Richard T. Petras

Privacy for the Twenty-First Century: Cryptography

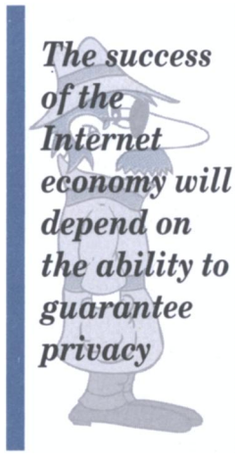
The Internet is everywhere today. E-mail is as common as a telephone call, and every company includes its Web site in its advertisements. The Internet economy was expected to surpass $1.3 trillion by summer 2000 (Must Read 1999a), and online retailing was expected to generate $36 billion in revenue in 1999, a 250 percent increase over 1998 (Must Read 1999b). In the present millennium, daily life at all levels will increasingly depend on the transmission over public lines of sensitive, private data, whether it is payment information or personal e-mail. Since "nearly 60% of US consumers think that transactions made via the Internet are unsafe" (Must Read 1999a), the ultimate success of the Internet economy depends on the ability to guarantee privacy on public systems. Cryptography and secure cryptosystems will help protect the privacy of all computer users, ranging from government and military organizations to the individual user at home.

Cryptography, from the Greek *kryptos* ("hidden") and *graphein* ("to write"), is defined as the creation of systems to render a message unintelligible to unauthorized readers. Cryptanalysis, in contrast, is the practice of breaking codes, usually when the key is not known. Cryptology is the study of the two disciplines. Every cryptographic system consists of taking a message called *plaintext,* applying a cipher or code associated with a particular key that enciphers or encodes the message, and producing ciphertext. After the message is received, the rightful recipient, who possesses the key, can decipher or decode the message (Kahn 1967, p. xv).

Cryptography has been used since the first time that a secret message was sent through a third party. Early cryptosystems were crude, employing a simple letter shift, and reached a pinnacle with Germany's Enigma machine during World War II. Enigma was a portable, battery-powered machine that allowed the user to produce ciphertext one character at a time with a series of removable and interchangeable rotors (Kahn 1967, pp. 420–22).

Today, with the advent of e-mail and the Internet, privacy and security have become a concern to computer users on all levels. One method of increasing the privacy of all this traffic is to encrypt it, thereby preventing unauthorized users from accessing private information. All cryptosystems rely on keys, and in conventional systems the same key, called a *symmetric key,* is used for both encrypting and decrypting. According to Zimmerman (1998, p. 111), one problem is that this key must be "transmitted over a secure channel—a process that is often inconvenient. After all, if a secure channel exists, why is encryption needed in the first place?" Diffie and Hellman removed this restraint in 1976 with their groundbreaking article "New Directions in Cryptography," in which they described their work on a revolutionary new kind of cryptosystem.

In their article, Diffie and Hellman gave the first description of a new type of cryptosystem, called *public-key cryptography.* This new system was revolutionary because it removed the need for a symmetric key. In a public-key cryptosystem, the sender (Alice) and the receiver (Bob) each generate two keys, an enciphering key e, which can be published in a public file, and a related deciphering key d, which is kept secret. If Alice wants to send a message to Bob, she simply looks up Bob's enciphering key e_B, enciphers her message using e_B, and sends it to Bob over a regular and possibly insecure channel. Only Bob, who knows his own secret deciphering key d_B, can decipher the message. The strength of a public-key system lies in choosing the keys so that the process is not reversible. What we want are asymmetric keys: it should be "computationally infeasible to derive d [the deciphering key] from e [the public enciphering key]" (Hellman 1979, p. 147). This "irreversibility" is achieved through mathematical processes that are easy to compute in one direction but exceedingly difficult and slow to solve in the other. The two main public-key cryptosystems are Diffie-Hellman,



Richard Petras, petras@horacemann.org, teaches at Horace Mann School, Riverdale, NY 10471. His interests include mathematics history, technology, and the teaching of mathematics.

which uses discrete logarithms, and the system that we discuss in this article, RSA, which is based on the difficulty of factoring large numbers (Zimmerman 1998, p. 112).

RSA is one of the most popular public-key cryptosystems in use in the world today. The name *RSA* comes from the last names of its three inventors: Ronald L. Rivest, Adi Shamir, and Leonard Adelman. The RSA encryption system uses a large number n, which is the product of two large primes, p and q, to construct an enciphering function f and a deciphering function f^{-1}. To construct the enciphering function, we first need to choose an enciphering key, e, that is relatively prime to $\varphi(n) = (p-1)(q-1)$, the Euler phi function (the number of positive integers relatively prime to n but not greater than n). If our segment of plaintext is P_i, we define the enciphering function,

$$f(P_i) = P_i^e \pmod{n},$$

which creates a segment of ciphertext, C_i.

The deciphering function is constructed by first defining a number b as

$$b = [p-1, q-1],$$

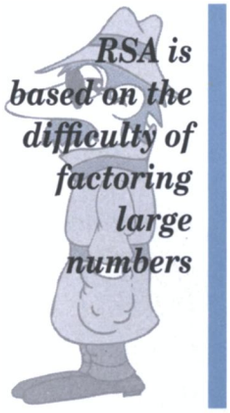
the least common multiple of $p-1$ and $q-1$. The deciphering key, d, is defined as the least positive solution of

$$e \cdot x \equiv 1 \pmod{b}.$$

Using d, the deciphering function is defined as

$$f^{-1}(C_i) = C_i^d \pmod{n},$$

which returns our plaintext segment, P_i.



In practice, to prevent unauthorized deciphering by powerful computers, p and q are about one hundred digits long, making $n = pq$ about two hundred digits long. Vanden Eynden (1987) describes a method that illustrates how RSA encryption works for smaller numbers, say, $p = 29$ and $q = 41$, with product $n = 1189$.

If Alice wants to send Bob a message, for example, she first needs to get Bob's encryption information: his enciphering key e_B and n. Bob has previously chosen $n = 1189$ and $e_B = 3$, which is relatively prime to $\varphi(1189) = 1120$. Usually, Bob's choices of n and e would be publicly available, possibly printed in some type of directory, but p and q are kept totally secret, even to Alice. Alice would then use any simple conversion to convert the message to numerical form and to break the resulting sequence into segments having fewer digits than n. For this example, we use a numerical conversion in which A converts to 01, Z converts to 26, and a space converts to 00. If, for example, Alice wants to send the message "MATHEMATICS," then the sequence of digits is

13 01 20 08 05 13 01 20 09 03 19.

Since $n = 1189$ has four digits, we break the message into three-digit blocks, resulting in the sequence $P_1, P_2, \ldots$ (P for plaintext)

130 120 080 513 012 009 031 900,

with two zeros appended to make the last block also three-digit.

At this stage, the plaintext blocks are enciphered using $f(P_i)$, resulting in $C_1, C_2, \ldots$ (C for ciphertext). Since n and e_B are public information, Alice can encipher her message for Bob. In this example, $f(P_i) = P_i^3 \pmod{1189}$ and the message is enciphered as shown in **figure 1.**

$P_1 = 130$	$f(P_1) = 130^3 \pmod{1189}$	$C_1 = 917$
$P_2 = 120$	$f(P_2) = 120^3 \pmod{1189}$	$C_2 = 383$
$P_3 = 80$	$f(P_3) = 80^3 \pmod{1189}$	$C_3 = 730$
$P_4 = 513$	$f(P_4) = 513^3 \pmod{1189}$	$C_4 = 692$
$P_5 = 12$	$f(P_5) = 12^3 \pmod{1189}$	$C_5 = 539$
$P_6 = 9$	$f(P_6) = 9^3 \pmod{1189}$	$C_6 = 729$
$P_7 = 31$	$f(P_7) = 31^3 \pmod{1189}$	$C_7 = 66$
$P_8 = 900$	$f(P_8) = 900^3 \pmod{1189}$	$C_8 = 320$

Fig. 1
Enciphering the message

Therefore, the enciphered message that Alice would send to Bob is

917 383 730 692 539 729 066 320.

This message seems to have little, if any, relationship to the original message.

After receiving Alice's message, Bob needs to decipher it. First, Bob computes $b = 280$ and $d_B = 187$. Bob can then decipher the message using $f^{-1}(P_i)$, producing $P_1, P_2, \ldots$. In this example, $f^{-1}(C_i) = C_i^{187} \pmod{1189}$ and the message is deciphered as shown in **figure 2.**

The result, which reproduces our original plaintext, is as follows:

130 120 080 513 012 009 031 900

$C_1 = 917$	$f(C_1) = 917^{187} \pmod{1189}$	$P_1 = 130$
$C_2 = 383$	$f(C_2) = 383^{187} \pmod{1189}$	$P_2 = 120$
$C_3 = 730$	$f(C_3) = 730^{187} \pmod{1189}$	$P_3 = 80$
$C_4 = 692$	$f(C_4) = 692^{187} \pmod{1189}$	$P_4 = 513$
$C_5 = 539$	$f(C_5) = 539^{187} \pmod{1189}$	$P_5 = 12$
$C_6 = 729$	$f(C_6) = 729^{187} \pmod{1189}$	$P_6 = 9$
$C_7 = 66$	$f(C_7) = 66^{187} \pmod{1189}$	$P_7 = 31$
$C_8 = 320$	$f(C_8) = 320^{187} \pmod{1189}$	$P_8 = 900$

Fig. 2
Deciphering the message

Regrouping results in

13 01 20 08 05 13 01 20 09 03 19.

Finally, converting back to letters, we get "MATHEMATICS," the original message.

The question next arises: Why does this process work? Namely, why does applying f^{-1} to our ciphertext segment, C_i, bring back the plaintext segment P_i? If we have plaintext segment P_i, the corresponding ciphertext C_i is defined as

$$f(P_i) = C_i \equiv P_i^e \pmod{n},$$

which is deciphered by computing

$$f^{-1}(C_i) = P_i' \equiv C_i^d \pmod{n}.$$

We would like to show that $P_i' = P_i$. Since they are both nonnegative numbers less than n, showing that

$$P_i' \equiv P_i \pmod{n}$$

will suffice. Using the definitions of C_i and P_i', we see that

$$P_i' \equiv C_i^d \equiv (P_i^e)^d \equiv P_i^{de} \pmod{n}.$$

We next let $de = 1 + kb$. If $(p, P) = 1$, then

$$P_i^p \equiv P_i \pmod{p}$$

and

$$P_i^{p-1} \equiv 1 \pmod{p}$$

by Fermat's little theorem, which states that if p is a prime number and a is any integer, then $a^p \bullet a \pmod{p}$. Then

$$P_i^{kb} \equiv 1 \pmod{p},$$

since $p - 1$ divides b. Multiplying both sides by P_i, we get

$$P_i^{kb+1} \equiv P_i \pmod{p}.$$

Thus,

$$P_i^{de} = P_i^{kb+1} \equiv P_i \pmod{p},$$

and this congruence is clearly true if p divides P_i. In the same way,

$$P_i^{de} \equiv P_i \pmod{q}.$$

Thus,

$$P_i^{de} \equiv P_i \pmod{n}$$

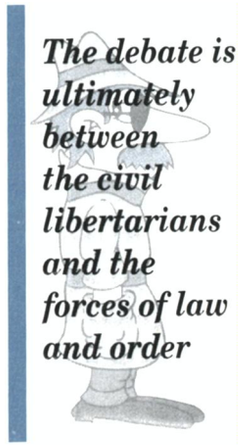
because if $(a, b) = 1$, then $z' \equiv z \pmod{a}$ and $z' \equiv z \pmod{b}$ if and only if $z' \equiv z \pmod{ab}$. Also, $P_i' = P_i$, since $P_i' \equiv P_i^{de} \pmod{n}$.

As previously stated, the RSA cryptosystem's security depends on the difficulty of factoring the large number n. As Vanden Eynden (1987, p. 142) indicates,

> a person trying to read the messages sent to us by factoring n will have to factor a number of 200 digits. . . . Even at one million operations per second, this will take about 10^{94} seconds, or about $3 \cdot 10^{86}$ years. . . . It turns out that even if the best methods presently known are used, it can be estimated that factoring a 200-digit number will take our imaginary computer about four billion years. By that time, we won't care who reads our mail.

This system is only as secure as the current factoring methods are slow and inefficient. If a much faster computer or more efficient factoring methods are developed, RSA will become obsolete.

The uses of the increased security of advanced cryptosystems like RSA have prompted an ethical debate about the needs of the public as opposed to the needs of the government. The growth of the Internet economy has vastly increased the amount of sensitive data passing through public telephone and computer lines every day. Consumers want to keep private information out of unauthorized hands. However, police and intelligence services have a legitimate need to secretly gather information on terrorists and organized crime groups. The type of strong encryption represented by RSA can render a wiretap useless. This debate is ultimately between the civil libertarians, who insist on the privacy of the individual, along with businesses, which want to guarantee the security of transactions, and the "forces of law and order," which want to keep strong cryptography out of public hands. Simon Singh asks, "Which do we value more—our privacy or an effective police force? Or is there a compromise?"(1999, p. xi).



Cryptography and the RSA algorithms are rich topics for mathematics classes on many levels. Gorini (1996) describes a student workshop she created that uses a simpler set of encryption and decryption keys and that allows students to send their own secret messages. This workshop would work very well in any class in which the students have discussed the laws of exponents and modular, or clock, arithmetic. A more in-depth discussion of the inner workings of RSA would be appropriate in an advanced high school or college class, where it could highlight one of the most important uses of number theory.

As we enter the twenty-first century, the Internet economy is booming. More and more private information will be broadcast through public lines. Such encryption systems as RSA use very simple but nonreversible mathematical operations to ensure the privacy of data. As Singh said, "[Cryptography] will provide the locks and keys of the information age" (1999, p. xi). Although G. H. Hardy thought that mathematics had nothing practical to offer to the world, RSA encryption has proved him wrong . . . even if it is an application of something that mathematicians cannot do.

(Continued on page 707)

Similarly, the key of D is inverted across C to

$$I_0(2) = [-2 - 4]_{12} = [-6]_{12} = [6]_{12} = F^\sharp.$$

We summarize these changes in **figure 18.** The keys of E (4) and B♭ (10) are invariant. We observe that the key changes produced by inverting about C can be visualized by a reflection across a line through E and B♭ on the circle of fifths, as shown in the first picture in **figure 19.** Likewise, we can easily verify that the key changes produced by inverting across any other note can be represented by a similar reflection across a line through the invariants. (Question: Why is it true that $I_{p+6}(x) = I_p(x)$?)

CONCLUSION

When people are asked how mathematics is generally used in the world, their responses usually have to do with the practical side of the discipline related to physics, engineering, business, and similar fields. Rarely do they think of the arts or music, since appreciation and invention within these domains are often considered to spring from the soul. People are always surprised to learn that most mathematicians would heartily agree that the soul is the wellspring of mathematical thought. Indeed, one might argue that the richness of the soul offers the most ideal environment for mathematics to send down its deepest roots. Why? As Edward Rothstein (1995, p. xv) said of his college days, "Music and math together satisfied a sort of abstract 'appetite,' a desire that was partly intellectual, partly aesthetic, partly emotional, partly, even, physical." The occurrence of patterns is the lifeblood of the permeation of mathematics through our existence, and nowhere are the creation and "feel" for patterns more prevalent than in the composition and enjoyment of music.

One thing he discovered . . . was that music held more for him than just pleasure. There was meat to it. What the music said was that there is a right way for things to be ordered so that life might not always be just tangle and drift but have a shape, an aim. It was a powerful argument against the notion that things just happen.

—Charles Frazier, *Cold Mountain*

BIBLIOGRAPHY

Apel, Willi, and Ralph T. Daniel. *The Harvard Dictionary of Music*. New York: Washington Square Press, 1960.

Berry, Wallace. *Form in Music*. Englewood Cliffs, N.J.: Prentice-Hall, 1966.

Brandt, William, Arthur Corra, William Christ, Richard DeLone, and Allen Winold. *Basic Principles of Music Theory: The Comprehensive Study of Music*. Vol. 6. New York: Harper & Row Publishers, 1980.

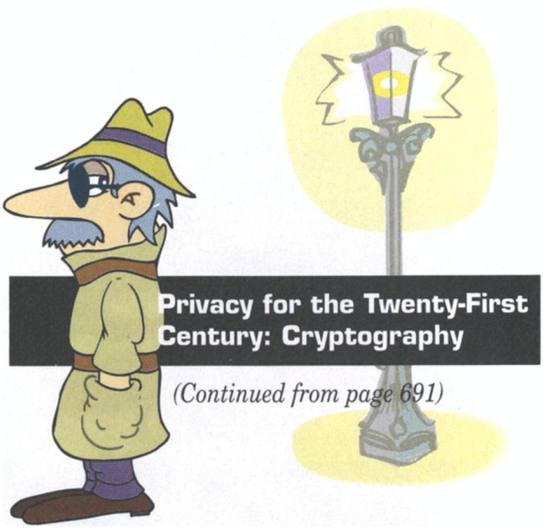
Mann, Alfred. *The Study of Fugue*. New Brunswick, N.J.: Rutgers University Press, 1958.

Maor, Eli. "What Is There So Mathematical about Music." *Mathematics Teacher* 72 (September 1979): 414–22.

Nallin, Walter E. *The Musical Idea*. New York: Macmillan Co., 1968.

Rothstein, Edward. *Emblems of Mind: The Inner Life of Music and Mathematics.* New York: Avon Books, 1995.

Schulenberg, David. *The Keyboard Music of J. S. Bach*. New York: Schirmer Books, 1992.



Privacy for the Twenty-First Century: Cryptography

(Continued from page 691)

REFERENCES

Diffie, Whitfield, and Martin E. Hellman. "New Directions in Cryptography." *IEEE Transactions on Information Theory.* Vol. IT-22, no. 6 (November 1976): 644–54.

Gorini, Catherine A. "Using Clock Arithmetic to Send Secret Messages." *Mathematics Teacher* 89 (February 1996): 100–104.

Hellman, Martin E. "The Mathematics of Public-Key Cryptography." *Scientific American,* August 1979, 146–57.

Kahn, Davis. *The Codebreakers: The Story of Secret Writing.* New York: Macmillan, 1967.

Must Read. *Wired,* October 1999a, 85–103.

Must Read. *Wired,* November 1999b, 99–116.

Singh, Simon. *The Code Book.* New York: Doubleday, 1999.

Vanden Eynden, Charles. *Elementary Number Theory.* New York: McGraw-Hill, 1987.

Zimmerman, Phillip R. "Cryptography for the Internet." *Scientific American,* October 1998, 110–15.