Cryptage et décryptage : communiquer en toute sécurité

Jean-Louis Nicolas, *professeur à l'Université Claude Bernard Lyon 1*
Christophe Delaunay, *professeur à l'Université de Franche-Comté*

La sécurisation de nos cartes bleues, ainsi que d'autres procédés de cryptages utilisés couramment, se basent sur l'impossibilité, en pratique, de factoriser de très grands nombres. Ce type de cryptage pourrait cependant être détrôné par d'autres méthodes, sa fiabilité étant sans cesse remise en question par les progrès de l'informatique.

En mars 2000, un gros titre avait fait la une des journaux : « Alerte à la sécurité des cartes bancaires ». Que s'était-il passé ? En France, le secret des cartes à puce était protégé depuis 1985 grâce à une méthode de cryptage faisant intervenir un grand nombre N, constitué de 97 chiffres. Ce nombre N doit être le produit de deux grands nombres premiers, c'est-à-dire de nombres qui, comme 7 ou 19, ne sont divisibles que par 1 et par eux-mêmes. Le secret d'une carte bancaire est constitué précisément par ce couple de nombres premiers ; les calculer à partir de N était pratiquement impossible dans la décennie 1980. Mais avec l'augmentation de la puissance des ordinateurs et l'amélioration des méthodes mathématiques, la taille des nombres N dont on peut calculer les facteurs premiers en un temps raisonnable a dépassé la centaine de chiffres dans les années 1990 (le record actuel, obtenu en décembre 2009, est la factorisation d'un nombre de 232 chiffres). Ainsi, un informaticien astucieux, Serge Humpich, avait pu trouver les deux nombres premiers ultra-secrets dont le produit valait le nombre N d'alors. Pour garantir la sécurité de nos petits rectangles de plastique, l'organisme de gestion des cartes ban-

caires avait été obligé de construire aussitôt de nouveaux nombres N, nettement plus grands. La page web de Paul Zimmerman (voir les références en fin d'article) offre une mise à jour des différents records de factorisation des entiers.

La taille des nombres N dont on peut calculer les facteurs premiers en un temps raisonnable a dépassé la centaine de chiffres dans les années 1990.

La cryptographie moderne, au croisement des mathématiques et de l'informatique

Cette péripétie illustre l'importance considérable que revêt aujourd'hui la science du cryptage, c'est-à-dire du codage de messages en vue de les rendre illisibles par des personnes indiscrètes. Crypter et décrypter des messages secrets est une activité vieille de plusieurs siècles, voire millénaires. Et cette activité a largement débordé du cadre strictement diplomatique ou militaire pour investir des pans entiers de l'univers des communications civiles : procédures d'authentification, transactions bancaires, commerce électronique, protection de sites et fichiers informatiques, etc.

La cryptographie a connu beaucoup d'avancées au cours des dernières décennies. Ce faisant, elle est devenue une science complexe, où les progrès sont généralement le fait de spécialistes ayant reçu une formation poussée en mathématiques et en informatique.

Cette spécialisation s'est manifestée dès la Deuxième guerre mondiale. On le sait aujourd'hui, le déchiffrage par les Alliés des messages codés par les fameuses machines allemandes Enigma a joué un rôle déterminant dans ce conflit. Or c'est un éminent mathématicien britannique, Alan Turing, par ailleurs l'un des pères de l'informatique théorique, qui a apporté une contribution essentielle à ce décryptage.

Dans les années 1970, la cryptographie a connu une petite révolution : l'invention de la cryptographie à « clé publique », avec la méthode RSA. De quoi s'agit-il ? Jusque-là, les correspondants voulant échanger des messages secrets devaient partager une clé secrète, et le risque d'interception de cette clé par l'ennemi était grand. Le protocole RSA, nommé ainsi d'après ses trois inventeurs (Ronald Rivest, Adi Shamir et Leonard Adleman), résout ce problème. Cette méthode utilise deux clés : une clé de

cryptage publique – elle peut être connue de tous – et une clé de décryptage, qui reste secrète. Elle est fondée sur le principe (utilisé par la suite pour protéger les cartes bancaires, comme on l'a vu plus haut) qu'il est possible de construire de grands nombres premiers (de cent, mille chiffres, voire plus), mais qu'il est extrêmement difficile de retrouver les facteurs premiers p et q d'un grand nombre $N = p \times q$ lorsque l'on connaît seulement N. Schématiquement, la connaissance de N revient à celle de la clé publique de cryptage, tandis que la connaissance de p et q revient à celle de la clé secrète de décryptage.

Évidemment, si quelqu'un trouvait une méthode pour décomposer rapidement en leurs facteurs premiers de grands nombres, le protocole RSA deviendrait caduc. Mais il se pourrait aussi que les mathématiciens prouvent qu'une telle méthode n'existe pas, ce qui renforcerait la sécurité du protocole RSA. Ce sont là des sujets de recherche décisifs.

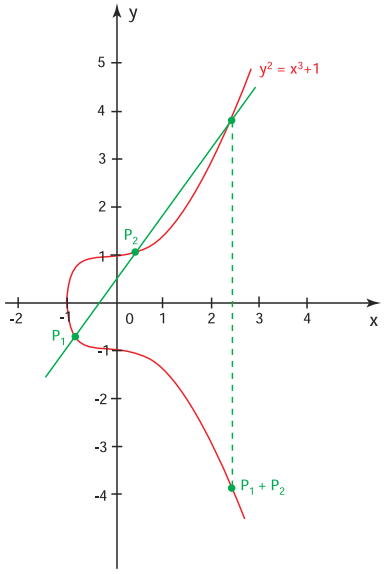
Les méthodes qui, comme le protocole RSA, font intervenir de la théorie des nombres élaborée, apportent une grande leçon : des recherches mathématiques (sur les nombres premiers notamment) tout à fait désintéressées peuvent se révéler, des années ou des décennies plus tard, cruciales pour telle ou telle application ; et ce de manière imprévisible.

Dans son livre *L'apologie d'un mathématicien*, le grand théoricien des nombres britannique G. H. Hardy (1877-1947), qui était un fervent pacifiste, se targuait de travailler dans un domaine parfaitement pur, l'arithmétique, et de n'avoir rien fait qui puisse être considéré comme « utile ». Ses travaux étaient peut-être « inutiles » à son époque. C'est faux aujourd'hui.

Courbes elliptiques : la géométrie algébrique au service des agents secrets

Et cela ne concerne pas uniquement la théorie des nombres. D'autres domaines des mathématiques, auparavant considérés comme dépourvus d'applications, contribuent à la science du cryptage. Des méthodes cryptographiques prometteuses et fondées sur des principes voisins de ceux du protocole RSA sont apparues au cours des dernières années. Il en est ainsi de la méthode dite du *logarithme discret*. Celle-ci a servi à son tour à concevoir des méthodes qui s'appuient sur les propriétés des *courbes elliptiques*. Il ne s'agit pas de courbes ayant la forme d'une ellipse, mais de courbes dont l'étude a débuté au XIX^e^ siècle pour résoudre

le problème difficile du calcul du périmètre d'une ellipse. Ces courbes, dont les coordonnées (x, y) de leurs points vérifient une équation de la forme $y^2 = x^3 + ax + b$, ont d'intéressantes propriétés – dont l'étude fait partie de la *géométrie algébrique*, très vaste domaine des mathématiques actuelles. Par exemple, à l'aide d'une construction géométrique appropriée, il est possible de définir une addition entre les points d'une courbe elliptique (voir figure ci-dessous).



Le graphe de la courbe elliptique d'équation $y^2 = x^3 + 1$. Les courbes elliptiques ont une propriété remarquable : on peut « additionner » leurs points selon le procédé représenté sur le dessin. L'« addition » ainsi définie respecte les lois arithmétiques attendues, telles que $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$. Certaines méthodes modernes de cryptographie font appel aux courbes elliptiques et à leurs propriétés algébriques.

Plus généralement, les objets géométriques que sont les courbes elliptiques possèdent des propriétés arithmétiques – que l'on continue d'explorer – susceptibles de rendre service à la cryptographie. C'est ainsi qu'a été développée une méthode cryptographique intitulée *logarithme discret sur les courbes elliptiques*. De façon anecdotique, les courbes elliptiques fournissent aussi une méthode originale pour factoriser les entiers (cependant, des méthodes bien plus techniques sont nécessaires pour obtenir les records actuels).

Les objets géométriques que sont les courbes elliptiques possèdent des propriétés arithmétiques susceptibles de rendre service à la cryptographie.

L'ordinateur quantique : l'outil de demain ?

Une autre direction, totalement différente, est apparue assez récemment. Il s'agit de la cryptographie quantique. Que signifie ce terme ? Il y a quelques années, des physiciens et des mathématiciens ont imaginé qu'il serait un jour possible de réaliser un ordinateur quantique, c'est-à-dire dont le fonctionnement exploiterait les lois bizarres de la physique quantique, celles qui règnent dans le monde infiniment petit. Or, on s'est rendu compte qu'un tel ordinateur, s'il était réalisable, serait capable de factoriser très vite de grands nombres et rendrait ainsi totalement inefficace la méthode RSA (dans ce contexte, lors du congrès international des mathématiciens à Berlin en 1998,

Peter Shor, des laboratoires AT & T, obtenait le prix Nevanlinna pour ses travaux sur la factorisation à l'aide des ordinateurs quantiques). Des recherches visant la réalisation concrète d'un ordinateur quantique ont d'ailleurs été publiées dans la revue britannique *Nature* (cf. référence ci-dessous). D'un autre côté, des chercheurs ont élaboré des protocoles de cryptographie quantique, c'est-à-dire des méthodes de cryptage utilisant des objets (photons, atomes…) obéissant aux lois de la physique quantique. Ces protocoles quantiques garantissent (du moins théoriquement) une sécurité infaillible. Tout cela est à l'étude et risque de devenir opérationnel dans un futur proche (par exemple, un câble de communication quantique reliant la ville de Genève à Lausanne fonctionne déjà depuis plusieurs années…).

Pour aller plus loin

La page web de Paul Zimmerman sur les records de factorisation des entiers : www.loria.fr/~zimmerma/records/factor.html

Kahn D., (1980). *La guerre des codes secrets* (Interéditions).

Stern J., (Jacob O. 1998). *La science du secret*.

Singh S., (Lattès J.-C., 1999) *Histoire des codes secrets.*

Delahaye J.-P., (2000). *Merveilleux nombres premiers* (Belin/Pour la Science).

Stinson D. (Vuibert, 2001). *Cryptographie, théorie et pratique*.

Vandersypen L. M. K., *et al.*, (2001) *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature*, vol. 414, p. 883-887.