

## 4.6 Cryptography

### Introduction

Number theory plays a key role in cryptography, the subject of transforming information so that it cannot be easily recovered without special knowledge. Number theory is the basis of many classical ciphers, first used thousands of years ago, and used extensively until the 20th century. These ciphers encrypt messages by changing each letter to a different letter, or each block of letters to a different block of letters. We will discuss some classical ciphers, including shift ciphers, which replace each letter by the letter a fixed number of positions later in the alphabet, wrapping around to the beginning of the alphabet when necessary. The classical ciphers we will discuss are examples of private key ciphers where knowing how to encrypt allows someone to also decrypt messages. With a private key cipher, two parties who wish to communicate in secret must share a secret key. The classical ciphers we will discuss are also vulnerable to cryptanalysis, which seeks to recover encrypted information without access to the secret information used to encrypt the message. We will show how to cryptanalyze messages sent using shift ciphers.

Number theory is also important in public key cryptography, a type of cryptography invented in the 1970s. In public key cryptography, knowing how to encrypt does not also tell someone how to decrypt. The most widely used public key system, called the RSA cryptosystem, encrypts messages using modular exponentiation, where the modulus is the product of two large primes. Knowing how to encrypt requires that someone know the modulus and an exponent. (It does not require that the two prime factors of the modulus be known.) As far as it is known, knowing how to decrypt requires someone to know how to invert the encryption function, which can only be done in a practical amount of time when someone knows these two large prime factors. In this chapter we will explain how the RSA cryptosystem works, including how to encrypt and decrypt messages.

The subject of cryptography also includes the subject of cryptographic protocols, which are exchanges of messages carried out by two or more parties to achieve a specific security goal. We will discuss two important protocols in this chapter. One allows two people to share a common secret key. The other can be used to send signed messages so that a recipient can be sure that they were sent by the purported sender.

### Classical Cryptography

One of the earliest known uses of cryptography was by Julius Caesar. He made messages secret by shifting each letter three letters forward in the alphabet (sending the last three letters of the alphabet to the first three). For instance, using this scheme the letter B is sent to E and the letter X is sent to A. This is an example of **encryption**, that is, the process of making a message secret.

To express Caesar's encryption process mathematically, first replace each letter by an element of  $\mathbf{Z}_{26}$ , that is, an integer from 0 to 25 equal to one less than its position in the alphabet. For example, replace A by 0, K by 10, and Z by 25. Caesar's encryption method can be represented by the function  $f$  that assigns to the nonnegative integer  $p$ ,  $p \leq 25$ , the integer  $f(p)$  in the set  $\{0, 1, 2, \dots, 25\}$  with

$$f(p) = (p + 3) \bmod 26.$$

In the encrypted version of the message, the letter represented by  $p$  is replaced with the letter represented by  $(p + 3) \bmod 26$ .

**EXAMPLE 1** What is the secret message produced from the message “MEET YOU IN THE PARK” using the Caesar cipher?

*Solution:* First replace the letters in the message with numbers. This produces

12 4 4 19      24 14 20      8 13      19 7 4      15 0 17 10.

Now replace each of these numbers  $p$  by  $f(p) = (p + 3) \bmod 26$ . This gives

15 7 7 22      1 17 23      11 16      22 10 7      18 3 20 13.

Translating this back to letters produces the encrypted message “PHHW BRX LQ WKH SDUN.”

To recover the original message from a secret message encrypted by the Caesar cipher, the function  $f^{-1}$ , the inverse of  $f$ , is used. Note that the function  $f^{-1}$  sends an integer  $p$  from  $\mathbb{Z}_{26}$ , to  $f^{-1}(p) = (p - 3) \bmod 26$ . In other words, to find the original message, each letter is shifted back three letters in the alphabet, with the first three letters sent to the last three letters of the alphabet. The process of determining the original message from the encrypted message is called **decryption**.

There are various ways to generalize the Caesar cipher. For example, instead of shifting the numerical equivalent of each letter by 3, we can shift the numerical equivalent of each letter by  $k$ , so that

$$f(p) = (p + k) \bmod 26.$$

Such a cipher is called a *shift cipher*. Note that decryption can be carried out using

$$f^{-1}(p) = (p - k) \bmod 26.$$

Here the integer  $k$  is called a **key**. We illustrate the use of a shift cipher in Examples 2 and 3.

**EXAMPLE 2** Encrypt the plaintext message “STOP GLOBAL WARMING” using the shift cipher with shift  $k = 11$ .

*Solution:* To encrypt the message “STOP GLOBAL WARMING” we first translate each letter to the corresponding element of  $\mathbb{Z}_{26}$ . This produces the string

18 19 14 15      6 11 14 1 0 11      22 0 17 12 8 13 6.

We now apply the shift  $f(p) = (p + 11) \bmod 26$  to each number in this string. We obtain

3 4 25 0      17 22 25 12 11 22      7 11 2 23 19 24 17.

Translating this last string back to letters, we obtain the ciphertext “DEZA RWZMLW HLCX-TYR.”

**EXAMPLE 3** Decrypt the ciphertext message “LEWLYPLUJL PZ H NYLHA ALHJOLY” that was encrypted with the shift cipher with shift  $k = 7$ .

*Solution:* To decrypt the ciphertext “LEWLYPLUJL PZ H NYLHA ALHJOLY” we first translate the letters back to elements of  $\mathbb{Z}_{26}$ . We obtain

11 4 22 11 24 15 11 20 9 11      15 25      7      13 24 11 7 0      0 11 7 9 14 11 24.

Next, we shift each of these numbers by  $-k = -7$  modulo 26 to obtain

4 23 15 4 17 8 4 13 2 4      8 18      0      6 17 4 0 19      19 4 0 2 7 4 17.

Finally, we translate these numbers back to letters to obtain the plaintext. We obtain “EXPERIENCE IS A GREAT TEACHER.”

We can generalize shift ciphers further to slightly enhance security by using a function of the form

$$f(p) = (ap + b) \bmod 26,$$

where  $a$  and  $b$  are integers, chosen so that  $f$  is a bijection. (The function  $f(p) = (ap + b) \bmod 26$  is a bijection if and only if  $\gcd(a, 26) = 1$ .) Such a mapping is called an *affine transformation*, and the resulting cipher is called an *affine cipher*.

**EXAMPLE 4** What letter replaces the letter K when the function  $f(p) = (7p + 3) \bmod 26$  is used for encryption?

**Solution:** First, note that 10 represents K. Then, using the encryption function specified, it follows that  $f(10) = (7 \cdot 10 + 3) \bmod 26 = 21$ . Because 21 represents V, K is replaced by V in the encrypted message.


We will now show how to decrypt messages encrypted using an affine cipher. Suppose that  $c = (ap + b) \bmod 26$  with  $\gcd(a, 26) = 1$ . To decrypt we need to show how to express  $p$  in terms of  $c$ . To do this, we apply the encrypting congruence  $c \equiv ap + b \pmod{26}$ , and solve it for  $p$ . To do this, we first subtract  $b$  from both sides, to obtain  $c - b \equiv ap \pmod{26}$ . Because  $\gcd(a, 26) = 1$ , we know that there is an inverse  $\bar{a}$  of  $a$  modulo 26. Multiplying both sides of the last equation by  $\bar{a}$  gives us  $\bar{a}(c - b) \equiv \bar{a}ap \pmod{26}$ . Because  $\bar{a}a \equiv 1 \pmod{26}$ , this tells us that  $p \equiv \bar{a}(c - b) \pmod{26}$ . This determines  $p$  because  $p$  belongs to  $\mathbf{Z}_{26}$ .

**CRYPTANALYSIS** The process of recovering plaintext from ciphertext without knowledge of both the encryption method and the key is known as **cryptanalysis** or **breaking codes**. In general, cryptanalysis is a difficult process, especially when the encryption method is unknown. We will not discuss cryptanalysis in general, but we will explain how to break messages that were encrypted using a shift cipher.

If we know that a ciphertext message was produced by enciphering a message using a shift cipher, we can try to recover the message by shifting all characters of the ciphertext by each of the 26 possible shifts (including a shift of zero characters). One of these is guaranteed to be the plaintext. However, we can use a more intelligent approach, which we can build upon to cryptanalyze ciphertext resulting from other ciphers. The main tool for cryptanalyzing ciphertext encrypted using a shift cipher is the count of the frequency of letters in the ciphertext. The nine most common letters in English text and their approximate relative frequencies are E 13%, T 9%, A 8%, O 8%, I 7%, N 7%, S 7%, H 6%, and R 6%. To cryptanalyze ciphertext that we know was produced using a shift cipher, we first find the relative frequencies of letters in the ciphertext. We list the most common letters in the ciphertext in frequency order; we hypothesize that the most common letter in the ciphertext is produced by encrypting E. Then, we determine the value of the shift under this hypothesis, say  $k$ . If the message produced by shifting the ciphertext by  $-k$  makes sense, we presume that our hypothesis is correct and that we have the correct value of  $k$ . If it does not make sense, we next consider the hypothesis that the most common letter in the ciphertext is produced by encrypting T, the second most common letter in English; we find  $k$  under this hypothesis, shift the letters of the message by  $-k$ , and see whether the resulting message makes sense. If it does not, we continue the process working our way through the letters from most common to least common.

Mathematicians make the best code breakers. Their work in World War II changed the course of the war.

**EXAMPLE 5** Suppose that we intercepted the ciphertext message ZNK KGXRE HOXJ MKZY ZNK CUXS that we know was produced by a shift cipher. What was the original plaintext message?

**Solution:** Because we know that the intercepted ciphertext message was encrypted using a shift cipher, we begin by calculating the frequency of letters in the ciphertext. We find that the most common letter in the ciphertext is K. So, we hypothesize that the shift cipher sent the plaintext letter E to the ciphertext letter K. If this hypothesis is correct, we know that  $10 = 4 + k \bmod 26$ , so  $k = 6$ . Next, we shift the letters of the message by  $-6$ , obtaining THE EARLY BIRD GETS THE WORM. Because this message makes sense, we assume that the hypothesis that  $k = 6$  is correct. 



**BLOCK CIPHERS** Shift ciphers and affine ciphers proceed by replacing each letter of the alphabet by another letter in the alphabet. Because of this, these ciphers are called **character** or **monoalphabetic ciphers**. Encryption methods of this kind are vulnerable to attacks based on the analysis of letter frequency in the ciphertext, as we just illustrated. We can make it harder to successfully attack ciphertext by replacing blocks of letters with other blocks of letters instead of replacing individual characters with individual characters; such ciphers are called **block ciphers**.


We will now introduce a simple type of block cipher, called the **transposition cipher**. As a key we use a permutation  $\sigma$  of the set  $\{1, 2, \dots, m\}$  for some positive integer  $m$ , that is, a one-to-one function from  $\{1, 2, \dots, m\}$  to itself. To encrypt a message we first split its letters into blocks of size  $m$ . (If the number of letters in the message is not divisible by  $m$  we add some random letters at the end to fill out the final block.) We encrypt the block  $p_1 p_2 \dots p_m$  as  $c_1 c_2 \dots c_m = p_{\sigma(1)} p_{\sigma(2)} \dots p_{\sigma(m)}$ . To decrypt a ciphertext block  $c_1 c_2 \dots c_m$ , we transpose its letters using the permutation  $\sigma^{-1}$ , the inverse of  $\sigma$ . Example 6 illustrates encryption and decryption for a transposition cipher.

**EXAMPLE 6** Using the transposition cipher based on the permutation  $\sigma$  of the set  $\{1, 2, 3, 4\}$  with  $\sigma(1) = 3$ ,  $\sigma(2) = 1$ ,  $\sigma(3) = 4$ , and  $\sigma(4) = 2$ ,

(a) Encrypt the plaintext message PIRATE ATTACK.

(b) Decrypt the ciphertext message SWUE TRAE OEHS, which was encrypted using this cipher.

**Solution:** (a) We first split the letters of the plaintext into blocks of four letters. We obtain PIRATEAT TACK. To encrypt each block, we send the first letter to the third position, the second letter to the first position, the third letter to the fourth position, and the fourth letter to the second position. We obtain IAPR ETTA AKTC.

(b) We note that  $\sigma^{-1}$ , the inverse of  $\sigma$ , sends 1 to 2, sends 2 to 4, sends 3 to 1, and sends 4 to 3. Applying  $\sigma^{-1}(m)$  to each block gives us the plaintext: USEW ATER HOSE. (Grouping together these letters to form common words, we surmise that the plaintext is USE WATER HOSE.) 


**CRYPTOSYSTEMS** We have defined two families of ciphers: shift ciphers and affine ciphers. We now introduce the notion of a cryptosystem, which provides a general structure for defining new families of ciphers.

#### DEFINITION 1

A *cryptosystem* is a five-tuple  $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ , where  $\mathcal{P}$  is the set of plaintext strings,  $\mathcal{C}$  is the set of ciphertext strings,  $\mathcal{K}$  is the *keyspace* (the set of all possible keys),  $\mathcal{E}$  is the set of encryption functions, and  $\mathcal{D}$  is the set of decryption functions. We denote by  $E_k$  the encryption function in  $\mathcal{E}$  corresponding to the key  $k$  and  $D_k$  the decryption function in  $\mathcal{D}$  that decrypts ciphertext that was encrypted using  $E_k$ , that is  $D_k(E_k(p)) = p$ , for all plaintext strings  $p$ .

We now illustrate the use of the definition of a cryptosystem.

**EXAMPLE 7** Describe the family of shift ciphers as a cryptosystem.

*Solution:* To encrypt a string of English letters with a shift cipher, we first translate each letter to an integer between 0 and 25, that is, to an element of  $\mathbf{Z}_{26}$ . We then shift each of these integers by a fixed integer modulo 26, and finally, we translate the integers back to letters. To apply the definition of a cryptosystem to shift ciphers, we assume that our messages are already integers, that is, elements of  $\mathbf{Z}_{26}$ . That is, we assume that the translation between letters and integers is outside of the cryptosystem. Consequently, both the set of plaintext strings  $\mathcal{P}$  and the set of ciphertext strings  $\mathcal{C}$  are the set of strings of elements of  $\mathbf{Z}_{26}$ . The set of keys  $\mathcal{K}$  is the set of possible shifts, so  $\mathcal{K} = \mathbf{Z}_{26}$ . The set  $\mathcal{E}$  consists of functions of the form  $E_k(p) = (p + k) \bmod 26$ , and the set  $\mathcal{D}$  of decryption functions is the same as the set of encrypting functions where  $D_k(p) = (p - k) \bmod 26$ . 

The concept of a cryptosystem is useful in the discussion of additional families of ciphers and is used extensively in cryptography.

## Public Key Cryptography

All classical ciphers, including shift ciphers and affine ciphers, are examples of **private key cryptosystems**. In a private key cryptosystem, once you know an encryption key, you can quickly find the decryption key. So, knowing how to encrypt messages using a particular key allows you to decrypt messages that were encrypted using this key. For example, when a shift cipher is used with encryption key  $k$ , the plaintext integer  $p$  is sent to

$$c = (p + k) \bmod 26.$$

Decryption is carried out by shifting by  $-k$ ; that is,

$$p = (c - k) \bmod 26.$$

So knowing how to encrypt with a shift cipher also tells you how to decrypt.

When a private key cryptosystem is used, two parties who wish to communicate in secret must share a secret key. Because anyone who knows this key can both encrypt and decrypt messages, two people who want to communicate securely need to securely exchange this key. (We will introduce a method for doing this later in this section.) The shift cipher and affine cipher cryptosystems are private key cryptosystems. They are quite simple and are extremely vulnerable to cryptanalysis. However, the same is not true of many modern private key cryptosystems. In particular, the current US government standard for private key cryptography, the Advanced Encryption Standard (AES), is extremely complex and is considered to be highly resistant to cryptanalysis. (See [St06] for details on AES and other modern private key cryptosystems.) AES is widely used in government and commercial communications. However, it still shares the property that for secure communications keys be shared. Furthermore, for extra security, a new key is used for each communication session between two parties, which requires a method for generating keys and securely sharing them.

To avoid the need for keys to be shared by every pair of parties that wish to communicate securely, in the 1970s cryptologists introduced the concept of **public key cryptosystems**. When such cryptosystems are used, knowing how to send an encrypted message does not help decrypt messages. In such a system, everyone can have a publicly known encryption key. Only the decryption keys are kept secret, and only the intended recipient of a message can decrypt it, because, as far as it is currently known, knowledge of the encryption key does not let someone recover the plaintext message without an extraordinary amount of work (such as billions of years of computer time).

## The RSA Cryptosystem

M.I.T. is also known as the 'Tute.

Unfortunately, no one calls this the Cocks cryptosystem.

In 1976, three researchers at the Massachusetts Institute of Technology—Ronald Rivest, Adi Shamir, and Leonard Adleman—introduced to the world a public key cryptosystem, known as the **RSA system**, from the initials of its inventors. As often happens with cryptographic discoveries, the RSA system had been discovered several years earlier in secret government research in the United Kingdom. Clifford Cocks, working in secrecy at the United Kingdom's Government Communications Headquarters (GCHQ), had discovered this cryptosystem in 1973. However, his invention was unknown to the outside world until the late 1990s, when he was allowed to share classified GCHQ documents from the early 1970s. (An excellent account of this earlier discovery, as well as the work of Rivest, Shamir, and Adleman, can be found in [Si99].)

In the RSA cryptosystem, each individual has an encryption key  $(n, e)$  where  $n = pq$ , the modulus is the product of two large primes  $p$  and  $q$ , say with 200 digits each, and an exponent  $e$  that is relatively prime to  $(p - 1)(q - 1)$ . To produce a usable key, two large primes must be found. This can be done quickly on a computer using probabilistic primality tests, referred to earlier in this section. However, the product of these primes  $n = pq$ , with approximately 400 digits, cannot, as far as is currently known, be factored in a reasonable length of time. As we will see, this is an important reason why decryption cannot, as far as is currently known, be done quickly without a separate decryption key.

### RSA Encryption

To encrypt messages using a particular key  $(n, e)$ , we first translate a plaintext message  $M$  into sequences of integers. To do this, we first translate each plaintext letter into a two-digit number, using the same translation we employed for shift ciphers, with one key difference. That is, we include an initial zero for the letters A through J, so that A is translated into 00, B into 01, . . . , and J into 09. Then, we concatenate these two-digit numbers into strings of digits. Next, we divide this string into equally sized blocks of  $2N$  digits, where  $2N$  is the largest even number such that the number 2525 . . . 25 with  $2N$  digits does not exceed  $n$ . (When necessary, we pad the plaintext message with dummy Xs to make the last block the same size as all other blocks.)

After these steps, we have translated the plaintext message  $M$  into a sequence of integers  $m_1, m_2, \dots, m_k$  for some integer  $k$ . Encryption proceeds by transforming each block  $m_i$  to a ciphertext block  $c_i$ . This is done using the function

$$C = M^e \bmod n.$$

(To perform the encryption, we use an algorithm for fast modular exponentiation, such as Algorithm 5 in Section 4.2.) We leave the encrypted message as blocks of numbers and send these to the intended recipient. Because the RSA cryptosystem encrypts blocks of characters into blocks of characters, it is a block cipher.



**CLIFFORD COCKS (BORN 1950)** Clifford Cocks, born in Cheshire, England, was a talented mathematics student. In 1968 he won a silver medal at the International Mathematical Olympiad. Cocks attended King's College, Cambridge, studying mathematics. He also spent a short time at Oxford University working in number theory. In 1973 he decided not to complete his graduate work, instead taking a mathematical job at the Government Communications Headquarters (GCHQ) of British intelligence. Two months after joining GCHQ, Cocks learned about public key cryptography from an internal GCHQ report written by James Ellis. Cocks used his number theory knowledge to invent what is now called the RSA cryptosystem. He quickly realized that a public key cryptosystem could be based on the difficulty of reversing the process of multiplying two large primes. In 1997 he was allowed to reveal declassified GCHQ internal documents describing his discovery. Cocks is also known for his invention of a secure identity based encryption scheme, which uses information about a user's identity as a public key. In 2001, Cocks became the Chief Mathematician at GCHQ. He has also set up the Heilbronn Institute for Mathematical Research, a partnership between GCHQ and the University of Bristol.



Example 8 illustrates how RSA encryption is performed. For practical reasons we use small primes  $p$  and  $q$  in this example, rather than primes with 200 or more digits. Although the cipher described in this example is not secure, it does illustrate the techniques used in the RSA cipher.

**EXAMPLE 8** Encrypt the message STOP using the RSA cryptosystem with key  $(2537, 13)$ . Note that  $2537 = 43 \cdot 59$ ,  $p = 43$  and  $q = 59$  are primes, and

$$\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1.$$

**Solution:** To encrypt, we first translate the letters in STOP into their numerical equivalents. We then group these numbers into blocks of four digits (because  $2525 < 2537 < 252525$ ), to obtain

1819 1415.

We encrypt each block using the mapping

$$C = M^{13} \bmod 2537.$$

Computations using fast modular multiplication show that  $1819^{13} \bmod 2537 = 2081$  and  $1415^{13} \bmod 2537 = 2182$ . The encrypted message is 2081 2182. ◀

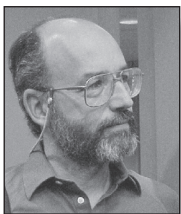
## RSA Decryption

The plaintext message can be quickly recovered from a ciphertext message when the decryption key  $d$ , an inverse of  $e$  modulo  $(p-1)(q-1)$ , is known. [Such an inverse exists because  $\gcd(e, (p-1)(q-1)) = 1$ .] To see this, note that if  $de \equiv 1 \pmod{(p-1)(q-1)}$ , there is an integer  $k$  such that  $de = 1 + k(p-1)(q-1)$ . It follows that

$$C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}.$$



**RONALD RIVEST (BORN 1948)** Ronald Rivest received a B.A. from Yale in 1969 and his Ph.D. in computer science from Stanford in 1974. Rivest is a computer science professor at M.I.T. and was a cofounder of RSA Data Security, which held the patent on the RSA cryptosystem that he invented together with Adi Shamir and Leonard Adleman. Areas that Rivest has worked in besides cryptography include machine learning, VLSI design, and computer algorithms. He is a coauthor of a popular text on algorithms ([CoLeRiSt09]).



**ADI SHAMIR (BORN 1952)** Adi Shamir was born in Tel Aviv, Israel. His undergraduate degree is from Tel Aviv University (1972) and his Ph.D. is from the Weizmann Institute of Science (1977). Shamir was a research assistant at the University of Warwick and an assistant professor at M.I.T. He is currently a professor in the Applied Mathematics Department at the Weizmann Institute and leads a group studying computer security. Shamir's contributions to cryptography, besides the RSA cryptosystem, include cracking knapsack cryptosystems, cryptanalysis of the Data Encryption Standard (DES), and the design of many cryptographic protocols.



**LEONARD ADLEMAN (BORN 1945)** Leonard Adleman was born in San Francisco, California. He received a B.S. in mathematics (1968) and his Ph.D. in computer science (1976) from the University of California, Berkeley. Adleman was a member of the mathematics faculty at M.I.T. from 1976 until 1980, where he was a coinventor of the RSA cryptosystem, and in 1980 he took a position in the computer science department at the University of Southern California (USC). He was appointed to a chaired position at USC in 1985. Adleman has worked on computer security, computational complexity, immunology, and molecular biology. He invented the term "computer virus." Adleman's recent work on DNA computing has sparked great interest. He was a technical adviser for the movie *Sneakers*, in which computer security played an important role.

By Fermat's little theorem [assuming that  $\gcd(M, p) = \gcd(M, q) = 1$ , which holds except in rare cases, which we cover in Exercise 28], it follows that  $M^{p-1} \equiv 1 \pmod{p}$  and  $M^{q-1} \equiv 1 \pmod{q}$ . Consequently,

$$C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 = M \pmod{p}$$

and

$$C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 = M \pmod{q}.$$

Because  $\gcd(p, q) = 1$ , it follows by the Chinese remainder theorem that


$$C^d \equiv M \pmod{pq}.$$

Example 9 illustrates how to decrypt messages sent using the RSA cryptosystem.

**EXAMPLE 9** We receive the encrypted message 0981 0461. What is the decrypted message if it was encrypted using the RSA cipher from Example 8?

**Solution:** The message was encrypted using the RSA cryptosystem with  $n = 43 \cdot 59$  and exponent 13. As Exercise 2 in Section 4.4 shows,  $d = 937$  is an inverse of 13 modulo  $42 \cdot 58 = 2436$ . We use 937 as our decryption exponent. Consequently, to decrypt a block  $C$ , we compute

$$M = C^{937} \bmod 2537.$$

To decrypt the message, we use the fast modular exponentiation algorithm to compute  $0981^{937} \bmod 2537 = 0704$  and  $0461^{937} \bmod 2537 = 1115$ . Consequently, the numerical version of the original message is 0704 1115. Translating this back to English letters, we see that the message is HELP. 

## RSA as a Public Key System



Why is the RSA cryptosystem suitable for public key cryptography? First, it is possible to rapidly construct a public key by finding two large primes  $p$  and  $q$ , each with more than 200 digits, and to find an integer  $e$  relatively prime to  $(p-1)(q-1)$ . When we know the factorization of the modulus  $n$ , that is, when we know  $p$  and  $q$ , we can quickly find an inverse  $d$  of  $e$  modulo  $(p-1)(q-1)$ . [This is done by using the Euclidean algorithm to find Bézout coefficients  $s$  and  $t$  for  $d$  and  $(p-1)(q-1)$ , which shows that the inverse of  $d$  modulo  $(p-1)(q-1)$  is  $s \bmod (p-1)(q-1)$ .] Knowing  $d$  lets us decrypt messages sent using our key. However, no method is known to decrypt messages that is not based on finding a factorization of  $n$ , or that does not also lead to the factorization of  $n$ .

Factorization is believed to be a difficult problem, as opposed to finding large primes  $p$  and  $q$ , which can be done quickly. The most efficient factorization methods known (as of 2010) require billions of years to factor 400-digit integers. Consequently, when  $p$  and  $q$  are 200-digit primes, it is believed that messages encrypted using  $n = pq$  as the modulus cannot be found in a reasonable time unless the primes  $p$  and  $q$  are known.

Although no polynomial-time algorithm is known for factoring large integers, active research is under way to find new ways to efficiently factor integers. Integers that were thought, as recently as several years ago, to be far too large to be factored in a reasonable amount of time can now be factored routinely. Integers with more than 150 digits, as well as some with more than 200 digits, have been factored using team efforts. When new factorization techniques are found,



it will be necessary to use larger primes to ensure secrecy of messages. Unfortunately, messages that were considered secure earlier can be saved and subsequently decrypted by unintended recipients when it becomes feasible to factor the  $n = pq$  in the key used for RSA encryption.

The RSA method is now widely used. However, the most commonly used cryptosystems are private key cryptosystems. The use of public key cryptography, via the RSA system, is growing. Nevertheless, there are applications that use both private key and public key systems. For example, a public key cryptosystem, such as RSA, can be used to distribute private keys to pairs of individuals when they wish to communicate. These people then use a private key system for encryption and decryption of messages.

## Cryptographic Protocols

So far we have shown how cryptography can be used to make messages secure. However, there are many other important applications of cryptography. Among these applications are **cryptographic protocols**, which are exchanges of messages carried out by two or more parties to achieve a particular security goal. In particular, we will show how cryptography can be used to allow two people to exchange a secret key over an insecure communication channel. We will also show how cryptography can be used to send signed secret messages so that the recipient can be sure that the message came from the purported sender. We refer the reader to [St05] for thorough discussions of a variety of cryptographic protocols.

**KEY EXCHANGE** We now discuss a protocol that two parties can use to exchange a secret key over an insecure communications channel without having shared any information in the past. Generating a key that two parties can share is important for many applications of cryptography. For example, for two people to send secure messages to each other using a private key cryptosystem they need to share a common key. The protocol we will describe is known as the **Diffie-Hellman key agreement protocol**, after Whitfield Diffie and Martin Hellman, who described it in 1976. However, this protocol was invented in 1974 by Malcolm Williamson in secret work at the British GCHQ. It was not until 1997 that his discovery was made public.

Suppose that Alice and Bob want to share a common key. The protocol follows these steps, where the computations are done in  $\mathbf{Z}_p$ .

- (1) Alice and Bob agree to use a prime  $p$  and a primitive root  $a$  of  $p$ .
- (2) Alice chooses a secret integer  $k_1$  and sends  $a^{k_1} \bmod p$  to Bob.
- (3) Bob chooses a secret integer  $k_2$  and sends  $a^{k_2} \bmod p$  to Alice.
- (4) Alice computes  $(a^{k_2})^{k_1} \bmod p$ .
- (5) Bob computes  $(a^{k_1})^{k_2} \bmod p$ .

At the end of this protocol, Alice and Bob have computed their shared key, namely

$$(a^{k_2})^{k_1} \bmod p = (a^{k_1})^{k_2} \bmod p.$$

To analyze the security of this protocol, note that the messages sent in steps (1), (2), and (3) are not assumed to be sent securely. We can even assume that these communications were in the clear and that their contents are public information. So,  $p$ ,  $a$ ,  $a^{k_1} \bmod p$ , and  $a^{k_2} \bmod p$  are assumed to be public information. The protocol ensures that  $k_1$ ,  $k_2$ , and the common key  $(a^{k_2})^{k_1} \bmod p = (a^{k_1})^{k_2} \bmod p$  are kept secret. To find the secret information from this public information requires that an adversary solves instances of the discrete logarithm problem,

because the adversary would need to find  $k_1$  and  $k_2$  from  $a^{k_1} \bmod p$  and  $a^{k_2} \bmod p$ , respectively. Furthermore, no other method is known for finding the shared key using just the public information. We have remarked that this is thought to be computationally infeasible when  $p$  and  $a$  are sufficiently large. With the computing power available now, this system is considered unbreakable when  $p$  has more than 300 decimal digits and  $k_1$  and  $k_2$  have more than 100 decimal digits each.


**DIGITAL SIGNATURES** Not only can cryptography be used to secure the confidentiality of a message, but it also can be used so that the recipient of the message knows that it came from the person they think it came from. We first show how a message can be sent so that a recipient of the message will be sure that the message came from the purported sender of the message. In particular, we can show how this can be accomplished using the RSA cryptosystem to apply a **digital signature** to a message.

Suppose that Alice's RSA public key is  $(n, e)$  and her private key is  $d$ . Alice encrypts a plaintext message  $x$  using the encryption function  $E_{(n,e)}(x) = x^e \bmod n$ . She decrypts a ciphertext message  $y$  using the decryption function  $D_{(n,e)}(y) = y^d \bmod n$ . Alice wants to send the message  $M$  so that everyone who receives the message knows that it came from her. Just as in RSA encryption, she translates the letters into their numerical equivalents and splits the resulting string into blocks  $m_1, m_2, \dots, m_k$  such that each block is the same size which is as large as possible so that  $0 \leq m_i \leq n$  for  $i = 1, 2, \dots, k$ . She then applies her decryption function  $D_{(n,e)}$  to each block, obtaining  $D_{n,e}(m_i)$ ,  $i = 1, 2, \dots, k$ . She sends the result to all intended recipients of the message.

When a recipient receives her message, they apply Alice's encryption function  $E_{(n,e)}$  to each block, which everyone has available because Alice's key  $(n, e)$  is public information. The result is the original plaintext block because  $E_{(n,e)}(D_{(n,e)}(x)) = x$ . So, Alice can send her message to as many people as she wants and by signing it in this way, every recipient can be sure it came from Alice. Example 10 illustrates this protocol.

**EXAMPLE 10** Suppose Alice's public RSA cryptosystem key is the same as in Example 8. That is,  $n = 43 \cdot 59 = 2537$  and  $e = 13$ . Her decryption key is  $d = 937$ , as described in Example 9. She wants to send the message "MEET AT NOON" to her friends so that they are sure it came from her. What should she send?

**Solution:** Alice first translates the message into blocks of digits, obtaining 1204 0419 0019 1314 1413 (as the reader should verify). She then applies her decryption transformation  $D_{(2537,13)}(x) = x^{937} \bmod 2537$  to each block. Using fast modular exponentiation (with the help of a computational aid), she finds that  $1204^{937} \bmod 2537 = 817$ ,  $419^{937} \bmod 2537 = 555$ ,  $19^{937} \bmod 2537 = 1310$ ,  $1314^{937} \bmod 2537 = 2173$ , and  $1413^{937} \bmod 2537 = 1026$ .

So, the message she sends, split into blocks, is 0817 0555 1310 2173 1026. When one of her friends gets this message, they apply her encryption transformation  $E_{(2537,13)}$  to each block. When they do this, they obtain the blocks of digits of the original message which they translate back to English letters. 

We have shown that signed messages can be sent using the RSA cryptosystem. We can extend this by sending signed secret messages. To do this, the sender applies RSA encryption using the publicly known encryption key of an intended recipient to each block that was encrypted using sender's decryption transformation. The recipient then first applies his private decryption transformation and then the sender's public encryption transformation. (Exercise 32 asks for this protocol to be carried out.)

## Exercises

- Encrypt the message DO NOT PASS GO by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
    - $f(p) = (p + 3) \bmod 26$  (the Caesar cipher)
    - $f(p) = (p + 13) \bmod 26$
    - $f(p) = (3p + 7) \bmod 26$
  - Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
    - $f(p) = (p + 4) \bmod 26$
    - $f(p) = (p + 21) \bmod 26$
    - $f(p) = (17p + 22) \bmod 26$
  - Encrypt the message WATCH YOUR STEP by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
    - $f(p) = (p + 14) \bmod 26$
    - $f(p) = (14p + 21) \bmod 26$
    - $f(p) = (-7p + 1) \bmod 26$
  - Decrypt these messages that were encrypted using the Caesar cipher.
    - EOXH MHDQV
    - WHVW WRGDB
    - HDW GLP VXP
  - Decrypt these messages encrypted using the shift cipher  $f(p) = (p + 10) \bmod 26$ .
    - CEBBOXNOB XYG
    - LO WI PBSOXN
    - DSWO PYB PEX
  - Suppose that when a long string of text is encrypted using a shift cipher  $f(p) = (p + k) \bmod 26$ , the most common letter in the ciphertext is X. What is the most likely value for  $k$  assuming that the distribution of letters in the text is typical of English text?
  - Suppose that when a string of English text is encrypted using a shift cipher  $f(p) = (p + k) \bmod 26$ , the resulting ciphertext is DY CVOOZ ZOBMRKXMO DY NBOKW. What was the original plaintext string?
  - Suppose that the ciphertext DVE CFMV KF NFEUVI, REU KYRK ZJ KYV JVVU FW JTZVETV was produced by encrypting a plaintext message using a shift cipher. What is the original plaintext?
  - Suppose that the ciphertext ERC WYJMG MIRXPC EHZERGIH XIGLRSPSKC MW MRHMWXM-RKYMWLEFPI JVSQ QEKMG was produced by encrypting a plaintext message using a shift cipher. What is the original plaintext?
  - Determine whether there is a key for which the enciphering function for the shift cipher is the same as the deciphering function.
  - What is the decryption function for an affine cipher if the encryption function is  $c = (15p + 13) \bmod 26$ ?
  - \* Find all pairs of integers keys  $(a, b)$  for affine ciphers for which the encryption function  $c = (ap + b) \bmod 26$  is the same as the corresponding decryption function.
  - Suppose that the most common letter and the second most common letter in a long ciphertext produced by encrypting a plaintext using an affine cipher  $f(p) = (ap + b) \bmod 26$  are Z and J, respectively. What are the most likely values of  $a$  and  $b$ ?
  - Encrypt the message GRIZZLY BEARS using blocks of five letters and the transposition cipher based on the permutation of  $\{1, 2, 3, 4, 5\}$  with  $\sigma(1) = 3$ ,  $\sigma(2) = 5$ ,  $\sigma(3) = 1$ ,  $\sigma(4) = 2$ , and  $\sigma(5) = 4$ . For this exercise, use the letter X as many times as necessary to fill out the final block of fewer than five letters.
  - Decrypt the message EABW EFRO ATMR ASIN which is the ciphertext produced by encrypting a plaintext message using the transposition cipher with blocks of four letters and the permutation  $\sigma$  of  $\{1, 2, 3, 4\}$  defined by  $\sigma(1) = 3$ ,  $\sigma(2) = 1$ ,  $\sigma(3) = 4$ , and  $\sigma(4) = 2$ .
  - \* Suppose that you know that a ciphertext was produced by encrypting a plaintext message with a transposition cipher. How might you go about breaking it?
  - Suppose you have intercepted a ciphertext message and when you determine the frequencies of letters in this message, you find the frequencies are similar to the frequency of letters in English text. Which type of cipher do you suspect was used?
- The **Vigenère cipher** is a block cipher, with a key that is a string of letters with numerical equivalents  $k_1 k_2 \dots k_m$ , where  $k_i \in \mathbb{Z}_{26}$  for  $i = 1, 2, \dots, m$ . Suppose that the numerical equivalents of the letters of a plaintext block are  $p_1 p_2 \dots p_m$ . The corresponding numerical ciphertext block is  $(p_1 + k_1) \bmod 26 (p_2 + k_2) \bmod 26 \dots (p_m + k_m) \bmod 26$ . Finally, we translate back to letters. For example, suppose that the key string is RED, with numerical equivalents 17 4 3. Then, the plaintext ORANGE, with numerical equivalents 14 17 00 13 06 04, is encrypted by first splitting it into two blocks 14 17 00 and 13 06 04. Then, in each block we shift the first letter by 17, the second by 4, and the third by 3. We obtain 5 21 03 and 04 10 07. The ciphertext is FVDEKH.
- Use the Vigenère cipher with key BLUE to encrypt the message SNOWFALL.
  - The ciphertext OIKYWVHBX was produced by encrypting a plaintext message using the Vigenère cipher with key HOT. What is the plaintext message?

20. Express the Vigenère cipher as a cryptosystem.

To break a Vigenère cipher by recovering a plaintext message from the ciphertext message without having the key, the first step is to figure out the length of the key string. The second step is to figure out each character of the key string by determining the corresponding shift. Exercises 21 and 22 deal with these two aspects.

21. Suppose that when a long string of text is encrypted using a Vigenère cipher, the same string is found in the ciphertext starting at several different positions. Explain how this information can be used to help determine the length of the key.
22. Once the length of the key string of a Vigenère cipher is known, explain how to determine each of its characters. Assume that the plaintext is long enough so that the frequency of its letters is reasonably close to the frequency of letters in typical English text.
- \*23. Show that we can easily factor  $n$  when we know that  $n$  is the product of two primes,  $p$  and  $q$ , and we know the value of  $(p-1)(q-1)$ .

In Exercises 24–27 first express your answers without computing modular exponentiations. Then use a computational aid to complete these computations.

24. Encrypt the message ATTACK using the RSA system with  $n = 43 \cdot 59$  and  $e = 13$ , translating each letter into integers and grouping together pairs of integers, as done in Example 8.
25. Encrypt the message UPLOAD using the RSA system with  $n = 53 \cdot 61$  and  $e = 17$ , translating each letter into integers and grouping together pairs of integers, as done in Example 8.
26. What is the original message encrypted using the RSA system with  $n = 53 \cdot 61$  and  $e = 17$  if the encrypted message is 3185 2038 2460 2550? (To decrypt, first find the decryption exponent  $d$ , which is the inverse of  $e = 17$  modulo  $52 \cdot 60$ .)
27. What is the original message encrypted using the RSA system with  $n = 43 \cdot 59$  and  $e = 13$  if the encrypted message is 0667 1947 0671? (To decrypt, first find the decryption exponent  $d$  which is the inverse of  $e = 13$  modulo  $42 \cdot 58$ .)
- \*28. Suppose that  $(n, e)$  is an RSA encryption key, with  $n = pq$  where  $p$  and  $q$  are large primes and  $\gcd(e, (p-1)(q-1)) = 1$ . Furthermore, suppose that  $d$  is an inverse of  $e$  modulo  $(p-1)(q-1)$ . Suppose that  $C \equiv M^e \pmod{pq}$ . In the text we showed that RSA decryption, that is, the congruence  $C^d \equiv M \pmod{pq}$  holds when  $\gcd(M, pq) = 1$ . Show that this decryption congruence also holds when  $\gcd(M, pq) > 1$ . [Hint: Use congruences modulo  $p$  and modulo  $q$  and apply the Chinese remainder theorem.]

29. Describe the steps that Alice and Bob follow when they use the Diffie-Hellman key exchange protocol to generate a shared key. Assume that they use the prime  $p = 23$  and take  $a = 5$ , which is a primitive root of 23, and that Alice selects  $k_1 = 8$  and Bob selects  $k_2 = 5$ . (You may want to use some computational aid.)
30. Describe the steps that Alice and Bob follow when they use the Diffie-Hellman key exchange protocol to generate a shared key. Assume that they use the prime  $p = 101$  and take  $a = 2$ , which is a primitive root of 101, and that Alice selects  $k_1 = 7$  and Bob selects  $k_2 = 9$ . (You may want to use some computational aid.)

In Exercises 31–32 suppose that Alice and Bob have these public keys and corresponding private keys:  $(n_{\text{Alice}}, e_{\text{Alice}}) = (2867, 7) = (61 \cdot 47, 7)$ ,  $d_{\text{Alice}} = 1183$  and  $(n_{\text{Bob}}, e_{\text{Bob}}) = (3127, 21) = (59 \cdot 53, 21)$ ,  $d_{\text{Bob}} = 1149$ . First express your answers without carrying out the calculations. Then, using a computational aid, if available, perform the calculation to get the numerical answers.

31. Alice wants to send to all her friends, including Bob, the message “SELL EVERYTHING” so that he knows that she sent it. What should she send to her friends, assuming she signs the message using the RSA cryptosystem.
32. Alice wants to send to Bob the message “BUY NOW” so that he knows that she sent it and so that only Bob can read it. What should she send to Bob, assuming she signs the message and then encrypts it using Bob’s public key?
33. We describe a basic key exchange protocol using private key cryptography upon which more sophisticated protocols for key exchange are based. Encryption within the protocol is done using a private key cryptosystem (such as AES) that is considered secure. The protocol involves three parties, Alice and Bob, who wish to exchange a key, and a trusted third party Cathy. Assume that Alice has a secret key  $k_{\text{Alice}}$  that only she and Cathy know, and Bob has a secret key  $k_{\text{Bob}}$  which only he and Cathy know. The protocol has three steps:

(i) Alice sends the trusted third party Cathy the message “request a shared key with Bob” encrypted using Alice’s key  $k_{\text{Alice}}$ .

(ii) Cathy sends back to Alice a key  $k_{\text{Alice}, \text{Bob}}$ , which she generates, encrypted using the key  $k_{\text{Alice}}$ , followed by this same key  $k_{\text{Alice}, \text{Bob}}$ , encrypted using Bob’s key,  $k_{\text{Bob}}$ .

(iii) Alice sends to Bob the key  $k_{\text{Alice}, \text{Bob}}$  encrypted using  $k_{\text{Bob}}$ , known only to Bob and to Cathy.

Explain why this protocol allows Alice and Bob to share the secret key  $k_{\text{Alice}, \text{Bob}}$ , known only to them and to Cathy.

## Key Terms and Results

### TERMS

**$a \mid b$  ( $a$  divides  $b$ ):** there is an integer  $c$  such that  $b = ac$

**$a$  and  $b$  are congruent modulo  $m$ :  $m$  divides  $a - b$**

**modular arithmetic:** arithmetic done modulo an integer  $m \geq 2$

**prime:** an integer greater than 1 with exactly two positive integer divisors

**composite:** an integer greater than 1 that is not prime

**Mersenne prime:** a prime of the form  $2^p - 1$ , where  $p$  is prime

**$\gcd(a, b)$  (greatest common divisor of  $a$  and  $b$ ):** the largest integer that divides both  $a$  and  $b$

**relatively prime integers:** integers  $a$  and  $b$  such that  $\gcd(a, b) = 1$

**pairwise relatively prime integers:** a set of integers with the property that every pair of these integers is relatively prime

**$\text{lcm}(a, b)$  (least common multiple of  $a$  and  $b$ ):** the smallest positive integer that is divisible by both  $a$  and  $b$

**$a \bmod b$ :** the remainder when the integer  $a$  is divided by the positive integer  $b$

**$a \equiv b \pmod{m}$  ( $a$  is congruent to  $b$  modulo  $m$ ):**  $a - b$  is divisible by  $m$

**$n = (a_k a_{k-1} \dots a_1 a_0)_b$ :** the base  $b$  representation of  $n$

**binary representation:** the base 2 representation of an integer

**octal representation:** the base 8 representation of an integer

**hexadecimal representation:** the base 16 representation of an integer

**linear combination of  $a$  and  $b$  with integer coefficients:** an expression of the form  $sa + tb$ , where  $s$  and  $t$  are integers

**Bézout coefficients of  $a$  and  $b$ :** integers  $s$  and  $t$  such that the Bézout identity  $sa + tb = \gcd(a, b)$  holds

**inverse of  $a$  modulo  $m$ :** an integer  $\bar{a}$  such that  $\bar{a}a \equiv 1 \pmod{m}$

**linear congruence:** a congruence of the form  $ax \equiv b \pmod{m}$ , where  $x$  is an integer variable

**pseudoprime to the base  $b$ :** a composite integer  $n$  such that  $b^{n-1} \equiv 1 \pmod{n}$

**Carmichael number:** a composite integer  $n$  such that  $n$  is a pseudoprime to the base  $b$  for all positive integers  $b$  with  $\gcd(b, n) = 1$

**primitive root of a prime  $p$ :** an integer  $r$  in  $\mathbb{Z}_p$  such that every integer not divisible by  $p$  is congruent modulo  $p$  to a power of  $r$

**discrete logarithm of  $a$  to the base  $r$  modulo  $p$ :** the integer  $e$  with  $0 \leq e \leq p - 1$  such that  $r^e \equiv a \pmod{p}$

**encryption:** the process of making a message secret

**decryption:** the process of returning a secret message to its original form

**encryption key:** a value that determines which of a family of encryption functions is to be used

**shift cipher:** a cipher that encrypts the plaintext letter  $p$  as  $(p + k) \bmod m$  for an integer  $k$

**affine cipher:** a cipher that encrypts the plaintext letter  $p$  as  $(ap + b) \bmod m$  for integers  $a$  and  $b$  with  $\gcd(a, m) = 1$

**character cipher:** a cipher that encrypts characters one by one

**block cipher:** a cipher that encrypts blocks of characters of a fixed size

**crytanalysis:** the process of recovering the plaintext from ciphertext without knowledge of the encryption method, or with knowledge of the encryption method, but not the key

**cryptosystem:** a five-tuple  $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$  where  $\mathcal{P}$  is the set of plaintext messages,  $\mathcal{C}$  is the set of ciphertext messages,  $\mathcal{K}$  is the set of keys,  $\mathcal{E}$  is the set of encryption functions, and  $\mathcal{D}$  is the set of decryption functions

**private key encryption:** encryption where both encryption keys and decryption keys must be kept secret

**public key encryption:** encryption where encryption keys are public knowledge, but decryption keys are kept secret

**RSA cryptosystem:** the cryptosystem where  $\mathcal{P}$  and  $\mathcal{C}$  are both  $\mathbb{Z}_{26}$ ,  $\mathcal{K}$  is the set of pairs  $k = (n, e)$  where  $n = pq$  where  $p$  and  $q$  are large primes and  $e$  is a positive integer,  $E_k(p) = p^e \bmod n$ , and  $D_k(c) = c^d \bmod n$  where  $d$  is the inverse of  $e$  modulo  $(p - 1)(q - 1)$

**key exchange protocol:** a protocol used for two parties to generate a shared key

**digital signature:** a method that a recipient can use to determine that the purported sender of a message actually sent the message

### RESULTS

**division algorithm:** Let  $a$  and  $d$  be integers with  $d$  positive. Then there are unique integers  $q$  and  $r$  with  $0 \leq r < d$  such that  $a = dq + r$ .

Let  $b$  be an integer greater than 1. Then if  $n$  is a positive integer, it can be expressed uniquely in the form  $n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$ .

The algorithm for finding the base  $b$  expansion of an integer (see Algorithm 1 in Section 4.2)

The conventional algorithms for addition and multiplication of integers (given in Section 4.2)

The modular exponentiation algorithm (see Algorithm 5 in Section 4.2)

**Euclidean algorithm:** for finding greatest common divisors by successively using the division algorithm (see Algorithm 1 in Section 4.3)

**Bézout's theorem:** If  $a$  and  $b$  are positive integers, then  $\gcd(a, b)$  is a linear combination of  $a$  and  $b$ .

**sieve of Eratosthenes:** A procedure for finding all primes not exceeding a specified number  $n$ , described in Section 4.3

**fundamental theorem of arithmetic:** Every positive integer can be written uniquely as the product of primes, where the prime factors are written in order of increasing size.

If  $a$  and  $b$  are positive integers, then  $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$ .

If  $m$  is a positive integer and  $\gcd(a, m) = 1$ , then  $a$  has a unique inverse modulo  $m$ .

**Chinese remainder theorem:** A system of linear congruences modulo pairwise relatively prime integers has a unique solution modulo the product of these moduli.

**Fermat's little theorem:** If  $p$  is prime and  $p \nmid a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .



## Review Questions

- Find  $210 \div 17$  and  $210 \bmod 17$ .
- Define what it means for  $a$  and  $b$  to be congruent modulo 7.
  - Which pairs of the integers  $-11, -8, -7, -1, 0, 3$ , and  $17$  are congruent modulo 7?
  - Show that if  $a$  and  $b$  are congruent modulo 7, then  $10a + 13$  and  $-4b + 20$  are also congruent modulo 7.
- Show that if  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$ .
- Describe a procedure for converting decimal (base 10) expansions of integers into hexadecimal expansions.
- Convert  $(1101\ 1001\ 0101\ 1011)_2$  to octal and hexadecimal representations.
- Convert  $(7206)_8$  and  $(A0EB)_{16}$  to a binary representation.
- State the fundamental theorem of arithmetic.
- Describe a procedure for finding the prime factorization of an integer.
  - Use this procedure to find the prime factorization of  $80,707$ .
- Define the greatest common divisor of two integers.
  - Describe at least three different ways to find the greatest common divisor of two integers. When does each method work best?
  - Find the greatest common divisor of  $1,234,567$  and  $7,654,321$ .
  - Find the greatest common divisor of  $2^3 3^5 5^7 7^9 11$  and  $2^9 3^7 5^5 7^3 13$ .
- How can you find a linear combination (with integer coefficients) of two integers that equals their greatest common divisor?
  - Express  $\gcd(84, 119)$  as a linear combination of  $84$  and  $119$ .
- What does it mean for  $\bar{a}$  to be an inverse of  $a$  modulo  $m$ ?
  - How can you find an inverse of  $a$  modulo  $m$  when  $m$  is a positive integer and  $\gcd(a, m) = 1$ ?
  - Find an inverse of  $7$  modulo  $19$ .
- How can an inverse of  $a$  modulo  $m$  be used to solve the congruence  $ax \equiv b \pmod{m}$  when  $\gcd(a, m) = 1$ ?
  - Solve the linear congruence  $7x \equiv 13 \pmod{19}$ .
- State the Chinese remainder theorem.
  - Find the solutions to the system  $x \equiv 1 \pmod{4}$ ,  $x \equiv 2 \pmod{5}$ , and  $x \equiv 3 \pmod{7}$ .
- Suppose that  $2^{n-1} \equiv 1 \pmod{n}$ . Is  $n$  necessarily prime?
- Use Fermat's little theorem to evaluate  $9^{200} \bmod 19$ .
- Explain how the check digit is found for a 10-digit ISBN.
- Encrypt the message APPLES AND ORANGES using a shift cipher with key  $k = 13$ .
- What is the difference between a public key and a private key cryptosystem?
  - Explain why using shift ciphers is a private key system.
  - Explain why the RSA cryptosystem is a public key system.
- Explain how encryption and decryption are done in the RSA cryptosystem.
- Describe how two parties can share a secret key using the Diffie-Hellman key exchange protocol.

## Supplementary Exercises

- The odometer on a car goes to up 100,000 miles. The present owner of a car bought it when the odometer read 43,179 miles. He now wants to sell it; when you examine the car for possible purchase, you notice that the odometer reads 89,697 miles. What can you conclude about how many miles he drove the car, assuming that the odometer always worked correctly?
- Explain why  $n \div 7$  equals the number of complete weeks in  $n$  days.
  - Explain why  $n \div 24$  equals the number of complete days in  $n$  hours.
- Find four numbers congruent to 5 modulo 17.
- Show that if  $a$  and  $d$  are positive integers, then there are integers  $q$  and  $r$  such that  $a = dq + r$  where  $-d/2 < r \leq d/2$ .
- \* Show that if  $ac \equiv bc \pmod{m}$ , where  $a, b, c$ , and  $m$  are integers with  $m > 2$ , and  $d = \gcd(m, c)$ , then  $a \equiv b \pmod{m/d}$ .
- Show that the sum of the squares of two odd integers cannot be the square of an integer.
- Show that if  $n^2 + 1$  is a perfect square, where  $n$  is an integer, then  $n$  is even.
- Prove that there are no solutions in integers  $x$  and  $y$  to the equation  $x^2 - 5y^2 = 2$ . [Hint: Consider this equation modulo 5.]
- Develop a test for divisibility of a positive integer  $n$  by 8 based on the binary expansion of  $n$ .
- Develop a test for divisibility of a positive integer  $n$  by 3 based on the binary expansion of  $n$ .
- Devise an algorithm for guessing a number between 1 and  $2^n - 1$  by successively guessing each bit in its binary expansion.
- Determine the complexity, in terms of the number of guesses, needed to determine a number between 1 and  $2^n - 1$  by successively guessing the bits in its binary expansion.
- Show that an integer is divisible by 9 if and only if the sum of its decimal digits is divisible by 9.



- \*\*14.** Show that if  $a$  and  $b$  are positive irrational numbers such that  $1/a + 1/b = 1$ , then every positive integer can be uniquely expressed as either  $\lfloor ka \rfloor$  or  $\lfloor kb \rfloor$  for some positive integer  $k$ .
- 15.** Prove there are infinitely many primes by showing that  $Q_n = n! + 1$  must have a prime factor greater than  $n$  whenever  $n$  is a positive integer.
- 16.** Find a positive integer  $n$  for which  $Q_n = n! + 1$  is not prime.
- 17.** Use Dirichlet's theorem, which states there are infinitely many primes in every arithmetic progression  $ak + b$  where  $\gcd(a, b) = 1$ , to show that there are infinitely many primes that have a decimal expansion ending with a 1.
- 18.** Prove that if  $n$  is a positive integer such that the sum of the divisors of  $n$  is  $n + 1$ , then  $n$  is prime.
- \*19.** Show that every integer greater than 11 is the sum of two composite integers.
- 20.** Find the five smallest consecutive composite integers.
- 21.** Show that Goldbach's conjecture, which states that every even integer greater than 2 is the sum of two primes, is equivalent to the statement that every integer greater than 5 is the sum of three primes.
- 22.** Find an arithmetic progression of length six beginning with 7 that contains only primes.
- \*23.** Prove that if  $f(x)$  is a nonconstant polynomial with integer coefficients, then there is an integer  $y$  such that  $f(y)$  is composite. [Hint: Assume that  $f(x_0) = p$  is prime. Show that  $p$  divides  $f(x_0 + kp)$  for all integers  $k$ . Obtain a contradiction of the fact that a polynomial of degree  $n$ , where  $n > 1$ , takes on each value at most  $n$  times.]
- \*24.** How many zeros are at the end of the binary expansion of  $100_{10}$ ?
- 25.** Use the Euclidean algorithm to find the greatest common divisor of 10,223 and 33,341.
- 26.** How many divisions are required to find  $\gcd(144, 233)$  using the Euclidean algorithm?
- 27.** Find  $\gcd(2n + 1, 3n + 2)$ , where  $n$  is a positive integer. [Hint: Use the Euclidean algorithm.]
- 28. a)** Show that if  $a$  and  $b$  are positive integers with  $a \geq b$ , then  $\gcd(a, b) = a$  if  $a = b$ ,  $\gcd(a, b) = 2 \gcd(a/2, b/2)$  if  $a$  and  $b$  are even,  $\gcd(a, b) = \gcd(a/2, b)$  if  $a$  is even and  $b$  is odd, and  $\gcd(a, b) = \gcd(a - b, b)$  if both  $a$  and  $b$  are odd.
- b)** Explain how to use (a) to construct an algorithm for computing the greatest common divisor of two positive integers that uses only comparisons, subtractions, and shifts of binary expansions, without using any divisions.
- c)** Find  $\gcd(1202, 4848)$  using this algorithm.
- 29.** Adapt the proof that there are infinitely many primes (Theorem 3 in Section 4.3) to show that there are infinitely many primes in the arithmetic progression  $6k + 5, k = 1, 2, \dots$
- 30.** Explain why you cannot directly adapt the proof that there are infinitely many primes (Theorem 3 in Section 4.3) to show that there are infinitely many primes in the arithmetic progression  $3k + 1, k = 1, 2, \dots$
- 31.** Explain why you cannot directly adapt the proof that there are infinitely many primes (Theorem 3 in Section 4.3) to show that there are infinitely many primes in the arithmetic progression  $4k + 1, k = 1, 2, \dots$
- 32.** Show that if the smallest prime factor  $p$  of the positive integer  $n$  is larger than  $\sqrt[3]{n}$ , then  $n/p$  is prime or equal to 1.
- A set of integers is called **mutually relatively prime** if the greatest common divisor of these integers is 1.
- 33.** Determine whether the integers in each of these sets are mutually relatively prime.
- a)** 8, 10, 12                      **b)** 12, 15, 25  
**c)** 15, 21, 28                      **d)** 21, 24, 28, 32
- 34.** Find a set of four mutually relatively prime integers such that no two of them are relatively prime.
- \*35.** For which positive integers  $n$  is  $n^4 + 4^n$  prime?
- 36.** Show that the system of congruences  $x \equiv 2 \pmod{6}$  and  $x \equiv 3 \pmod{9}$  has no solutions.
- 37.** Find all solutions of the system of congruences  $x \equiv 4 \pmod{6}$  and  $x \equiv 13 \pmod{15}$ .
- \*38. a)** Show that the system of congruences  $x \equiv a_1 \pmod{m_1}$  and  $x \equiv a_2 \pmod{m_2}$ , where  $a_1, a_2, m_1$ , and  $m_2$  are integers with  $m_1 > 0$  and  $m_2 > 0$ , has a solution if and only if  $\gcd(m_1, m_2) \mid a_1 - a_2$ .
- b)** Show that if the system in part (a) has a solution, then it is unique modulo  $\text{lcm}(m_1, m_2)$ .
- 39.** Prove that 30 divides  $n^9 - n$  for every nonnegative integer  $n$ .
- 40.** Prove that  $n^{12} - 1$  is divisible by 35 for every integer  $n$  for which  $\gcd(n, 35) = 1$ .
- 41.** Show that if  $p$  and  $q$  are distinct prime numbers, then  $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ .
- The check digit  $a_{13}$  for an ISBN-13 with initial digits  $a_1 a_2 \dots a_{12}$  is determined by the congruence  $(a_1 + a_3 + \dots + a_{13}) + 3(a_2 + a_4 + \dots + a_{12}) \equiv 0 \pmod{10}$ .
- 42.** Determine whether each of these 13-digit numbers is a valid ISBN-13.
- a)** 978-0-073-20679-1  
**b)** 978-0-45424-521-1  
**c)** 978-3-16-148410-0  
**d)** 978-0-201-10179-9
- 43.** Show that the check digit of an ISBN-13 can always detect a single error.
- 44.** Show that there are transpositions of two digits that are not detected by an ISBN-13.
- A **routing transit number (RTN)** is a bank code used in the United States which appears on the bottom of checks. The most common form of an RTN has nine digits, where the last digit is a check digit. If  $d_1 d_2 \dots d_9$  is a valid RTN,

the congruence  $3(d_1 + d_4 + d_7) + 7(d_2 + d_5 + d_8) + (d_3 + d_6 + d_9) \equiv 0 \pmod{10}$  must hold.

45. Show that if  $d_1 d_2 \dots d_9$  is a valid RTN, then  $d_9 = 7(d_1 + d_4 + d_7) + 3(d_2 + d_5 + d_8) + 9(d_3 + d_6) \pmod{10}$ . Furthermore, use this formula to find the check digit that follows the eight digits 11100002 in a valid RTN.
46. Show that the check digit of an RTN can detect all single errors and determine which transposition errors an RTN check digit can catch and which ones it cannot catch.
47. The encrypted version of a message is LJMKG MG-MXF QEXMW. If it was encrypted using the affine cipher  $f(p) = (7p + 10) \pmod{26}$ , what was the original message?

**Autokey ciphers** are ciphers where the  $n$ th letter of the plaintext is shifted by the numerical equivalent of the  $n$ th letter of a keystream. The keystream begins with a seed letter; its subsequent letters are constructed using either the plaintext or the ciphertext. When the plaintext is used, each character of the

keystream, after the first, is the previous letter of the plaintext. When the ciphertext is used, each subsequent character of the keystream, after the first, is the previous letter of the ciphertext computed so far. In both cases, plaintext letters are encrypted by shifting each character by the numerical equivalent of the corresponding keystream letter.

48. Use the autokey cipher to encrypt the message NOW IS THE TIME TO DECIDE (ignoring spaces) using
  - a) the keystream with seed X followed by letters of the plaintext.
  - b) the keystream with seed X followed by letters of the ciphertext.
49. Use the autokey cipher to encrypt the message THE DREAM OF REASON (ignoring spaces) using
  - a) the keystream with seed X followed by letters of the plaintext.
  - b) the keystream with seed X followed by letters of the ciphertext.

## Computer Projects

Write programs with these inputs and outputs.

1. Given integers  $n$  and  $b$ , each greater than 1, find the base  $b$  expansion of this integer.
2. Given the positive integers  $a$ ,  $b$ , and  $m$  with  $m > 1$ , find  $a^b \pmod{m}$ .
3. Given a positive integer, find the Cantor expansion of this integer (see the preamble to Exercise 48 of Section 4.2).
4. Given a positive integer, determine whether it is prime using trial division.
5. Given a positive integer, find the prime factorization of this integer.
6. Given two positive integers, find their greatest common divisor using the Euclidean algorithm.
7. Given two positive integers, find their least common multiple.
8. Given positive integers  $a$  and  $b$ , find Bézout coefficients  $s$  and  $t$  of  $a$  and  $b$ .
9. Given relatively prime positive integers  $a$  and  $b$ , find an inverse of  $a$  modulo  $b$ .
10. Given  $n$  linear congruences modulo pairwise relatively prime moduli, find the simultaneous solution of these congruences modulo the product of these moduli.
11. Given a positive integer  $N$ , a modulus  $m$ , a multiplier  $a$ , an increment  $c$ , and a seed  $x_0$ , where  $0 \leq a < m$ ,  $0 \leq c < m$ , and  $0 \leq x_0 < m$ , generate the sequence of  $N$  pseudo-random numbers using the linear congruential generator  $x_{n+1} = (ax_n + c) \pmod{m}$ .
12. Given a set of identification numbers, use a hash function to assign them to memory locations where there are  $k$  memory locations.
13. Compute the check digit when given the first nine digits of an ISBN-10.
14. Given a message and a positive integer  $k$  less than 26, encrypt this message using the shift cipher with key  $k$ ; and given a message encrypted using a shift cipher with key  $k$ , decrypt this message.
15. Given a message and positive integers  $a$  and  $b$  less than 26 with  $\gcd(a, 26)$ , encrypt this message using an affine cipher with key  $(a, b)$ ; and given a message encrypted using the affine cipher with key  $(a, b)$ , decrypt this message, by first finding the decryption key and then applying the appropriate decryption transformation.
16. Find the original plaintext message from the ciphertext message produced by encrypting the plaintext message using a shift cipher. Do this using a frequency count of letters in the ciphertext.
- \*17. Construct a valid RSA encryption key by finding two primes  $p$  and  $q$  with 200 digits each and an integer  $e > 1$  relatively prime to  $(p - 1)(q - 1)$ .
18. Given a message and an integer  $n = pq$  where  $p$  and  $q$  are odd primes and an integer  $e > 1$  relatively prime to  $(p - 1)(q - 1)$ , encrypt the message using the RSA cryptosystem with key  $(n, e)$ .
19. Given a valid RSA key  $(n, e)$ , and the primes  $p$  and  $q$  with  $n = pq$ , find the associated decryption key  $d$ .
20. Given a message encrypted using the RSA cryptosystem with key  $(n, e)$  and the associated decryption key  $d$ , decrypt this message.
21. Generate a shared key using the Diffie-Hellman key exchange protocol.
22. Given the RSA public and private keys of two parties, send a signed secret message from one of the parties to the other.

## Computations and Explorations

Use a computational program or programs you have written to do these exercises.

1. Determine whether  $2^p - 1$  is prime for each of the primes not exceeding 100.
2. Test a range of large Mersenne numbers  $2^p - 1$  to determine whether they are prime. (You may want to use software from the GIMPS project.)
3. Determine whether  $Q_n = p_1 p_2 \cdots p_n + 1$  is prime where  $p_1, p_2, \dots, p_n$  are the  $n$  smallest primes, for as many positive integer  $n$  as possible.
4. Look for polynomials in one variables whose values at long runs of consecutive integers are all primes.
5. Find as many primes of the form  $n^2 + 1$  where  $n$  is a positive integer as you can. It is not known whether there are infinitely many such primes.
6. Find 10 different primes each with 100 digits.
7. How many primes are there less than 1,000,000, less than 10,000,000, and less than 100,000,000? Can you propose an estimate for the number of primes less than  $x$  where  $x$  is a positive integer?
8. Find a prime factor of each of 10 different 20-digit odd integers, selected at random. Keep track of how long it takes to find a factor of each of these integers. Do the same thing for 10 different 30-digit odd integers, 10 different 40-digit odd integers, and so on, continuing as long as possible.
9. Find all pseudoprimes to the base 2 that do not exceed 10,000.

## Writing Projects

Respond to these with essays using outside sources.

1. Describe the Lucas–Lehmer test for determining whether a Mersenne number is prime. Discuss the progress of the GIMPS project in finding Mersenne primes using this test.
2. Explain how probabilistic primality tests are used in practice to produce extremely large numbers that are almost certainly prime. Do such tests have any potential drawbacks?
3. The question of whether there are infinitely many Carmichael numbers was solved recently after being open for more than 75 years. Describe the ingredients that went into the proof that there are infinitely many such numbers.
4. Summarize the current status of factoring algorithms in terms of their complexity and the size of numbers that can currently be factored. When do you think that it will be feasible to factor 200-digit numbers?
5. Describe the algorithms that are actually used by modern computers to add, subtract, multiply, and divide positive integers.
6. Describe the history of the Chinese remainder theorem. Describe some of the relevant problems posed in Chinese and Hindu writings and how the Chinese remainder theorem applies to them.
7. When are the numbers of a sequence truly random numbers, and not pseudorandom? What shortcomings have been observed in simulations and experiments in which pseudorandom numbers have been used? What are the properties that pseudorandom numbers can have that random numbers should not have?
8. Explain how a check digit is found for an International Bank Account Number (IBAN) and discuss the types of errors that can be found using this check digit.
9. Describe the Luhn algorithm for finding the check digit of a credit card number and discuss the types of errors that can be found using this check digit.
10. Show how a congruence can be used to tell the day of the week for any given date.
11. Describe how public key cryptography is being applied. Are the ways it is applied secure given the status of factoring algorithms? Will information kept secure using public key cryptography become insecure in the future?
12. Describe how public key cryptography can be used to produce signed secret messages so that the recipient is relatively sure the message was sent by the person expected to have sent it.
13. Describe the Rabin public key cryptosystem, explaining how to encrypt and how to decrypt messages and why it is suitable for use as a public key cryptosystem.
- \*14. Explain why it would not be suitable to use  $p$ , where  $p$  is a large prime, as the modulus for encryption in the RSA cryptosystem. That is, explain how someone could, without excessive computation, find a private key from the corresponding public key if the modulus were a large prime, rather than the product of two large primes.
15. Explain what is meant by a cryptographic hash function? What are the important properties such a function must have?