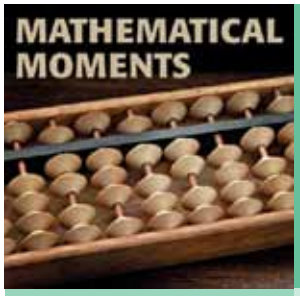


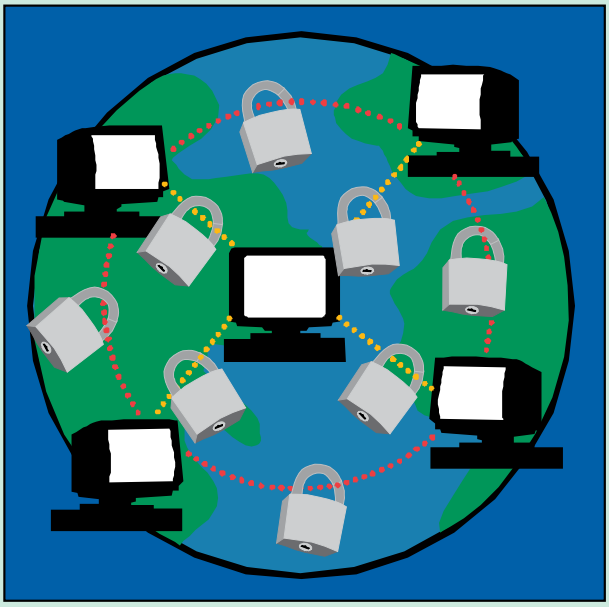
Sécuriser les communications Internet

Personne ne pourrait magasiner, payer des factures, ou faire affaire sur Internet de façon sécuritaire sans les mathématiques de cryptage. Bien qu'elles soient basées sur des résultats algébriques démontrés il y a plusieurs siècles, les techniques sophistiquées de cryptage moderne ont été développées au cours des vingt-cinq dernières années.

Le cryptage à clé publique permet à un utilisateur de publier la clé de chiffrement pour l'usage de tous tout en gardant sa clé de décryptage secrète. Un tel algorithme, appelé RSA, se cache derrière le chiffrement dans les fureteurs web modernes. L'agence américaine National Institute of Standards and Technology a récemment adopté un standard avancé de cryptage qui sera utilisé pour les communications électroniques dans les années à venir. Ce nouveau standard fait usage de permutations, d'arithmétique modulaire, de polynômes, de matrices et de corps finis, toujours dans le but de transmettre de l'information librement, mais de façon sécuritaire.

Pour plus de renseignements: "Communications Security for the Twenty-first Century," Susan Landau, *Notices of the American Mathematical Society*, avril 2000.

Traducteur: Hugo Drouin-Vaillancourt



AMS
American Mathematical Society

*Le programme **Mathematical Moments** a pour but de promouvoir l'appréciation et la comprehénsion du rôle que jouent les mathématiques dans la science, dans la nature, dans la technologie et dans la culture humaine.*