Por una comunicación más segura en Internet

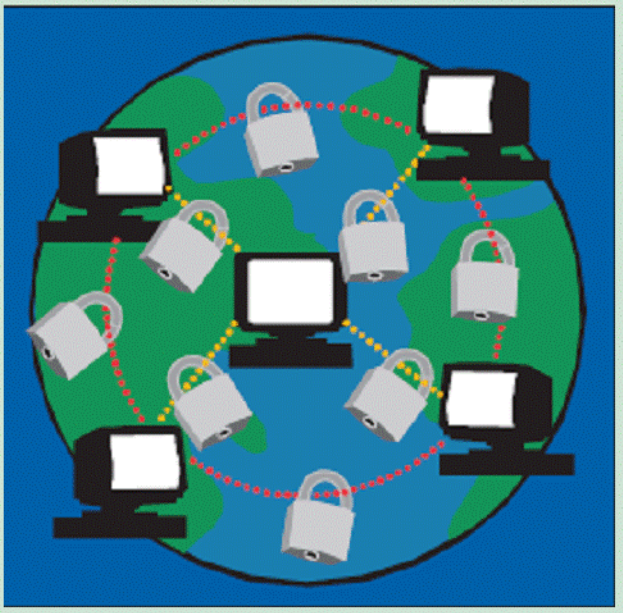
No podríamos comprar, pagar recibos o realizar negocios a través de Internet de una forma segura sin las matemáticas de la criptografía. Aunque están basadas en resultados algebraicos probados hace siglos, las sofisticadas técnicas actuales de cifrado han sido formuladas apenas en los últimos treinta años.

La criptografía de clave pública permite al usuario divulgar la clave de cifrado para que todos puedan usarla, pero manteniendo la clave de descifrado en secreto. Uno de estos algoritmos, denominado RSA, es el utilizado hoy para codificar los modernos navegadores de Internet.

El Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*, NIST) estadounidense ha adoptado un Estándar de Codificación Avanzado que se usará en las comunicaciones electrónicas en los próximos años. Este nuevo estándar usa permutaciones, aritmética modular, polinomios, matrices y campos finitos para transmitir la información de forma libre pero segura.

Más información:

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



AMS
American Mathematical Society

El programa ***Momentos Matemáticos*** *promueve la apreciación y el conocimiento del papel que desempeñan las matemáticas en la ciencia, la naturaleza, la tecnología y la cultura.*

www.ams.org/mathmoments

Versión en español de
www.matematicalia.net
REAL SOCIEDAD MATEMÁTICA ESPAÑOLA

matematicalia
revista digital de divulgación matemática

MM/4