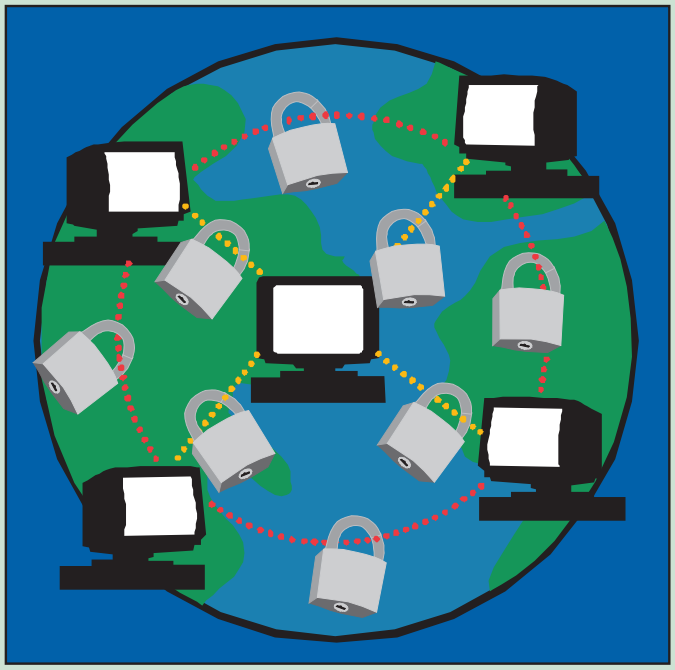
Securing Internet Communication

No one could shop, pay bills, or conduct business securely on the Internet without the mathematics of encryption. Although based on algebraic facts proved centuries ago, today's sophisticated encryption techniques were formulated within the past twenty-five years.

Public key encryption allows a user to publish the encryption key for all to use, while keeping the decryption key secret. One such algorithm, called RSA, is behind the encryption in modern browsers. The National Institute of Standards and Technology recently adopted an Advanced Encryption Standard that will be used for electronic communication in the years to come. This new standard uses permutations, modular arithmetic, polynomials, matrices, and finite fields to transmit information freely but securely.

For More Information:

"Communications Security for the Twenty-first Century," Susan Landau, *Notices of the American Mathematical Society*, April 2000.



AMS
American Mathematical Society

*The **Mathematical Moments** program promotes appreciation and understanding of the role mathematics plays in science, nature, technology, and human culture.*

www.ams.org/mathmoments