Pour la libéralisation de la cryptographie

RONALD RIVEST

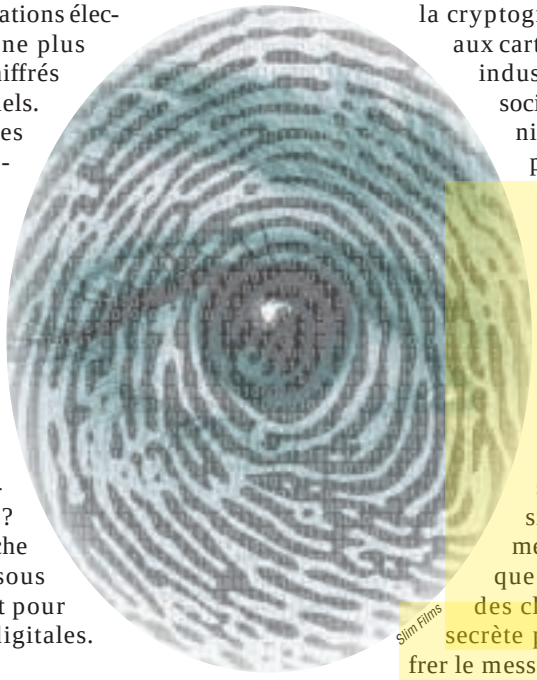
L'un des pionniers de la sécurité informatique s'oppose au contrôle gouvernemental de la cryptographie.

Le développement de la cryptographie est une conséquence inéluctable de la révolution informatique. Avec l'apparition des communications entre les ordinateurs, les utilisateurs cherchent à sécuriser les conversations et les transactions. La cryptographie est la… clé de cette sécurisation, mais sa généralisation est débattue. Aux États-Unis, le gouvernement veut restreindre l'usage de la cryptographie, car il craint que les criminels et les espions ne l'utilisent.

Avant 1970, la cryptographie était trop compliquée et trop onéreuse pour un usage courant. Grâce à deux inventions – la cryptographie à clé publique et le microprocesseur –, les méthodes cryptographiques sont devenues si performantes qu'il faudrait des années de calcul sur ordinateur pour décoder un message dont on ignore la clé. Les ordinateurs capables d'exécuter ces méthodes sont devenus largement accessibles.

Toutefois, vers la fin des années 1980, lorsqu'une cryptographie civile devint ainsi possible, deux agences américaines s'inquiétèrent de sa généralisation. L'Agence de sécurité américaine (NSA, soit *National Security Agency*), qui surveille les communications électroniques mondiales, s'alarma de ne plus pouvoir décrypter les messages chiffrés d'espions ou de terroristes potentiels. D'autre part, le FBI craignit que les criminels n'usent de logiciels de cryptographie pour déjouer la surveillance de leurs communications. Durant la dernière décennie, ces organismes ont poussé le gouvernement américain à réglementer l'usage de la cryptographie et à limiter l'exportation de logiciels de cryptographie performants.

Doit-on priver l'ensemble des utilisateurs de techniques, sous prétexte que quelques criminels pourraient les utiliser à leur avantage? L'argument est spécieux : on n'empêche pas le public d'acheter des gants sous prétexte que les voleurs en utilisent pour éviter de laisser des empreintes digitales. Restons sur ce dernier exemple.



La cryptographie protège les données ; les gants protègent les mains. La cryptographie protège contre les intrus et les espions industriels ; les gants protègent contre les coupures, la chaleur, le froid et les infections. La cryptographie peut gêner la police, qui ne pourra plus pratiquer d'écoutes téléphoniques ; les gants peuvent gêner la police qui trouve difficilement des empreintes digitales. La cryptographie est devenue bon marché et d'emploi facile ; les gants le sont depuis longtemps. Enfin, on peut télécharger des logiciels de cryptographie à partir du réseau Internet pour un coût inférieur à celui d'une bonne paire de gants.

Le travail de la police deviendra certainement plus difficile si tous les utilisateurs du réseau chiffrent leurs échanges, mais nous ne sortirons correctement de ce dilemme que si nous pesons les avantages et les inconvénients collectifs de l'innovation. La plupart des utilisateurs envisagent d'utiliser la cryptographie pour prévenir les crimes plutôt que pour les cacher, comme ils utilisent les gants pour protéger leurs mains plutôt que pour dissimuler leurs empreintes. En assurant la confidentialité et l'authentification des opérations bancaires et commerciales, la cryptographie empêche le vol et la fraude aux cartes de crédit, et elle évite le piratage industriel. Paradoxalement, on créera une société plus sûre si l'on adopte une technique qui entrave quelque peu l'application des lois.

Certains ont souhaité un compromis qui généraliserait les systèmes cryptographiques élaborés en permettant aux États de déchiffrer les messages en cas de besoin : par exemple, on pourrait demander aux utilisateurs d'enregistrer leurs clés de chiffrement auprès d'organismes assermentés ou de donner aux autorités des moyens secrets d'accéder à ces clés. Une version cryptée de la clé qui a chiffré le message serait envoyée en même temps que celui-ci. Un centre de recouvrement des clés pourrait utiliser une super clé secrète pour déchiffrer la clé, puis déchiffrer le message lui-même.

La réglementation en France

Pendant longtemps, la cryptographie a été considérée comme une arme ; son usage était réglementé, aussi bien pour la fourniture et l'exportation que pour l'utilisation à titre personnel.

En février 1998, toutefois, l'État français à autorisé tout procédé nécessaire à l'authentification de données ou d'entités (intégrité, signature numérique et contrôle d'accès), ainsi que le chiffrement des communications, en limitant, dans ce dernier cas, la clé secrète à 40 bits. Une telle taille de clé ne garantissait pas un niveau de confidentialité suffisant pour des applications «sérieuses» : à raison d'un million d'essais par seconde, une station de travail trouve la clé en moins de 15 jours.

Comment accroître la sécurité ? En augmentant la taille de la clé et en déposant alors la clé secrète auprès d'un tiers de confiance. Ce dépôt permettait alors aux instances judiciaires d'obtenir, de ce tiers de confiance, la clé secrète nécessaire au déchiffrement de communications chiffrées, en cas de besoin justifié.

Le 19 janvier 1999, le premier ministre, Lionel Jospin, annonçait une proche libéralisation de l'usage de la cryptographie. Après avoir interrogé les acteurs, les experts et les partenaires internationaux, le gouvernement a retenu les orientations suivantes : libéraliser complètement la cryptographie ; supprimer le recours obligatoire aux tiers de confiance pour le dépôt des clés secrètes de chiffrement ; compléter le dispositif juridique afin d'obliger la remise aux autorités judiciaires de la transcription en clair des documents chiffrés, lors de leur demande. De telles modifications législatives nécessiteront plusieurs mois.

Pour lever rapidement les principales entraves au développement du commerce électronique et pour assurer la confidentialité des communications, des décrets, parus le 19 mars 1999, relèvent le seuil de la cryptographie libre de toute autorisation de 40 bits à 128 bits. Plus précisément, ces décrets stipulent que «les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clé est d'une longueur inférieure ou égale à 40 bits sont totalement libres» et que «les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clef est d'une longueur supérieure 40 bits et inférieure ou égale 128 bits sont libres sans condition pour un usage privé, et soumis à déclaration dans les autres cas».

Ces décrets représentent l'étape essentielle, car des clés de 128 bits garantissent une sécurité plus que suffisante : une attaque par recherche exhaustive (essai de toutes les clés) nécessiterait plusieurs siècles, même avec tous les ordinateurs de la planète réunis. Une autre étape importante, sera «d'assurer, avec toutes les garanties nécessaires, la valeur probante du document sous forme numérique et des signatures électroniques. Les obstacles juridiques qui demeurent au développement des transactions dématérialisées seront ainsi levés».

David POINTCHEVAL, École normale supérieure, Paris

Ces systèmes ne satisferont personne, car ils sont faciles à détourner. Les espions et les criminels peuvent modifier les logiciels de chiffrement pour empêcher la recherche de la clé ou utiliser d'autres logiciels disponibles sur le réseau Internet. De surcroît, avec ces solutions, la recherche des clés serait très onéreuse et le coût du recouvrement des clés n'a pas été envisagé : qui paiera ? Enfin, la confiance dans le gouvernement risquerait de s'éroder, et la procédure serait très compliquée : imaginez qu'à chaque achat de gants vous soyez légalement tenus de coudre des copies en latex de vos empreintes digitales aux doigts de ces gants !

Les systèmes de recouvrement de clés seraient également dangereux. La procédure secrète utilisée par le FBI pour déchiffrer les messages pourrait être détournée au profit de criminels, d'intrus, d'espions ou même d'employés mécontents du FBI. En volant une super clé secrète, ces indélicats pourraient déchiffrer toutes les communications. Des millions de secrets appartenant à des sociétés, à des personnes privées ou au gouvernement seraient brusquement vulnérables.

En 1993, le Congrès américain a réclamé une étude de ces problèmes. Après deux années de travail, la commission réunie pour l'occasion a estimé que la libéralisation de la cryptographie était plus avantageuse que son interdiction. Aucune loi ne devrait limiter la fabrication, la vente et l'utilisation des systèmes cryptographiques à l'intérieur des États-Unis.

Les membres de la commission ont également estimé que l'État ne pourrait pas faire respecter une interdiction de la cryptographie. Pourtant, le FBI et la NSA prônent toujours la mise en place d'un service de recouvrement des clés ; ils s'opposent au relâchement des contrôles à l'exportation, tant que la possibilité de retrouver les clés secrètes n'est pas incorporée dans les logiciels exportés.

Entre-temps, la cryptographie s'est développée, les utilisateurs se sont familiarisés avec les programmes de cryptographie, et le contrôle deviendra inéluctablement difficile. Les entreprises adoptent des standards publics de cryptographie que même des lycéens peuvent convertir en programmes. De surcroît, il existe de nouvelles techniques qui ne chiffrent pas le message, mais permettent la confidentialité en le cachant dans un fouillis de données aléatoires. D'où la difficulté d'un contrôle !

Je maintiens que les citoyens doivent avoir le droit d'avoir des conversations privées. La démocratie repose sur la possibilité que possède chaque citoyen de partager librement ses façons de voir, sans crainte de surveillance ou de représailles. Ce principe doit être appliqué au «cyberespace», comme il l'est au monde réel. Si les États-Unis restreignaient le droit d'utiliser la cryptographie, ce serait un recul de la démocratie et une victoire de *Big Brother*.

Donald RIVEST est l'un des inventeurs de la méthode de chiffrement RSA. Il enseigne à l'Institut de technologie du Massachusetts.

Whitfield DIFFIE et Susan LANDAU, *Privacy on the Line : The Politics of Wiretapping and Ecryption*, MIT Press, 1998.