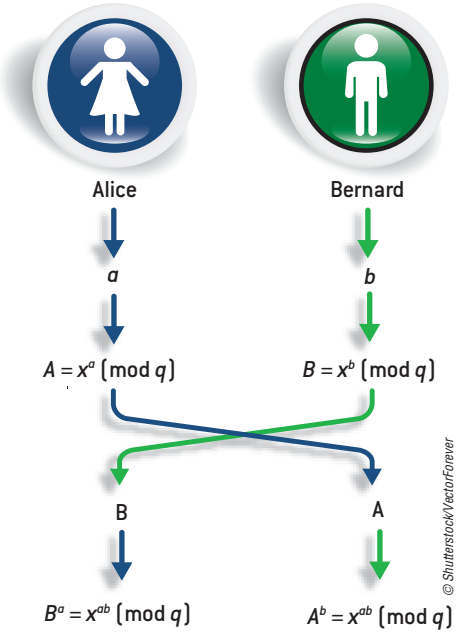

© Shutterstock/VectorForever

3. LE PRINCIPE DE L'ÉCHANGE entre deux correspondants, nommés Alice et Bernard, permettant de définir en toute sécurité un secret commun représenté par $x^{ab} \pmod q$ (où q est le cardinal d'un corps fini et x une « racine primitive » de ce corps), les données x et q étant publiques.

Pour obtenir un protocole asymétrique pratique et fiable, il faut que la fonction de codage soit facile à calculer, mais qu'au contraire la fonction de décodage soit difficile à calculer si l'on ignore le code secret, même si l'on connaît la fonction de codage. Dans le cas d'une généralisation du chiffre de César où l'on permuterait les lettres d'une façon plus subtile qu'un simple décalage, il suffirait de 24 essais (le nombre de lettres de l'alphabet latin) pour savoir à quelle lettre correspond une lettre chiffrée. Cela prendrait donc juste un peu plus de temps de déchiffrer un message que de le crypter.

Mais lorsque l'ensemble des messages est très grand (10^{100} éléments, par exemple), il devient impossible de coder tous les messages possibles en espérant tomber sur un message chiffré donné : cela prendrait plus de temps que la durée de vie du Système solaire !

Face à ce problème, l'algèbre est potentiellement très utile, car se donner une formule est une façon très économique de définir une application, même entre ensembles gigantesques, et les corps finis fournissent de façon naturelle de tels ensembles tout en étant très faciles à construire.

LA THÉORIE DE GALOIS IRRIGUE

une grande partie des mathématiques d'aujourd'hui, de la théorie des nombres à celle des équations différentielles.

Dans cet ordre d'idées, expliquons comment, suivant W. Diffie et M. Hellman, deux individus, que nous appellerons Alice et Bernard, peuvent convenir d'un code secret même si Charles espionne leur conversation.

Pour cela, nos deux amis choisissent un corps fini, de cardinal q, ainsi qu'une racine primitive x (c'est-à-dire un élément x tel que la suite 0, 1, x, x^2, ..., x^{q-2} décrive tous les éléments du corps).

Alice et Bernard commencent par choisir chacun un nombre entier compris entre 1 et $q - 1$, sans le divulguer. Supposons qu'Alice ait choisi l'entier a et que Bernard ait choisi l'entier b. Alice communique alors à Bernard la valeur de x^a, tandis que Bernard communique à sa correspondante la valeur de x^b. Il est important de remarquer que, bien que x^a soit défini comme le produit de a facteurs égaux à x, un tel produit peut être calculé très rapidement *(voir page 28, en haut)*. Alice calcule alors $(x^b)^a$ dans le corps fini, et Bernard calcule $(x^a)^b$. Ainsi, les deux ont pu calculer l'élément x^{ab}, qui sera leur secret commun *(voir la figure 3)*.

Imaginons que Charles ait espionné tout l'échange entre Alice et Bernard ; il connaît donc x, x^a et x^b. L'efficacité du système repose sur le fait que personne ne sait efficacement calculer x^{ab} à partir de ces données. Une solution consisterait à retrouver la valeur de a ; c'est ce qu'on appelle le problème du « logarithme discret », a étant en quelque sorte le logarithme en base x de x^a. La méthode évidente pour ce faire consiste à calculer successivement x^2, x^3, etc., jusqu'à ce qu'apparaisse la valeur x^a ; mais, si a est choisi très grand, elle n'a aucune chance d'aboutir avant l'extinction du Soleil... Il existe cependant d'autres méthodes, plus subtiles et un peu plus efficaces. Pour que le système de communication secrète soit sûr, l'existence de ces méthodes impose que $q - 1$ ait au moins un facteur premier de très grande taille.

On gagne un peu en sécurité et en souplesse en remplaçant le calcul dans un corps fini par un calcul dans une structure algébrique plus compliquée. L'une des méthodes en vue consiste à utiliser le groupe des points d'une courbe elliptique définie sur un corps fini *(voir l'encadré page 28 et les figures 1 et 2)*. En d'autres termes, on se donne un corps fini assez grand F, une courbe elliptique E définie par une équation dont les coefficients appartiennent à F et un point P de cette courbe (dont les coordonnées appartiennent à F). L'intérêt des courbes elliptiques est que l'on peut y définir une addition entre points. Comme précédemment, Alice et Bernard choisissent des entiers a et b, calculent l'une aP et l'autre bP ; leur secret commun est le point (ab)P de la courbe E.

De tels protocoles sont implantés dans tous les systèmes de télécommunications modernes et témoignent de l'actualité de l'œuvre de Galois. Mais l'héritage de Galois est loin de se réduire au cryptage et au codage de données. Ce que l'on nomme aujourd'hui théorie de Galois est un édifice complexe qui irrigue une bonne partie des recherches mathématiques modernes, de la théorie des nombres à celle des équations différentielles, en passant par la géométrie algébrique et le programme de Langlands, dont la démonstration du célèbre théorème de Fermat constitue une retombée. ■

✔ BIBLIOGRAPHIE

N. Verdier, **Galois, le mathématicien maudit**, Belin-Pour la Science, 2011.

C. Ehrhardt, **Évariste Galois, la fabrication d'une icône mathématique**, Éditions de l'EHESS, à paraître, octobre 2011.

P. Pesic, **Abel, Galois et les équations algébriques**, *Pour la Science*, n° 366, avril 2008.

R. Langlands, **Le programme de Langlands**, *Pour la Science*, n° 361, novembre 2007.

A. Chambert-Loir, **Algèbre corporelle**, Éditions de l'École Polytechnique, 2005.

L'art du secret, *Dossier Pour la Science*, n° 36, juillet-octobre 2002.