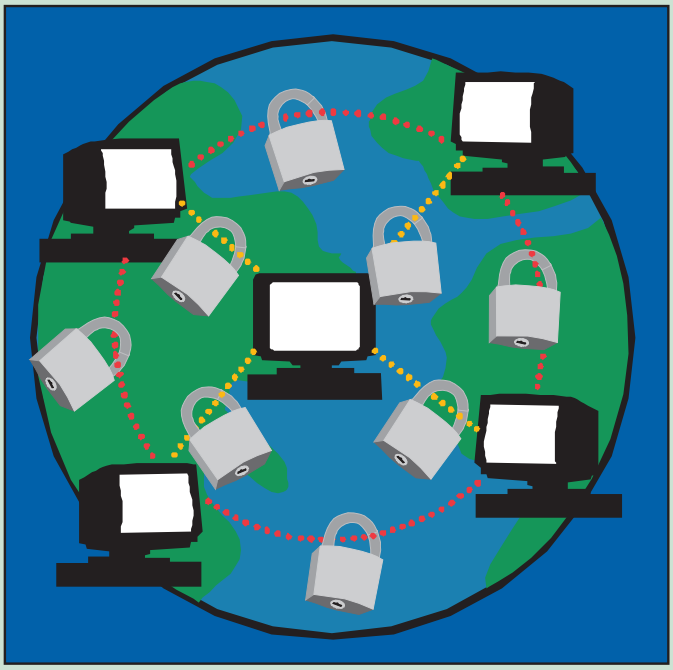
Internetkommunikation sicherer machen

Niemand könnte einkaufen, Rechnungen bezahlen oder Geschäfte sicher im Internet betreiben ohne die Mathematik der Verschlüsselung. Obwohl die Grundlagen heutiger ausgeklügelter Verschlüsselungstechniken auf algebraischen Tatsachen beruhen, die bereits vor Jahrhunderten bewiesen wurden, hat man sie erst innerhalb der letzten 25 Jahre formuliert.

Die Verschlüsselung mit öffentlichen Schlüsseln (sogenannte Public-Key-Verschlüsselung) erlaubt einem Nutzer, den Verschlüsselungsschlüssel für alle zur Verwendung zu veröffentlichen und gleichzeitig die Entschlüsselung geheim zu halten. Ein solcher Algorithmus, RSA genannt, steckt hinter der Verschlüsselung in modernen Browsern. Das „National Institute of Standards and Technology“ übernahm kürzlich einen fortgeschrittenen Verschlüsselungsstandard, der für elektronische Kommunikation in den kommenden Jahren Verwendung finden wird. Dieser neue Standard verwendet Permutationen, modulare Arithmetik, Polynome, Matrizen und endliche Körper, um Informationen frei aber sicher zu übertragen.



Für mehr Informationen:

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

AMS
American Mathematical Society

*Die **Mathematical Moments** sollen die Würdigung und das Verständnis der Rolle der Mathematik in Wissenschaft, Natur, Technologie und in der menschlichen Kultur fördern.*

Deutsche Übersetzung:
Mark Krüger, Kopernikus-Gymnasium Bargteheide

MM/4/GE

www.ams.org/mathmoments