A Case for Encryption

Charles Hodgson

For journal editors concerned about the security of e-mailed documents, encryption provides increased confidentiality. Encryption programs create and validate digital signatures and provide for the encryption and decryption of signed data. Nevertheless, users must still take precautions, such as guarding their private keys and passwords and protecting paper copies of the documents.

This article provides a viewpoint of the technical aspects of security on the Internet. Although it does not analyze Professor Appel's specific system (see p 8), it does serve as background for the Dialogue discussion about the security risks of using e-mail for handling proprietary manuscripts.

GM Smith, Guest Editor

Editors of scientific journals must get referees and associate editors to provide prompt evaluations of technical papers. E-mail provides instantaneous communication in the world of global networking (1). The use of e-mail to transmit encrypted peer-reviewed manuscripts from point to point is more secure than traditional methods like the US Postal Service or private carriers.

Encryption, nothing more than a method to provide confidentiality (2), transforms data into a format that is unreadable without the secret decryption key. It ensures confidentiality by keeping the information hidden from anyone for whom it is not intended (3). Sending encrypted files by e-mail from point to point allows secured communication over an unsecured communications network.

The integrity of the encrypted e-mail data depends upon the authentication process. Authentication, whereby the receiver of an encrypted message can be confident of the identity of the sender and/or the integrity of the encrypted message (2), verifies the identity of the source of the data, the encrypted file's sender (3).

This article provides a nontechnical explanation of the use of encryption and e-mail in the peer-review process.

The security of a peer-reviewed manuscript from submission through final publication (Figure 1) is subject to casual security violations when traditional carriers and media or electronic communications are used without encryption. Casual in this context means that the security violator simply has to be in the right place at the right time with a minimal commitment of resources.

Overview of Traditional Carriers

1. An author completes a manuscript and prints out a hard copy that conforms to the particular journal's instructions to authors (Figure 1, image 1).
2. If the manuscript is mailed to the editor of the journal by means of a public or private carrier, it is subject to being lost or stolen without immediate detection, similar to the theft of a Social Security check. The private carrier, for instance, picks up the manuscript at 5 PM and promises delivery by 10 AM the following morning, but cannot promise that the manuscript will not be altered or copied by anyone who comes in casual contact with the manuscript anytime during the 17-hour interval between pickup and delivery (Figure 1, images 2 and 3).
3. The editor receives the manuscript and sends copies to the appropriate referees (Figure 1, images 3-5). Even at this point, a casual observer could remove the manuscript from the editor's desk, make copies, and return the manuscript without detection. The manuscript is also subject to being lost or stolen in transit.
4. In any event, the manuscript is vulnerable to security risks every time it sits on someone's desk or is transmitted through public or private carriers (Figure 1, images 3-7).

Overview of E-mail

1. An author completes a manuscript and e-mails an unencrypted copy to the editor of a journal. The manuscript conforms to the particular journal's instructions to authors (Figure 1, image 1).
2. Unencrypted, the e-mailed manuscript is subject to interception on unsecured electronic communications media.
3. The editor receives the manuscript and e-mails unencrypted copies to the appropriate referees (Figure 1, images 3-5). At this point, the unencrypted e-mailed manuscript is subject to interception.
4. In any event, the manuscript is vulnerable to security risks every time it is e-mailed without using encryption (Figure 1, images 3-7).

Discussion

Casual and not so casual security threats can be virtually eliminated when transmitting peer-reviewed manuscripts from point to point when commercially available encryption technology is used. Encryption is the process of taking plaintext (the actual message, text, data program, GIF file, and such that can be read, run, or viewed by anyone) and converting it into ciphertext (what the plaintext looks like after it is encrypted and is unreadable, unrunable, and unviewable, except by the person with the key to decrypt it) (1). The simplest encryption scenario requires that 1) both the sender and the receiver use the same encryption program and 2) the receiver can authenticate the identity of the sender.

Pretty Good Privacy (PGP) and Privacy Enhanced Mail (PEM) are both end-user oriented security tools that provide similar encryption features. The main function of PGP and PEM is to provide the creation and validation of digital signatures and, in addition, the encryption and decryption of signed data (4). PGP, developed by Philip Zimmermann, is the encryption program

CHARLES HODGSON *is a computer science instructor at the University of New Orleans and a project manager in the Information Services Division at Alton Ochsner Medical Foundation in New Orleans, Louisiana.*

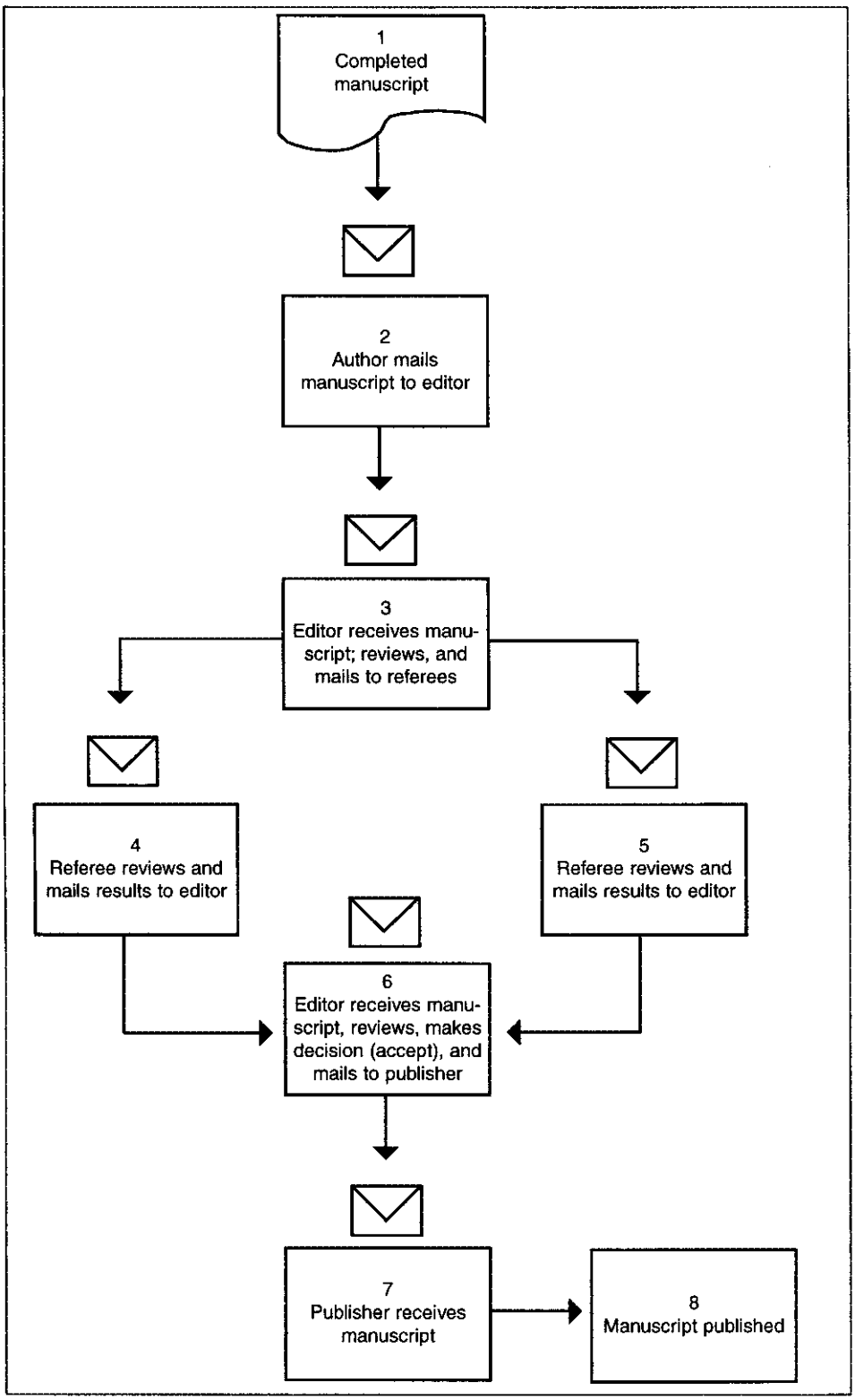

Figure 1 Course of a peer-reviewed manuscript by mail or unencrypted e-mail

used in this discussion and is a program that gives your e-mail something that it otherwise does not have—privacy. It does this by encrypting your e-mail so that no one but the intended person can read it. When encrypted, the plaintext message looks like a meaningless jumble of random characters (2). PGP and PEM uses asymmetric cryptography, which is an encryption system that uses different keys for encryption and decryption. The 2 keys have an intrinsic mathematical relationship to each other (2). PGP was selected because no central key server is required to authenticate keys.

Figure 2 illustrates the initial steps required to use PGP and e-mail to transmit and receive encrypted material electronically. The sender represents the author or the peer-reviewed manuscript, and the receiver represents the editor. The ideal scenario has both the sender and the receiver using the same version of PGP. To transmit a PGP encrypted manuscript, the sender and the receiver must create and validate digital signatures by each generating public and private keys (Figure 2, images 2 and 3). The public key is the part of PGP that is used to encrypt text and is the key that you give other people so they can send ciphertext to you that only you can read. The private or secret key is the part of PGP that is used to decrypt text and is the key that allows you and only you to read the ciphertext that was made by your public key. It is protected by your pass phrase (5).

The most secure generation of public and private keys requires the use of a non-networked or stand-alone computer because a computer on a network is vulnerable to unauthorized snooping. Hardware and software are available today that allow 1 party to monitor the activity and scan the storage devices of other networked workstations, but generation of keys on non-networked workstations render snooping hardware and software nearly worthless. PGP allows the user to define key size by selecting one of several options. The sender and the receiver should select the option that generates the largest key size, which is more than 1000

bits. The bigger the key, the better the security, making the code more difficult to crack by brute force because there is any one of 2^{128} possible key combinations, and only one would successfully decrypt all message blocks.

As an example, suppose a computer chip existed that could try a billion keys per second, although such a chip is far beyond anything that really could be developed today (6). With a billion of these super chips working on the problem at the same time, it still would require more than 10 trillion years to try all of the possible 2^{128} bit keys (6). While theoretically possible, the use of brute force is impractical and economically unfeasible.

During private-key generation, PGP requires the creation of a pass phrase that can be used only in combination with the private key. Both are required to decipher messages. A pass phrase is analogous to a PIN number, but is more secure because the phrase is not a single word or simple string of numbers but can be several sentences and contain any combination of characters. Standard password-security practices should render the private key useless if it falls into the wrong hands as long as the correct password is unavailable. For example, the pass phrase and the private key are never stored in the same place. Ideally, the private key should not be stored on any workstation's hard drive but on a write-protected diskette that is never out of the owner's possession. To this end, the public and private key combinations generated by PGP provide a high level of security.

To facilitate the exchange of an encrypted peer-reviewed manuscript, the sender and the receiver should exchange public keys, such as by e-mail (Figure 2, image 4). Before the sender uses the public key of the receiver to encrypt a manuscript for electronic transmission, security considerations necessitate using the public key only after its authenticity has been verified. A convenient way to verify authenticity is to call the public key's owner and read the key over the telephone (Figure 2, image 5) (7). The entire key can be read or just the key's fingerprint

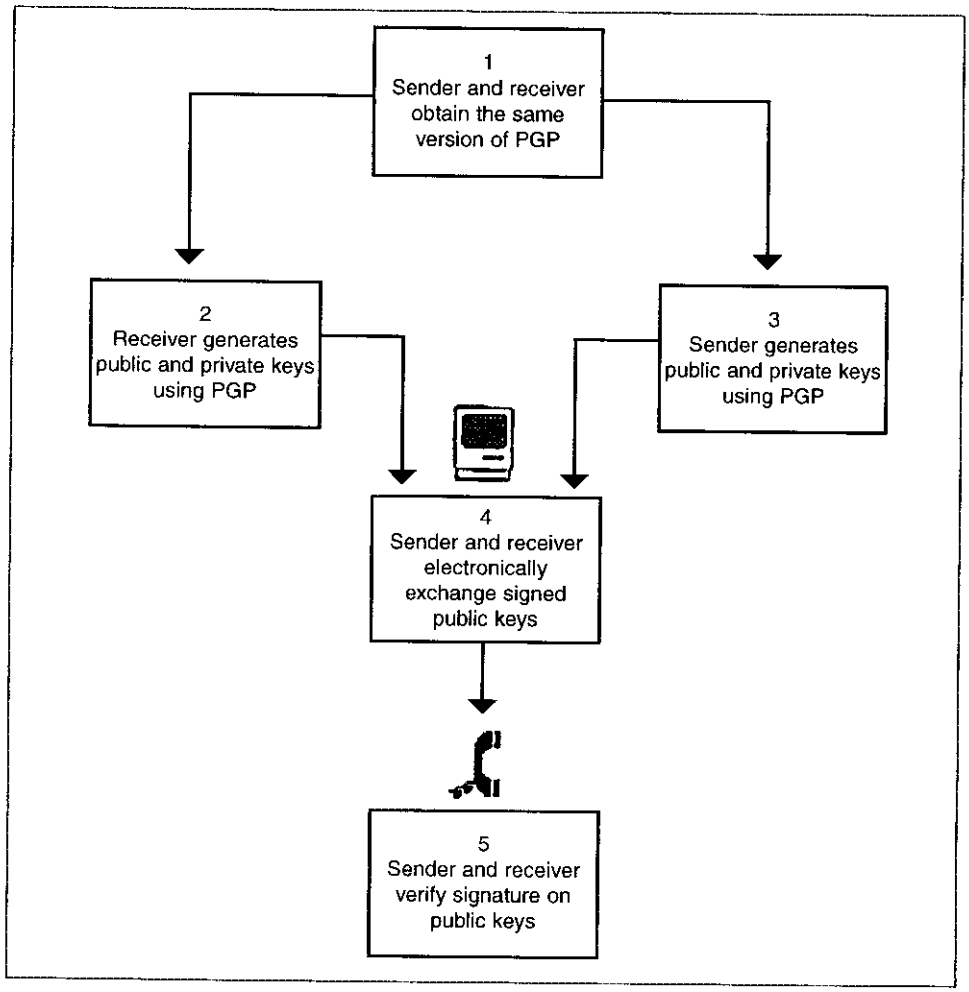

Figure 2 Creation and validation of digital signatures

as displayed by a PGP command. The fingerprint is a 16-byte digest of the public key components. Once verified, the sender can use the receiver's public key to transmit encrypted messages or manuscripts, which can be deciphered only by the verified owner of the public key. The authentication process occurs the 1st time a new public key is used.

In order to transmit a manuscript electronically, the sender must break it down into transmission packets (Figure 3, image 1) because most Internet service providers prohibit sending e-mail messages that are longer than 65 000 bytes. Consequently, longer messages must be broken into smaller chunks that can be mailed separately (8), which makes e-mail security superior to public or private carriers because the entire manuscript is sent to the editor in packets over a period of time. The increased security of separate packets is analogous to the use of separate mailings for a bank's customers to receive an ATM card and a PIN number. The bank uses separate mailings because if one is lost or stolen it is useless without the other.

After the manuscript is divided into packets, the sender compresses each by using PGPs or a commercially available compression utility, which the sender and the receiver both must have. Most cryptanalysis techniques exploit redundancies found in the plaintext to crack cipher. Data compression, however, reduces this redundancy in the

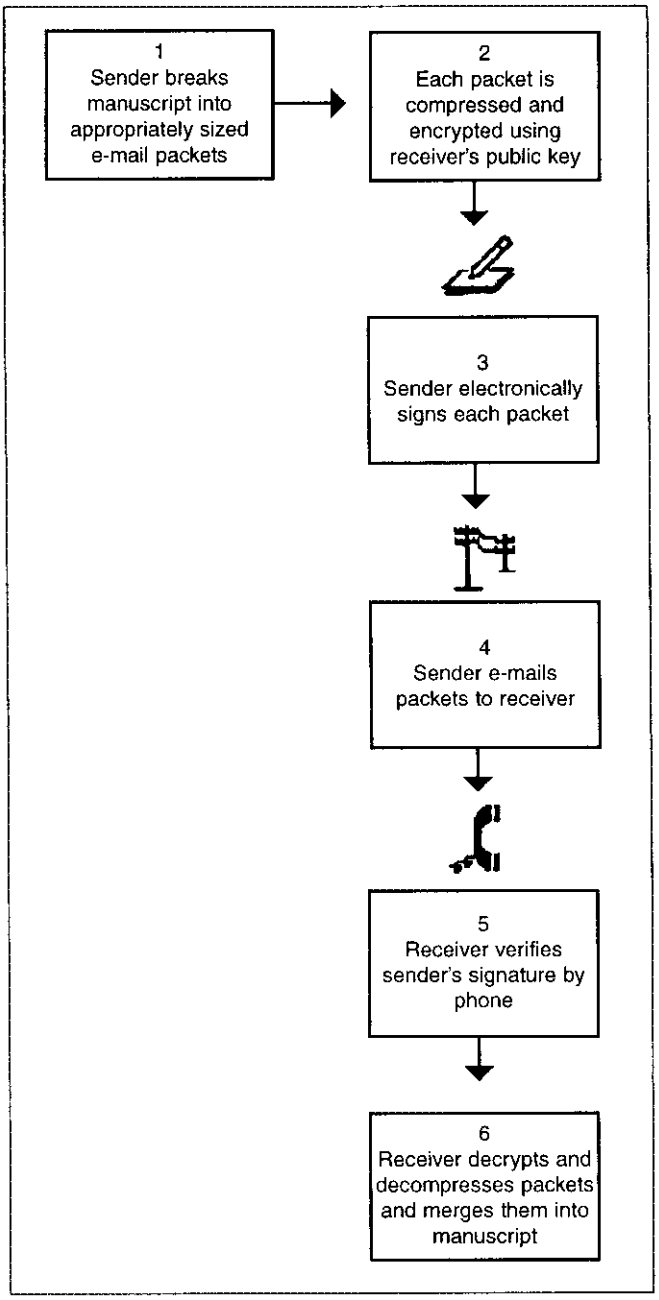

Figure 3 Encryption and de-encryption of a manuscript

plaintext, thereby greatly enhancing resistance to cryptanalysis (7).

The sender uses the receiver's public key to encrypt the packets (Figure 3, image 2), which can be deciphered only by using the private key. The sender also applies a digital signature, which is impossible to forge, to the encrypted packet to strengthen security (Figure 3, image 3). This signature is created by using the sender's private key. The receiver already has a copy of the sender's authentic public key and can use it to check the signature on the packet. It would be virtually impossible for anyone but the sender to have created the signature, since he or she is the only person with access to the private key and the pass phrase necessary to create the signature (6).

The sender e-mails the manuscript packets to the receiver (Figure 3, image 4), and the receiver phones or e-mails the sender to inform him or her that the packets have arrived (Figure 3, image 5). The elapsed time between sending and receiving e-mail packets versus sending and receiving manuscripts by public or private carriers is much shorter, greatly improving security of the peer-reviewed manuscript. When public or private carriers are used, hours can elapse before a security violation is discovered. The interception of an unencrypted manuscript by e-mail may never be discovered.

The receiver uses the sender's public key to verify the sender's digital signature, then uses his or her own private key to decipher the manuscript packets (Figure 3, image 6), which are decompressed and merged to form the entire manuscript.

The editor (sender) then e-mails the encrypted manuscript, via PGP, to the appropriate referees (receivers) for review. The sender and receiver exchange public keys and keep secret and secure their own private keys and associated pass phrases. After review, the referees return the manuscript to the editor by using PGP encryption (Figure 1, images 4, 5, and 6). The editor removes all references to the referee, encrypts the manuscript with referee comments, and e-mails the encrypted manuscript with comments to the author for modifications. The author decrypts the editor's e-mail containing the manuscript and the anonymous referee comments, modifies the manuscript, and begins the process again. The encrypted manuscript is returned to the editor. At this stage, the peer-reviewed manuscript is ready for publication. The editor and the publisher exchange a PGP-encrypted copy of the manuscript (Figure 1, images 6 and 7), and the publisher deciphers the manuscript and publishes it (Figure 1, image 8).

As long as the public keys are authenticated and the private key and pass phrase remain secure, casual security breaks are impossible and more sophisticated breaks are unlikely because of economic costs. The casual observer would not have easy access to remove a hard copy of the manuscript as long as it is encrypted and the private key and pass phrase required to decipher it remain secret. An electronic casual observer intercepting e-mail transmissions would not be able to read the manuscript without the appropriate keys for decryption. As stated earlier, with the use of e-mail the manuscript may never be transmitted as a single document, and the casual observer would have to electronically intercept multiple transmissions to acquire the entire manuscript in addition to deciphering the encryption.

Breaches

However, no data security system is impenetrable, and PGP can potentially be circumvented in a variety of ways, such as pass-phrase or private-key compromise, public-key tampering, files that are deleted but still remain on the disk, and electromagnetic emissions (8). As long as the receiver's

pass phrase and private key are not compromised, an intruder has no chance to decipher an encrypted message quickly and economically. Brute-force attacks would take years at enormous economic cost, and public-key tampering can be averted with a simple telephone call. Moreover, although the sender reads the receiver's public-key fingerprint for the receiver to verify, if the public key were ever compromised, the receiver simply regenerates a new public- and private-key combination and distributes the public key appropriately.

After encryption, the sender should delete the plaintext from his or her hard disk. However, even a casual observer with a utilities program such as Norton Utilities could recover the deleted manuscript. PGP can encrypt a plaintext file and remove all traces of the plaintext, rendering it unrecoverable. After PGP makes a ciphertext file, it can automatically overwrite the plaintext file and delete it. In this way, PGP leaves no trace of the plaintext file on disks.

Another kind of attack that has been used by well-equipped offenders involves the remote detection of the electromagnetic signals from a computer. An appropriately instrumented van can park near your computer's location and remotely pick up all of your keystrokes and messages displayed on your video screen. Such an attack can be thwarted by properly shielding all computer equipment so that no signals are emitted. This is an expensive and somewhat labor-intensive counterattack, but it would work (7). As long as the information is less valuable to the attacker than the cost of the attack, the chances that electromagnetic emissions will be monitored are low.

References

1. Appel AW. How to edit a journal by e-mail. Journal of Scholarly Publishing 1996;27(2): 82-99.
2. Haller N, Atkinson R. Internet authentication guidelines. ftp://saturn.darmstadt.gmd.de/pub/secude/Security/other/draft-haller-auth-requirements-03.txt. 14 February 1994.
3. Fahn P. Answers to frequently asked questions about today's cryptography. ftp://saturn.darmstadt.gmd.de/pub/secude/Security/other/draft-ietf-saag-cryptography-faq-00.txt. 22 September 1993.
4. Morton B. The beginner's guide to Pretty Good Privacy, version 1. http://netaccess.on.ca/^barclay/bg2pgp.txt. 13 April 1996.
5. Kolletzki S. Secure Internet banking with Privacy Enhanced Mail—a protocol for reliable exchange of secured order forms. http://www.darmstadt.gmd.de./TKT/Publications/bako/bako-doc.htm. 1996.
6. Licquia, J. Pretty Good Privacy—frequently asked questions. http://www.prairienet.org/^jalicqui/pgpfaq.txt. 1996.
7. Zimmermann P. PGP user's guide. Vol. I, Special topics. http://fglb.ord.org:8080/docs/pgp/pgpdoc2/pgpdoc2.html. 11 October 1994.
8. Zimmermann P. PGP user's guide. Vol. I, Essential topics. http://www.unicom.com/docs/pgp/pgpdoc2/pgpdoc2./html. 11 October 1994.

Information for *CBE Views* Contributors

- Submit manuscripts for the "Articles" section as 3 typed, double-spaced paper copies for peer review. A computer file of the final copy of accepted manuscripts is requested (preferably on a high-density 3-1/2" computer disk and as an ASCII file or a format readable by Microsoft Word (6.0) for Windows 95).
- Submit material for the "Features" and "CBE News" sections as 1 typed, double-spaced paper copy and, if possible, as an ASCII computer file on a disk or as an e-mail message.
- All submissions should include the phone and fax numbers and e-mail address of the corresponding author.
- All material should be in the style recommended by *Scientific Style and Format*, with references in the citation-sequence format.
- All material is subject to copyediting.

Send material and editorial inquiries to Martha Tacker, Editor, *CBE Views*, 704 228th NE, Suite 623, Redmond WA 98053; phone: 206-836-3284, fax: 206-836-3284; e-mail: tvnt30a@prodigy.com