RONALD LINN RIVEST ET LE CHIFFREMENT À CLÉ PUBLIQUE

Few persons can be made to believe
that it is not quite an easy thing
to invent a method of secret writing
which shall baffle investigation.
Yet it may be roundly asserted
that human ingenuity cannot concoct
a cipher which human ingenuity cannot resolve.

Edgar Allan Poe, *A Few Words on Secret Writing* (1841).

One of the most singular characteristics of the art of deciphering
is the strong conviction possessed by every person,
even moderately acquainted with it,
that he is able to construct a cipher which nobody else can decipher.
I have also observed that the cleverer the person,
the more intimate is his conviction.

Charles Babbage, *Passages from the Life of a Philosopher* (1864).

The General : *Incidentally, you know, they know*
you know they know you know [their] code.
Hooper Moulsworth : *What? Are you sure?*
The General : *I'm positive, because I've been talking, you know...*
Hooper Moulsworth : *Thank you ! Thank you! I shan't forget this!*
The General : *YOU MEAN YOU DIDN'T KNOW?*
Hooper Moulsworth : *NO!*

Peter Ustinov, *Romanoff and Juliet* (1961).

Plus les secrets que l'on doit garder pour assurer et maintenir la sécurité d'un système de communication sûre sont nombreux et complexes, plus le risque de compromission est important. Pour le dire autrement, en matière de communication sécurisée, tout élément devant être tenu secret (autres que les messages eux-mêmes) représente un point de défaillance potentiel. En revanche, si un système de communication demeure entièrement sûr même lorsque des parties tierces viennent à connaître tout du système lui-même à l'exception de la clé

cryptographique, alors ce système est grandement résilient. Nul besoin, si le caractère secret de la clé devait être compromis, de développer, de tester et de distribuer un nouveau système cryptographique ; il suffit de simplement générer et de distribuer une nouvelle clé.

À la lumière de ce qui précède, il apparaît naturel de se demander : existe-t-il un système de chiffrement (1) ne reposant sur aucun secret à l'exception de la clé cryptographique ; (2) pouvant être utilisé de manière répétée sans qu'il soit nécessaire de changer la clé ; et (3) offrant une sécurité pratiquement infaillible ?

Connue des spécialistes depuis 1975, la réponse à cette question a de quoi surprendre : en principe oui. À l'origine de cette réponse étonnante se trouvent deux spécialistes du génie électrique basés à l'Université Stanford : Bailey Whitfield Diffie et Martin Edward Hellman [1]. Ces deux hommes ont imaginé un système de cryptage dit à clé publique reposant sur l'emploi de fonctions dites à trappe ou à porte dérobée, à savoir des fonctions réversibles pour lesquelles il est facile d'aller dans un sens (c'est-à-dire évaluer l'image de n'importe quel point du domaine), mais prohibitivement difficile d'aller dans l'autre (à savoir calculer la préimage d'un point), à moins de disposer d'une information particulière – appelée la porte dérobée – qui est si soigneusement dissimulée que la probabilité de la trouver par hasard ou par déduction est pratiquement nulle. Voyons maintenant comment un groupe de personnes (disons des agents de renseignements) souhaitant communiquer les uns avec les autres certaines informations sensibles devant être tenues secrètes pourrait employer le système conçu par Diffie et Hellman pour parvenir à leurs fins [1 ; 2 ; 3].

Dans un premier temps, chaque membre du groupe doit concevoir sa propre fonction à porte dérobée (chacune d'elles possède ses propres algorithmes de codage et de décodage). On publie ensuite un bottin des algorithmes de codage de chacun des membres du groupe. Les algorithmes de décodage, eux, sont tenus secrets. Dans ce cadre, il est possible à qui que ce soit (tant les membres du groupe que les étrangers) de faire parvenir un message codé à n'importe quel membre du groupe. Quiconque veut communiquer avec le membre lambda, par exemple, n'a qu'à transformer le texte qu'il souhaite transmettre en un message codé en suivant la procédure de codage spécifique au destinataire qui se trouve détaillée dans le bottin. Le message codé peut

alors être envoyé à Lambda, qui pourra le déchiffrer en employant son algorithme secret. Si d'aventure une oreille indiscrète venait à intercepter le message codé, aucune conséquence malheureuse n'est à redouter puisque pour quiconque ne possède pas l'algorithme secret le message secret est virtuellement impossible à déchiffrer.

L'autre particularité du système de chiffrement conçu par Diffie et Hellman est qu'il permet de se prémunir contre la possibilité qu'un individu mal intentionné écoutant aux portes cherche à propager de fausses informations en se faisant passer pour un membre du groupe. Chaque membre du groupe a en effet la possibilité d'inscrire sur chaque message une signature numérique indélébile et inimitable prouvant de façon incontestable (tant au destinataire qu'à un tiers si cela devait s'avérer nécessaire) qu'il est l'auteur du message. Voyons maintenant comment apposer sa signature personnelle sur un message que l'on destine au membre lambda [2 ; 3].

Il nous suffit d'appliquer au message que l'on souhaite acheminer notre propre algorithme secret de déchiffrement. On applique ensuite l'algorithme de chiffrement spécifique au membre lambda qui se trouve détaillé dans le bottin. À la réception du message, Lambda n'a qu'à appliquer son propre algorithme secret de déchiffrement, puis à appliquer notre algorithme public de chiffrement afin d'exposer le message original. La certitude voulant que nous soyons bel et bien l'auteur du message vient du fait que l'encodage de celui-ci a nécessité l'emploi de l'algorithme secret que nous seuls possédons [2 ; 3].

En apparence révolutionnaire, l'article de Diffie et Hellman détaillant le fonctionnement d'un système de cryptage à clé publique comporte un défaut majeur : on n'y décrit aucune fonction à porte dérobée jouissant de l'ensemble des propriétés requises. L'applicabilité de leur idée était donc tributaire de la découverte d'une façon de générer des fonctions à porte dérobée.

Martin Gardner reçut un jour une lettre rédigée par le cryptologue américain Ronald Linn Rivest[1] dans laquelle ce dernier sollicitait une rencontre et promettait de transmettre au vénérable vulgarisateur

1. Né à Schenectady, dans l'État de New York, en 1947 au sein d'une famille d'origine canadienne-française, Ronald Rivest est titulaire d'un diplôme de premier cycle en mathématiques de l'Université Yale obtenu en 1969 ainsi que d'un doctorat en sciences informatiques décerné par l'Université Stanford en 1974. Rivest fit carrière au sein du Département de génie électrique et de sciences informatiques du Massachusetts Institute of Technology, où il fonda un groupe travaillant sur la sécurité de l'information.

mathématique des informations exclusives susceptibles d'intéresser les lecteurs de *Scientific American*, voire de générer de l'intérêt bien au-delà du lectorat habituel. L'individu, que Gardner ne connaissait ni d'Ève ni d'Adam, affirmait en effet avoir co-inventé avec ses collègues Adi Shamir et Leonard Adleman un système de cryptage à clé publique basé sur des fonctions à porte dérobée exploitant le haut niveau de difficulté associé au problème consistant à factoriser un nombre entier de grande taille de la forme $n = pq$, où p et q sont des nombres premiers [2 ; 3 ; 5]. Un système de chiffrement reposant sur cette idée n'est donc pas infaillible dans l'absolu puisqu'un cryptanalyste astucieux et persévérant étudiant l'algorithme de codage pourrait en principe découvrir l'algorithme de décodage qui lui est associé. Rivest soutenait qu'en pratique, toutefois, son système de chiffrement était infaillible, car le casser nécessiterait un supercalculateur et quelques millions d'années de fonctionnement. Une chose est sûre, Gardner – qui avait en commun avec l'un de ses héros littéraires, Edgar Allan Poe, un intérêt marqué pour la cryptologie – ne regretta pas d'avoir accepté la rencontre avec Rivest, car celle-ci fut à l'origine de l'une des plus grandes nouvelles en primeur qu'il lui fut donné d'offrir à ses lecteurs au cours du quart de siècle qu'il passa à la barre de la chronique *Mathematical Games*.

Espérant rapidement atteindre un large public et disséminer les fruits de leurs travaux (qui, après tout, possédaient un haut potentiel d'application), Rivest, Shamir et Adleman, tous trois des lecteurs assidus des chroniques de Gardner dans le périodique *Scientific American*, se tournèrent presque instinctivement vers lui plutôt que de se contenter de soumettre un article à une revue scientifique hautement spécialisée, mais à faible tirage, comme c'est l'usage dans le milieu académique. Gardner, fidèle à lui-même, saisit immédiatement le caractère révolutionnaire[2] de l'invention des trois cryptologues et il vit à ce qu'un article consacré au système de cryptage à clé publique RSA (nommé par les initiales de ses trois inventeurs) paraisse dans les plus brefs délais.

En plus d'avoir marqué le début d'une nouvelle ère dans le monde de la cryptographie, la chronique *Mathematical Games* d'août 1977 fut à

2. Ronald Rivest, Adi Shamir et Leonard Adleman reçurent le Prix Turing 2002 pour cette découverte. Décerné depuis 1966 par l'Association for Computing Machinery, ce prestigieux prix est parfois décrit comme étant en quelque sorte le Nobel de l'informatique.

l'origine d'une controverse que ni Rivest et ses collègues ni Gardner n'avaient anticipée.

Le chroniqueur scientifique transmit dans son article une invitation formulée par Ronald Rivest à l'endroit de tout lecteur intéressé à en savoir plus au sujet du système de chiffrement : le chercheur s'engageait à faire parvenir une copie d'un document technique non publié donnant des détails au sujet du système de cryptage RSA à quiconque enverrait à son laboratoire du MIT une enveloppe de retour préaffranchie. Le cryptologue fut bientôt submergé de lettres venant des quatre coins du monde. En effet, en l'espace de quelques semaines, il reçut plus de 7 000 lettres de lecteurs demandant une copie du rapport technique détaillant le fonctionnement du système RSA [4]. L'enthousiasme généré par l'article de Gardner à propos des travaux de Rivest, Shamir et Adleman incita toutefois Joseph Meyer, un agent de la National Security Agency (NSA) quelque peu bilieux, à brandir la menace d'engager des actions juridiques contre les trois chercheurs du MIT si ceux-ci continuaient à divulguer les détails du système de chiffrement qu'ils avaient conçu [4].

Suivant cette intervention gouvernementale, les trois cryptologues du MIT durent interrompre les envois postaux. Ce fut alors au tour de Gardner de recevoir un flot de lettres de lecteurs mécontents de n'avoir pas obtenu de réponse de la part du professeur Rivest. S'étant vu enjoint de s'abstenir de partager quelque document que ce soit ayant été produit par Rivest et son équipe, le vulgarisateur fut lui aussi réduit au silence. Au terme d'un processus d'examen méticuleux, les avocats du MIT conclurent que la divulgation du rapport technique produit par Rivest, Shamir et Adleman ne violait aucune loi [4].

En terminant, ajoutons que, dans le but de rendre sa chronique *Mathematical Games* d'août 1977 [2 ; 3] plus divertissante, Gardner avait mis au défi ses lecteurs de décoder un message codé par Rivest en suivant la méthode expliquée dans l'article. Ce dernier s'engagea de plus à remettre un chèque de 100 $ à la première personne qui parviendrait à décoder le message.

En 1988, à l'occasion de la parution prochaine de son recueil de chroniques intitulé *Penrose Tiles to Trapdoor Ciphers... And the Return of Dr. Matrix*, Gardner prit contact avec le co-inventeur du chiffrement RSA pour savoir si le prix avait déjà été réclamé. On lui répondit par la négative. De fait, Rivest ne se souvenait plus de la teneur du message

(choisi en partie au hasard) ni de la clé privée de déchiffrement. Mais, puisque la clé publique de chiffrement figurait dans l'article de Gardner, il lui serait néanmoins possible de vérifier la validité d'une solution soumise par un lecteur. Un post-scriptum apparaissant dans l'édition révisée de 1997 nous apprend toutefois qu'un chèque de 100$ dut être remis par Rivest au cryptologue néerlandais Arjen Lenstra en 1994 après que l'équipe qui travaillait sous sa direction aux laboratoires Bellcore est parvenue à décoder le message secret. Le décryptage du message de Rivest – qui se lit ainsi : « The magic words are squeamish ossifrage » – n'avait pas été une mince affaire. Il a en effet fallu compter sur le concours de 600 volontaires et sur la puissance de calcul de 1 600 ordinateurs travaillant en tandem pendant de très nombreuses heures.

L'exploit calculatoire réalisé par Arjen Lenstra et son équipe ne signifie pas que le chiffrement RSA est devenu obsolète. Au contraire, ce système demeure à ce jour sûr pourvu que l'on emploie des nombres entiers suffisamment grands (en date de 2020, on recommande d'utiliser des nombres entiers à 600 chiffres en notation décimale), car, selon les spécialistes de la théorie des nombres et de la cryptologie, il n'y aurait nulle part sur Terre ne serait-ce que l'esquisse d'une idée prometteuse sur la manière de résoudre efficacement le problème de la factorisation des nombres de très grande taille.

Références

[1] Diffie, W., et Hellman, M. E. (1976). « New Directions in Cryptography ». *IEEE Transactions on Information Theory*, *22* (6).

[2] Gardner, M. (1977, août). « Mathematical Games: A new kind of ciphers that would take millions of years to break ». *Scientific American*, *237* (2), 120-125. [www.jstor.org/stable/24954008]

[3] Gardner, M. (1989). « Trapdoor Ciphers ». Ch. 13 dans *Penrose Tiles to Trapdoor Ciphers… And the Return of Dr. Matrix*. W. H. Freeman & Co.

[4] Gardner, M. (1989). « Trapdoor Ciphers II ». Ch. 14 dans *Penrose Tiles to Trapdoor Ciphers… And the Return of Dr. Matrix*. W. H. Freeman & Co.

[5] Rivest, R. L., Shamir, A., et Adleman, L. (1978). « A method for obtaining digital signatures and public-key cryptosystems ». *Communications of the ACM*, *21* (2), 120-126.