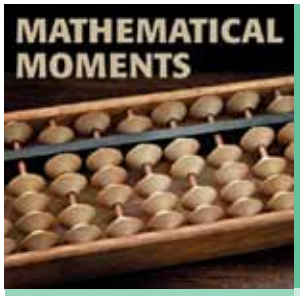
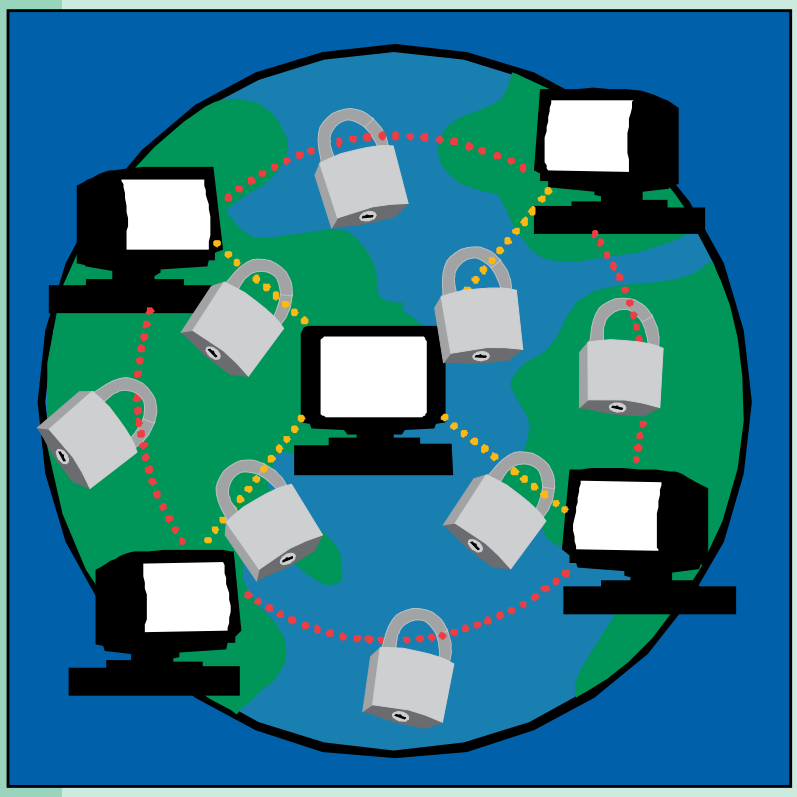


Asegurando la Comunicación por Internet

Nadie podría comprar, pagar cuentas o hacer negocios de manera segura sin las matemáticas de la criptografía. A pesar que está basada en resultados algebraicos probados hace siglos, las técnicas sofisticadas de cifrado de hoy en día fueron formuladas en los últimos veinticinco años.

El cifrado con clave pública permite al usuario publicar la clave de cifrado para que todos la usen, mientras mantiene la clave de descifrado en secreto. Uno de esos algoritmos, llamado RSA, es la base del cifrado en los navegadores de internet modernos. El Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology) ha adoptado recientemente un Estándar de Cifrado Avanzado que será usado en comunicación electrónica en los próximos años. Este nuevo estándar usa permutaciones, aritmética modular, polinomios, matrices y campos finitos para transmitir información de manera libre pero segura.



Para Mayor Información:

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

Traducción cortesía de Alan Veliz-Cuba y Betty Paredes-Alvarez, Virginia Polytechnic Institute and State University.

AMS
American Mathematical Society

*El programa **Momentos Matemáticos** promueve la apreciación y el entendimiento del rol que las matemáticas tienen en ciencia, naturaleza, tecnología y la cultura humana.*

www.ams.org/mathmoments

MM/4/SP