, $20 \equiv 4a + k \pmod{26}$. Now there are three choices for the next most commonly occurring letter, namely, H, N, and Y. If we assume H corresponds to T, then $7 \equiv 19a + k \pmod{26}$. Thus we have

$$4a + k \equiv 20 \pmod{26}$$
$$19a + k \equiv 7 \pmod{26}$$

Ciphertext Letter	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
Frequency	0	2	1	1	0	0	3	4	1	0	1	1	0	4	1	1	1	1	1	2	5	3	0	1	4	0

Table 9.6

Solving this linear system, $a \equiv 13 \pmod{26}$ and $k \equiv 20 \pmod{26}$, so $C \equiv 13P+20 \pmod{26}$. But $(13, 26) \neq 1$, so this is not a valid cipher. Thus our guess that H corresponds to T was not a valid one.

So let us assume that N corresponds to T. This yields the linear system

$$4a + k \equiv 20 \pmod{26}$$
$$19a + k \equiv 13 \pmod{26}$$

Solving this system, $a \equiv 3 \pmod{26}$ and $k \equiv 8 \pmod{26}$. Since $(3, 26) = 1$, this yields a valid cipher $C \equiv 3P + 8 \pmod{26}$. Then $P \equiv 3^{-1}(C - 8) \equiv 9(C - 8) \equiv 9C + 6 \pmod{26}$.

Using this deciphering formula, next we construct Table 9.7, which displays the plaintext letters corresponding to the ciphertext ones. Using the table, we can translate given encryptic message as POVER TYIST HEPAR ENTOF REVOL UTION ANDCR IME, that is, POVERTY IS THE PARENT OF REVOLUTION AND CRIME, a statement made by the Greek philosopher Aristotle. (It would be interesting to check if the third choice leads to an intelligent plaintext message.)

Ciphertext Letter	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
	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Plaintext Letter	06	15	24	07	16	25	08	17	00	09	18	01	10	19	02	11	20	03	12	21	04	13	22	05	14	23
	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X
										↑													↑			

Table 9.7 ■

An interesting bonus: It follows from Table 9.7 that the plaintext letters J and W are not affected by the transformation $C \equiv 3P + 8 \pmod{26}$. They are said to be left **fixed** by the cipher. See Exercises 15–18 also.

By and large, a ciphertext generated by an affine cipher does not provide adequate security. One way to make breaking complicated is by using a finite sequence of affine ciphers $C \equiv a_iP + k_i \pmod{26}$, as Figure 9.3 shows, where $1 \leq i \leq n$. Such a cipher is the **product** (or **composition**) of the n ciphers. Exercises 22–25 further explore such ciphers.

Another option is to use the enciphering scheme developed by the French cryptographer B. de Vigenère in 1586. The Vigenère cryptosystem employs a **keyword**

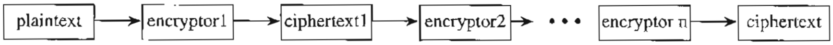


Figure 9.3

$w_1w_2\dots w_n$ of length n and n shift ciphers $C \equiv P_i + k_i \pmod{26}$ to each plaintext block of length n, where k_i is the ordinal number of the letter w_i and $1 \le i \le n$.

The following example illustrates Vigenère encrypting.

EXAMPLE 9.7 Using the keyword CIPHER and a Vigenère cipher, encrypt the message CRYPTOGRAPHY IS FUN.

SOLUTION

Since the ordinal numbers of the letters C, I, P, H, E, and R in the word CIPHER are 02, 08, 15, 07, 04, and 17, respectively, they serve as the shift factors for each shift cipher for every block. So the six shift ciphers are $C \equiv P + k \pmod{26}$, where $k = 2, 8, 15, 7, 4,$ and 17.

Since the keyword is a six-letter word, first we group the letters of the plaintext into blocks of length six: CRYPTO GRAPHY ISFUN.

Now apply the ith cipher to the letter w_i in each block, where $1 \le i \le n$. For instance, consider the first block CRYPTO. Since the ordinal numbers of its letters are 02, 17, 24, 15, 19, and 14, respectively, add to them the key values 2, 8, 15, 7, 4, and 17 in that order modulo 26. The resulting numbers are 4, 25, 13, 22, 23, and 5, and the corresponding letters are E, Z, N, W, X, and F, respectively, so the first ciphertext block is EZNWXF. The other two blocks are similarly transformed to IZPWLT and IAUBU, as Table 9.8 shows. Thus the resulting ciphertext is EZNWXF IZPWLT IAUBU.

Plaintext Block	C	R	Y	P	T	O	G	R	A	P	H	Y	I	S	F	U	N
	02	17	24	15	19	14	06	17	00	15	07	24	08	18	05	20	13
Ciphertext Block	04	25	13	22	23	05	08	25	15	22	11	19	04	00	20	01	20
	E	Z	N	W	X	F	I	Z	P	W	L	T	I	A	U	B	U

Table 9.8

■

It is important to remember that an affine cipher substitutes the very same letter C for each occurrence of the plaintext letter P, whereas a Vigenère cipher need not. A Vigenère cipher may substitute the same letter C for different plaintext letters. For instance, in the preceding example the plaintext letters G and I are enciphered into I, as are F and N into U. This makes both encrypting and decrypting in Vigenère more difficult. The two R's are transformed into Z because they occupy the same spot in their respective blocks.

EXERCISES 9.1

Using the Caesar cipher, encipher each proverb.

1. ALL IS WELL THAT ENDS WELL.
2. ALL THAT GLITTERS IS NOT GOLD.

Decipher each ciphertext created by the Caesar cipher.

3. QHFHV VLWBL VWKHP RWKHU RILQY HQWLR Q.
4. PDWKH PDWLF VLVWK HTXHH QRIWK HVFLH QFHV.

Enciphereach quotation using the shift cipher $C \equiv P + 11 \pmod{26}$.

5. NO LEGACY IS SO GREAT AS HONESTY. (W. Shakespeare)
6. THERE IS NO ROYAL ROAD TO GEOMETRY. (Euclid)

Decrypt each quotation below encrypted by the shift cipher $C \equiv P + k \pmod{26}$.

7. GVZRV FGURO RFGZR QVPVA R.
8. NSOZX YNHJF SDBMJ WJNXF YMWJF YYTOZ XYNHJ JAJWD BMJWJ.

Encipher each using the affine cipher $C \equiv 3P + 7 \pmod{26}$.

9. A THING OF BEAUTY IS A JOY FOR EVER. (John Keats)
10. A JOURNEY OF A THOUSAND MILES MUST BEGIN WITH A SINGLE STEP. (Lao-Tzu)

11–12. Encrypt the messages in Exercises 9 and 10 using the cipher $C \equiv 7P + 10 \pmod{26}$.

The enciphered messages in Exercises 13 and 14 were generated by the affine cipher $C \equiv 5P + 3 \pmod{26}$. Decipher each.

13. UMXIZ NBPUV APMXK X.
14. XEXKT IVSTP IZPRQ XPPRP QVIVS TPIZP RQXPP.

A plaintext letter is left **fixed** by a cipher if it remains the same in the ciphertext generated by the cipher. Find the letters left fixed by each affine cipher.

15. $C \equiv 5P + 11 \pmod{26}$
16. $C \equiv 7P + 13 \pmod{26}$
17. $C \equiv 5P + 14 \pmod{26}$
18. $C \equiv 9P + 18 \pmod{26}$

Cryptanalyze each ciphertext created by an affine cipher $C \equiv aP + k \pmod{26}$.

19. IRCCH EKKEV CLLFK EIOKL XKKLF ILIGM EKOIV EKKE.
20. KARRH HRSLR VUXER FKSRH HDHKA RYREL RYKDV SKAFK QDEKN RDHRS VNXA.
21. Find the total number of affine ciphers possible.

Encipher the message, SEND MORE MONEY, using the product of the given affine ciphers.

22. $C \equiv 3P + 7 \pmod{26}$, $C \equiv 5P + 8 \pmod{26}$
23. $C \equiv 5P + 7 \pmod{26}$, $C \equiv 7P + 5 \pmod{26}$

Cryptanalyze each ciphertext generated by the product of two affine ciphers. (*Hint:* The product of two affine ciphers is also an affine cipher.)

24. GIPJU QDHQG PCUHG XKPGJ LJPOX RGPUL PXRLJ APRGC VLGXJ U.
25. ZLFYL FCZFP TBLOO RSBYL FQPON CRELA JOSLE LYCRE RSB.

Encrypt each message using the keyword CIPHER for a Vinegère cipher.

26. SEND MORE MONEY.
27. MATHEMATICS IS THE DOOR AND THE KEY TO THE SCIENCES.

Decrypt each ciphertext generated by a Vinegère cipher using the keyword MATH.

28. TETS FHBZ IETS FH.
29. XIYL IOGA IABA.