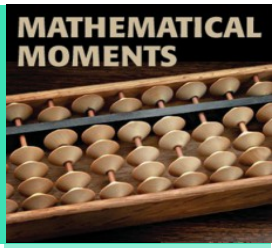

أمن اتصالات الانترنت

لن يتمكن أحد من التسوق أو تسديد الفواتير أو إبرام الصفقات التجارية عبر الإنترنت دون رياضيات علم التعمية والتشفير. مع أنها مبنية على حقائق في علم الجبر مبرهنة منذ عدة قرون إلا أن أنظمة التعمية المتطورة اليوم لم تتبلور إلا في الخمس وعشرين سنة الماضية.

تمكن أنظمة التعمية معلنة المفتاح المستخدم من إعلان مفتاح التعمية ليستخدمه الجميع للتعمية مع الإبقاء على مفتاح فك التعمية سرياً. أحد هذه الأنظمة يسمى RSA وهو المبني عليه عمليات التعمية والتشفير في المتصفحات الحديثة. وقد تبنى المعهد الوطني للمعايير والتكنولوجيا معياراً متقدماً للتعمية ليتم استخدامه في الاتصالات الالكترونية في السنوات القادمة. هذا المعيار الجديد يستخدم التباديل والحساب المقياسي modular arithmetic وكثيرات الحدود والمصفوفات والحقول المنتهية لنقل المعلومات بحرية وأمان.

ترجمة: د. .فهد بن مبارك الشمري، الجمعية السعودية للعلوم الرياضية

لمزيد من المعلومات:

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