# La cryptographie pour les nuls

**Dominique Forget**

Photo : Denis Bernier

**François Bergeron, professeur au Département de mathématiques.**

«Wrxwh od jdxoh hvw rffxshh». D'après vous, que signifie cette phrase? Vous croyez que c'est du charabia? Détrompez-vous! François Bergeron, professeur au Département de mathématiques, pourra la déchiffrer en quelques minutes à peine. «La clé est facile à trouver, affirme-t-il. Les lettres ont simplement été remplacées par celles situées trois rangs plus loin dans l'alphabet. C'est un très vieux code, mis au point par Jules César pour communiquer avec ses lieutenants.»

Une fois qu'on connaît le truc, il est facile de retracer le message original, en l'occurrence : «toute la Gaule est occupée.» Comme l'explique M. Bergeron, il existe plusieurs variantes du code César. On peut en effet faire correspondre les lettres à n'importe quel chiffre ou symbole. Mais peu importe le subterfuge, l'expéditeur contemporain ne pourra guère compter sur la confidentialité de son message. «Les scientifiques ont mis au point des algorithmes mathématiques et des logiciels qui permettent de décrypter en un tournemain ce type de message. Ils sont basés sur la fréquence d'apparition des lettres dans chacune des langues. En français par exemple, on sait que le E est la lettre la plus fréquemment utilisée.»

Les secrets de la cryptographie, François Bergeron les connaît presque tous. Le professeur cultive une véritable passion pour cette matière qui, à son avis, constitue une des très belles applications des mathématiques. Pour partager cette beauté avec le grand public, le professeur met actuellement la touche finale à un nouveau cours, en collaboration avec son collègue Alain Goupil. Fait intéressant : bien qu'il reposera sur des notions de statistiques, de probabilité et de calcul, le cours ne requerra aucune connaissance mathématique. Bienvenue aux néophytes.

## De l'Antiquité à aujourd'hui

Le cours de M. Bergeron abordera, entre autres, l'histoire de la cryptographie, de l'antiquité à nos jours. «Plusieurs personnages célèbres ont eu recours à la cryptographie pour transmettre des messages secrets, raconte M. Bergeron. Par exemple, George Sand et Alfred de Musset s'envoyaient des lettres où, si on ne lisait qu'une ligne sur deux, on découvrait un message pour le moins osé…»

On raconte aussi que la deuxième guerre mondiale aurait été gagnée non seulement grâce aux armes ou aux combattants, mais aussi grâce à des mathématiciens qui auraient percé le code employé par les Allemands pour communiquer avec leurs troupes. «La guerre aurait sûrement duré beaucoup plus longtemps si on n'avait pas réussi à déchiffrer les messages captés sur les ondes radio», explique M. Bergeron.

Bien entendu, les toutes dernières percées au chapitre de la cryptographie seront aussi abordées dans le cadre du cours. «Les transactions effectuées par Internet ont obligé les mathématiciens à mettre au point des façons d'encoder beaucoup plus performantes, entre autres pour les chiffres des cartes de crédit, on a trouvé une opération très simple. On élève la série de chiffres à encoder à la puissance d'un très grand nombre. La réponse est évidemment astronomique. Mais une seconde opération permet de la ramener à un petit chiffre.» Ce type d'encodage ne prend que quelques secondes. Mais pour faire l'opération inverse, un ordinateur mettrait une centaine d'années… sauf si on lui livre la clé.

## Maths pour tous

François Bergeron espère attirer des étudiants de toutes les facultés à son cours qui sera peut-être offert à la session d'automne 2004, sinon à l'hiver 2005. «Le cours sera donné sur une note légère et amusante, souligne-t-il. Tous les étudiants pourront y trouver leur compte. Après tout, les histoires de mystère et d'espionnage intéressent tout le monde.»

Pour le mathématicien, il s'agit d'une chance unique de donner aux mathématiques une nouvelle image. «Les maths sont enseignées de façon très ennuyante à l'école. On ne parle jamais que d'une toute petite partie des mathématiques. C'est un peu comme si on enseignait le français en ne faisant lire que le dictionnaire aux étudiants, sans jamais leur faire découvrir la littérature, le théâtre ou le cinéma.»

Pourtant, selon François Bergeron, les mathématiques sont partout autour de nous. On fait des maths à chaque jour et on ne le réalise pas. «Il est possible de rendre cette science passionnante pour le grand public. C'est ce que je compte démontrer avec mon cours.» ●