Mathématiques et secrets *

Nicolas Billerey

« Nous nous trouvons aujourd'hui à l'aube d'une révolution en cryptographie ». C'est ainsi que Whitfield Diffie et Martin Hellman débutent leur article *New Directions in Cryptography* publié en 1976 [1]. Pour mieux cerner les contours de cette rupture dans la « science du secret », il est sans doute utile de rappeler ici brièvement les mécanismes de la cryptographie conventionnelle. Dans un premier temps, expéditeur et destinataire (auxquels la tradition cryptologique a attribué les noms d'Alice et Bob) s'échangent via un canal sécurisé une clé secrète commune. C'est elle qui sert au premier à chiffrer le message qu'il souhaite transmettre autant qu'au second à le déchiffrer. La sécurité du système repose sur le fait qu'un espion qui ne connaît pas cette clef ne peut décrypter un message intercepté autrement que par des moyens détournés.

Pour ingénieuses et sophistiquées que soient les découvertes cryptographiques jusqu'en 1976, elles n'en fonctionnent pas moins toutes sur ce même principe. C'est ainsi le cas des chiffres de César ou de Vigenère décrits dans l'article *Blaise de Vigenère, diplomate et érudit bourbonnais* (ce volume) comme plus récemment de la fameuse machine Enigma utilisée par les Allemands durant la seconde guerre mondiale.

Au début des années 1970 cependant, l'extraordinaire développement des télécommunications, la multiplication vertigineuse des ordinateurs et la diminution du coût des outils informatiques ont largement contribué à l'émergence de besoins cryptographiques nouveaux dans lesquels l'échange de clés via des canaux parfaitement sécurisés est devenu impraticable. Si l'emploi de valises diplomatiques peut encore convenir aux communications secrètes entre une administration et ses antennes, on voit mal en effet comment relier par des canaux sécurisés tous les ordinateurs répartis aux quatre coins de la planète. Au point d'ailleurs que, comme l'écrivent les deux chercheurs, l'inadéquation de la cryptographie conventionnelle à ces nouveaux défis pourrait mettre en

*Le titre de cet article, comme d'ailleurs une partie substantielle de son contenu, s'inspirent de l'ouvrage *La science du secret* (Éd. Odile Jacob, 1998) du cryptologue français Jacques Stern.

1. IEEE Transactions on Information Theory **22** (6) : 644-654.

péril « beaucoup des bénéfices des télécommunications ». Quelle valeur aurait en effet un courrier électronique par rapport à un courrier papier s'il n'était ni authentifiable, ni confidentiel ?

La solution proposée par Diffie et Hellman est aussi simple que révolutionnaire : au lieu d'assurer au préalable qu'expéditeur et destinataire disposent de la même clé, il suffit à ce dernier de choisir une clé de déchiffrement qu'il gardera secrète et d'en publier une autre destinée au chiffrement des messages qui lui seront adressés.

Rien, sinon une habitude jusqu'alors fermement ancrée dans la pratique, n'exclut en effet de donner à un espion la possibilité d'envoyer des messages si tant est que d'une part l'expéditeur puisse l'identifier et d'autre part que la connaissance de cette clé de chiffrement ne lui permette pas, en pratique, de réaliser l'opération inverse de déchiffrement. La conclusion de leur article peut paraître presque magique au premier abord : il est possible de communiquer secrètement, à travers un canal non sécurisé, au moyen d'un procédé connu de tous ! Leur découverte porte le nom de cryptographie asymétrique (expéditeur et destinaire ne partagent désormais plus la même information) ou encore cryptographie à clé publique.

On est bien loin ici du mystère entourant jusqu'alors chaque découverte cryptographique. Pourtant le travail de Diffie et Hellman n'est pas exempt lui non plus d'une part d'inconnu : comment réaliser dans la pratique un tel procédé ? Cette question, cruciale, laissée en suspens (« le problème est encore largement ouvert ») dans l'article *New Directions in Cryptography*, va diviser un temps la communauté scientifique entre ceux qui croient en la possibilité d'y parvenir et ceux convaincus que le modèle de cryptographie asymétrique est intrinsèquement contradictoire.

Cette méfiance à l'égard des travaux de Diffie et Hellman renforce a posteriori le sentiment qu'il s'agit bien là d'une « révolution scientifique » telle qu'elle a été conceptualisée par Thomas Kuhn [2]. Comme la révolution copernicienne en Astronomie ou celle d'Einstein en Mécanique auxquelles il convient, toutes proportions gardées, de la comparer, l'apparition du concept de clé publique apporte d'une part une réponse à une situation de « crise » [3] et marque d'autre part l'émergence d'un nouveau paradigme en cryptographie ainsi qu'une transformation profonde du mode de pensée de ses acteurs.

2. Thomas S. Kuhn, *La structure des révolutions scientifiques*, Flammarion (2008).

3. La découverte, dans l'immédiate après-guerre, du fait que les Alliés emmenés par Turing et Welchman étaient en mesure de décrypter les messages réputés inviolables de la machine Enigma, combinée au développement fulgurant des ordinateurs avait rendu presque illusoire la possibilité de communiquer secrètement par les moyens cryptographiques conventionnels rappelés plus haut.

Parmi les sceptiques se trouvent à l'époque trois chercheurs : Ronald Rivest, Adi Shamir et Leonard Adleman. Ils se mettent au travail immédiatement après la parution de l'article de Diffie et Hellman et leurs résultats sont pour le moins surprenants : ils démontrent l'exact inverse de leur intuition initiale ! Le premier système de cryptographie à clé publique est né [4]. Il prendra rapidement le nom d'algorithme RSA, pour les trois initiales de ses inventeurs.

Leur découverte est instructive à plusieurs titres. Outre le fait qu'elle illustre ce principe maintes fois observé selon lequel la recherche conduit rarement au résultat escompté (réservant son lot de bonnes comme de mauvaises surprises !), elle apporte un démenti presque caricatural à l'inutilité pratique des mathématiques fondamentales. En effet, sans entrer dans le détail de la méthode employée par ces trois auteurs, signalons simplement que leur découverte repose sur des résultats fondamentaux, bien qu'élémentaires [5], de l'« arithmétique modulaire » dus à Euler et Fermat, deux mathématiciens ayant vécu aux 17ème et 18ème siècles ! Dans cette arithmétique « simplifiée », on commence par fixer un entier N, appelé module, puis dans chacun des calculs que l'on effectue, on « oublie » les multiples entiers de N. Par exemple, pour $N = 12$, si 17 et 5 ne sont bien entendu pas égaux, leur différence est un multiple de N, ce qu'on écrit « $17 \equiv 5 \pmod{12}$ » et qu'on lit « 17 est congru à 5 modulo 12 ». L'avantage alors est que tout se ramène à des calculs portant sur un ensemble fini de nombres. Par exemple, $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ et 11 lorsque $N = 12$. Le lecteur que cette digression mathématique aura dérouté pourra se convaincre qu'il pratique quotidiennement l'arithmétique modulaire (précisément avec $N = 12$) lorsqu'à la question de savoir l'heure il répond à son interlocuteur « il est 22h » quand sa montre indique 10h...

Loin d'apporter une réponse définitive [6] au problème de la réalisation pratique d'un système cryptographique à clef publique, la découverte de Rivest, Shamir et Adleman a ouvert la voie à tout un champ nouveau d'application des mathématiques d'autant plus actif de nos jours que les besoins cryptologiques se font toujours plus pressants. Désormais les outils mathématiques au service de la science du secret ne s'appellent plus seulement artihmétique mo-

4. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, Vol. 21 (2), pp.120-126, 1978.

5. On les retrouve d'ailleurs en partie au programme de l'enseignement de spécialité Mathématiques en Terminale Scientifique.

6. Signalons cependant que l'algorithme RSA est encore aujourd'hui largement employé. Le lecteur désireux d'acquérir des produits cryptologiques pourra d'ailleurs consulter à profit le site internet de la société éponyme : `http://www.rsa.com`.

dulaire, mais aussi, par exemple, « courbes elliptiques » [7]. Aussi surprenant que cela soit, ces dernières se retrouvent désormais au cœur des téléphones portables, cartes bancaires et autres cartes à puce. Le monde est « écrit en langage mathématique » affirmait Galilée en 1623. Quel que soit le crédit que l'on accorde à cette affirmation, notre société actuelle en est indiscutablement bien imprégnée.

7. Voir à ce propos l'article de N. Billerey et M. Rebolledo de ce volume.