



## Cryptologie, science et sécurité

Comité science et sécurité  
Olivier Pironneau et Christophe Soulé

7 mars 2006

### 1. Objectifs

*Nous nous sommes posés les questions suivantes : la cryptologie, une technologie clef pour la sécurité, répond-elle à nos besoins ? À l'inverse, la dépendance de notre société à l'égard de cette technologie ne constitue-t-elle pas un point faible au cas où un groupe serait capable d'en casser les codes ? Dans ce cas, ne faudrait-il pas encourager plus de travaux en cryptologie dans notre pays ? Si oui, lesquels et de quelle façon ?*

### 2. Synthèse

#### 2.1 La cryptologie : introduction

La cryptologie est une science au moins aussi vieille que les arts militaires. Son objet est de limiter l'accès à certaines informations aux seules personnes désirées.

Historiquement le cryptage est d'abord à clefs secrètes mais, dans un article séminal, Ron Rivest, Adi Shamir, et Leonard Adleman ont proposé un chiffrement à clef publique (chiffrement dit RSA, où seule la clef pour le déchiffrement est privée) et fourni des arguments indiquant qu'il ne pouvait probablement pas être cassé sans de très puissants moyens de calcul<sup>1</sup>. Depuis, RSA est de très loin la méthode la plus utilisée pour le cryptage d'informations ; ceci n'empêche pas la recherche d'être très active, pour trouver de nouvelles méthodes de cryptographie (créer des algorithmes de cryptage) et de cryptanalyse (analyser les faiblesses d'un algorithme), pour diminuer la taille des clefs, sécuriser leurs cryptages etc.

La recherche en cryptologie n'est pratiquement pas classifiée (ce n'est bien sûr pas le cas des protocoles mis en œuvre en pratique !) ; elle emprunte beaucoup à la théorie des

---

<sup>1</sup> à moins que quelqu'un ne parvienne à résoudre le problème suivant : étant donné un entier produit de deux nombres premiers gigantesques, trouver rapidement ces nombres premiers.

nombres, y compris à certains de ses développements les plus pointus, dans le domaine des courbes elliptiques par exemple. On part du principe qu'il est peu probable qu'une innovation technologique majeure (par exemple une solution au problème de la factorisation rapide mentionné ci-dessous) permette à des individus ou à un organisme de casser les codes des autres sans que cette avancée ne soit rapidement connue de tous. La recherche est donc principalement internationale. D'autres voies sont explorées, comme la cryptographie quantique, qui emprunte certaines idées aux théories quantiques de la physique et aux futurs ordinateurs quantiques mais qui se développe indépendamment.

## 2.2 Les diverses méthodes de cryptage

Le travail de Rivest, Shamir et Adleman d'une part, de Diffie et Hellman d'autre part, marque la naissance, au milieu des années soixante-dix, de la cryptologie comme discipline académique. Les travaux n'ont cessé depuis de se multiplier. On distingue notamment la cryptologie à clés secrètes et la cryptologie à clés publiques (telle que RSA), qui ont chacune leurs avantages.

Ce n'est pas le lieu de décrire la méthode RSA. On indiquera seulement qu'elle repose en définitive sur deux résultats arithmétiques élémentaires : le « petit théorème de Fermat » et le théorème de Bézout. Il en est de même d'une grande partie des protocoles cryptographiques. Certains livres de terminale S, option Mathématiques, présentent d'ailleurs en exercice une variante un peu simplifiée de RSA. Ceci dit, l'usage fait de cette arithmétique élémentaire est extrêmement astucieux, et, s'il est assez facile de comprendre un travail de cryptologie, il est beaucoup plus difficile d'inventer une méthode nouvelle.

Une des variantes développée par les cryptologues consiste à remplacer la multiplication de nombres entiers (modulo un nombre premier) par l'addition de points dans des courbes elliptiques. Cette cryptographie elliptique est nettement plus sophistiquée d'un point de vue mathématique, et permet de raccourcir la taille des clés. Il ne semble pas cependant qu'elle ait un grand succès dans les applications commerciales.

Pour le codage de longs messages en ligne, les algorithmes à clef publique ne sont utilisés que pour encrypter les clefs de session d'une autre technique de codage plus rapide. C'est une des raisons pour lesquelles on utilise en pratique beaucoup d'autres algorithmes que RSA. La recherche de nouvelles techniques, plus rapides et plus sécurisées, donne lieu à une intense activité. C'est d'autant plus vrai que toute nouvelle idée est immédiatement soumise à des "attaques" énergiques, visant à vérifier si elle augmente véritablement la sécurité. On peut citer en exemple l'histoire du "standard" DES, adopté dès 1977, mais considéré aujourd'hui comme trop faible.

La théorie des codes est une discipline voisine de la cryptologie, qui y fait appel dans certains protocoles. Elle repose aussi sur des mathématiques assez élaborées, par exemple l'étude des réseaux euclidiens.

Parmi les domaines des mathématiques qui contribuent peu ou prou à la cryptologie, signalons la théorie des nombres, la théorie des groupes, la géométrie algébrique, l'algèbre commutative effective, et la logique mathématique. Dans la Section 3 ci-dessous, J.-M. Couveignes décrit plus en détails certaines des directions importantes de la recherche dans ce domaine.

La cryptologie ne se réduit pas pour autant à l'écriture de logiciels de nature mathématique. Elle comporte aussi un aspect « hardware », et des innovations en physique peuvent se révéler décisives, aussi bien pour la conception des protocoles (cryptographie) que pour l'attaque de ceux-ci (cryptanalyse). Une des directions importantes est celle de la cryptologie quantique, présentée par P. Grangier dans la Section 4. On prendra soin ici de distinguer la cryptologie quantique, qui est déjà une réalité, de l'ordinateur quantique, qui n'est pour l'instant qu'une utopie.

Parmi les très nombreux excellents livres d'introduction à la cryptologie signalons :  
Bruce Schneier : *Applied Cryptography*, Second ed., 1996, *John Wiley & Sons*  
P.Barthélemy, R.Rolland, P.Véron : *Cryptographie, principes et mises en oeuvre* ,  
*Hermès*, 2005, Lavoisier

### **2.3 La cryptologie en France**

On voit donc qu'il est important de disposer en France de centres de recherche et de formation en cryptologie mais aussi, car les deux problèmes sont liés, en sécurité des systèmes informatiques. À en juger par le nombre de conférenciers invités aux deux grands colloques de cryptologie (Crypto et Eurocrypt), la France contribue activement à la recherche, au même titre que l'Allemagne, la Belgique, la Suisse, la Hollande ou la Grande-Bretagne. Mais ces contributions sont le fait d'un trop petit nombre de chercheurs. On constate cependant un engouement croissant des arithméticiens pour la cryptologie, ce qui est prometteur étant donné le niveau exceptionnel de la théorie des nombres dans notre pays.

Les équipes de recherche sont principalement à l'ENS-Ulm, à France-Telecom, à l'ENSTA, GEM+, Bull, CELAR, l'INRIA, l'école Polytechnique, dans les universités de Bordeaux, Grenoble, Limoges, Marseille, Rennes, Toulon, Versailles-Saint Quentin, ... avec des modules d'enseignement bien évidemment, lorsqu'il s'agit de grandes écoles ou d'universités.

A l'instar du comité américain PITAC (cf. Section 7), qui suggère d'insuffler 90 millions de dollars par an dans les universités et entreprises (donc hors NSA, l'organisme de la Défense chargé aux Etats-Unis des questions de sécurité) pour faire face au défi de la sécurité informatique, certains spécialistes recommandent de multiplier par dix l'effort de recherche et d'enseignement en France. Mais un tel effort devra porter sur la sécurité informatique dans son ensemble. Il convient en effet d'insister sur le fait que la cryptologie actuelle ne traite qu'une partie du problème de la sécurité informatique. Personne ne peut dire aujourd'hui d'où viendront, par exemple, les avancées théoriques et/ou technologiques permettant de sécuriser les transactions sur internet.

Il faut aussi remarquer que l'utilisation de technologies américaines tant matérielles que logicielles (et surtout celles de Microsoft) fragilise beaucoup l'Europe. Certains disent que la sécurité ne sera jamais totale, et c'est une des raisons pour laquelle la Chine a décidé d'écrire un système de type Unix et une bureautique entièrement endogène. Le SGDN fait en permanence des études pour évaluer les risques et remédier à ceux d'attaques éventuelles de réseaux stratégiques pour le contrôle aérien, la distribution d'électricité, les banques, etc.

Les **entreprises** sont nombreuses à utiliser la cryptologie, mais rares sont celles qui emploient des cryptologues. Par exemple, les banques sécurisent leurs communications à de nombreux niveaux, mais n'emploient pratiquement personne pour mettre au point les outils dont-elles ont besoin<sup>2</sup>. Des consortiums bancaires internationaux tiennent à jour les standards disponibles, en faisant appel à quelques-uns des meilleurs experts. Chaque banque peut ensuite s'adresser à des prestataires de service, en demandant tel ou tel outil cryptographique. Il s'agit principalement d'un choix économique : sont mis en balance les coûts des frais de poursuite des fraudeurs, aussi bien que ceux d'un renouvellement à grande échelle des protocoles utilisés. Ces derniers étant considérables, on comprend que les banques répugnent à changer trop souvent leurs moyens cryptographiques.

Parmi les rares entreprises ayant un service de cryptologie, la compagnie **Gemplus**, fabriquant des cartes bancaires, est un bon exemple des applications privées de la cryptologie. Une de ses prestations est aussi l'installation de systèmes informatiques sécurisés chez ses clients.

Avec **Thales, France-Telecom** est une des rares entreprises ayant un service important de recherche et de développement spécifiquement dédié à la sécurité informatique et à la cryptographie. Ce secteur de l'entreprise a connu un essor considérable ces dernières années.

Signalons aussi des entreprises de plus petite taille, comme **Id Quantique** par exemple, qui développent leur propre cryptographie pour des usages spécifiques dans des activités innovantes.

Les **organismes publics** qui développent la cryptologie dépendent surtout du ministère de la défense et de celui de l'intérieur. Il s'agit de la DCSSI (qui est interministérielle), du CELAR (défense), et de la DGSE et des services de police (intérieur). Pour des raisons évidentes, les informations sur les activités de ces derniers ne sont pas disponibles. Par contre, les services de cryptologie DCSSI et CELAR travaillent pour une part de façon ouverte, car, comme nous l'avons dit, cette discipline a besoin d'une telle ouverture. La tâche du CELAR, près de Rennes, est de sécuriser les informations et les communications classifiées pour le ministère de la défense et l'interministériel, ce qui exige une capacité à s'adapter à des contextes très diverses. Il met au point des protocoles originaux et du plus haut niveau possible, et peut, si nécessaire, disposer d'un budget important. Ces protocoles sont pour la plupart implémentés sur des matériels spécifiques. Les implémentations logicielles n'offrent en effet pas un niveau de sécurité équivalent. La réalisation de ces matériels fait appel à des industriels privés ou internationaux, car on peut éviter de révéler le contenu d'un protocole au fabricant. Une des spécificités des

---

<sup>2</sup> ...alors qu'elles ont participé activement à la mise au point initiale des cartes à puce.

protocoles défense est en effet d'être constitués d'une partie publique, qui ne révèle rien sur le protocole, et d'une partie secrète introduite par le CELAR au tout dernier moment de la fabrication.

Simultanément, le CELAR a une activité de veille technologique, et suit la recherche cryptologique avec attention. Certains de ses membres assistent à des conférences nationales ou internationales dans le domaine. Ils peuvent d'ailleurs, à l'occasion et avec l'autorisation de leur tutelle, publier leurs travaux de recherches.

Une initiative originale permet la collaboration de mathématiciens avec l'équipe du CELAR. Il s'agit d'un **séminaire conjoint** hebdomadaire au département de mathématiques de l'université de Rennes 1 (<http://www.math.univ-rennes1.fr/crypto/seminaire.html>). Ce département abrite quelques-uns des meilleurs spécialistes d'arithmétique, d'algèbre effective, de géométrie algébrique et arithmétique, et de géométrie réelle, tous ces domaines ayant (ou étant susceptibles d'avoir) des applications à la cryptologie. Ce séminaire fonctionne depuis quelques années, et invite des orateurs de nombreux horizons. Il est l'occasion pour les mathématiciens de découvrir l'utilité surprenante de recherches très abstraites et non finalisées. Pour leurs partenaires, il permet de connaître la communauté mathématique de l'intérieur, ce qui facilite grandement le recours aux meilleurs mathématiciens spécialistes de tel ou tel domaine prometteur, comme le développement d'une cryptographie à l'aide des formes modulaires et des représentations galoisiennes (généralisant la cryptologie elliptique), ou les recherches sur l'utilisation de l'algèbre commutative effective à des fins de cryptanalyse. Ces travaux peuvent faire l'objet de contrats.

## 2.4 Les centres de formation et de recherches

L'École normale supérieure de la rue d'Ulm possède une équipe de cryptologie de réputation mondiale (de 5 à 10 chercheurs). L'École Polytechnique possède aussi une équipe très compétente. La cryptologie est un des domaines de recherche de l'INRIA (deux projets, TANC et CODES), dont les équipes vont jusqu'à l'implémentation des algorithmes développés.

Les universités : plusieurs facultés ont un département ou des enseignements consacrés à la cryptologie. Le plus ancien de ces départements est celui de *Limoges*, qui date des années quatre-vingt (<http://www.cryptis.fr/>). Il offre aujourd'hui quatre masters, à des étudiants ayant reçu une formation en mathématiques, en informatique ou en électronique. Les étudiants trouvent des débouchés dans la sécurité informatique. La Section 6, écrite par deux responsables de ce département, décrit plus en détail les perspectives professionnelles de ces formations.

Le centre de *Marseille* à Luminy est plus spécialement orienté vers la théorie des codes, et a recruté certains des meilleurs spécialistes de l'ex Union Soviétique.

L'université de *Bordeaux* est un département très connu en arithmétique, et plus précisément la théorie des réseaux euclidiens et l'algorithmique ; il accueille depuis quelques années un enseignement de cryptologie de tout premier ordre.

Signalons aussi *Rennes, Versailles, Caen, Toulon, Grenoble, Besançon, Saint-Etienne, Toulouse, Clermont-Ferrand, Lille, Rouen, Nice, Nancy*, et des projets en cours de réalisation dans les centres universitaires de *Saint-Denis* et à *Paris 6*.

Les départements universitaires de cryptologie sont très attentifs aux débouchés de leurs étudiants, et ils ont pris contact avec diverses entreprises du secteur, contacts souvent concrétisés sous forme de bourses CIFRE.

L'Europe : plusieurs pays d'Europe ont des centres de cryptologie de grande qualité. La Suisse à l'École polytechnique fédérale de Lausanne, la Belgique à l'université de Louvain, l'Allemagne avec l'arithméticien G. Frey (célèbre pour avoir eu l'idée initiale qui a conduit à la preuve du théorème de Fermat), et les Pays Bas en sont quelques exemples. Par contre, l'Union européenne n'a pas conduit pour l'instant à beaucoup de collaborations, même s'il existe des appels d'offre de la Commission européenne dans le domaine. Le réseau NESSIE a mis au point et proposé des standards européens. Le budget de 250 millions d'euros mis en œuvre par l'Union européenne en août 2005 pour la recherche anti-terroriste et la sécurité profitera entre autres aux recherches universitaires et à la cryptologie.

## **2.5 Cryptologie et sécurité informatique**

Le PITAC constate que de nombreux secteurs vitaux de la société américaine - informatique, téléphone, transport, banque, défense...- sont menacés de paralysie temporaire en cas d'attaque à distance à travers leurs réseaux de communication (vers, cheval de Troie, virus, etc.). La sécurité de l'information est vitale pour la défense mais aussi pour les banques par exemple.

La sécurité informatique est un très vaste domaine qui va de la protection des ordinateurs militaires jusqu'aux téléphones portables. La plupart des installations utilisant de l'électronique digitale sont concernées par ce problème, surtout si elles communiquent avec des ordinateurs ou des réseaux externes. La Défense (militaires, ambassades), les banques (transactions électroniques), les entreprises (secrets commerciaux), mais aussi la RATP (faux billets), emploient des spécialistes de la sécurité informatique. De l'avis des spécialistes, le plus gros problème actuellement est dû à l'ignorance par les responsables des dangers encourus et des moyens de protection. Il y a donc un marché de l'emploi énorme pour des agents de sécurité informatique, et leur formation doit inclure la cryptologie.

La cryptologie est seulement, comme nous l'avons dit, un des outils de protection contre les agressions et interceptions indésirables, mais cet outil est essentiel. Il est estimé suffisamment robuste par les spécialistes, du moins tant que les agressions sont faites avec des outils de la cryptanalyse connus. Ceci n'est plus vrai lorsque l'agresseur a accès à des paramètres physiques du système (champs électromagnétique ou thermique, informations sur les composants électroniques utilisés). Casser une clef par des méthodes mathématiques est certes possible si l'on dispose de très gros moyens de calcul, mais les temps de calcul sont aussi fortement diminués si l'on dispose d'informations annexes.

Tout ceci conduit à juger de l'utilité de la cryptologie en la situant dans tout son environnement d'utilisation, et explique pourquoi la plupart des utilisateurs estiment que la technologie RSA suffit à leurs besoins.

Rappelons par ailleurs que de nombreux problèmes relevant de la cryptologie sont loin d'être parfaitement résolus. Un de ces problèmes est de mettre au point une signature pour authentifier de façon discrète les documents (les documents graphiques par exemple) ; une des méthodes utilisées consiste à mettre cette « signature » en filigrane dans une image. Un autre problème est celui de la confiance, c'est-à-dire de savoir si une information a bien été postée par celui qui s'en revendique l'auteur.

## 2.6 Cryptologie et citoyen

Une des fonctions de la Commission nationale informatique et liberté (CNIL) est d'éviter que des informations confidentielles dans un secteur (médical par exemple) ne soient utilisées à d'autres fins (comme le crédit bancaire), nuisant ainsi à la vie privée des citoyens. Il s'agit donc de restreindre la circulation de l'information et/ou d'imposer le cryptage de la banque de données. On trouvera dans la Section 5 plusieurs exemples illustrant bien les atteintes à la vie privée que représente la trop libre circulation des données. Mais là encore l'usage du chiffrement RSA suffit lorsqu'il est possible. La CNIL identifie parfois des cas non standards, qui demandent des recherches spécifiques. C'est ainsi que l'usage de deux banques de données à accès crypté (pour établir des relations statistiques en recherche médicale par exemple) pose le problème d'empêcher l'accès complet à au moins l'une des banques, de manière à en empêcher la fusion en une seule banque de données ; la méthode cryptologique dite de « double hashage » fournit en principe une solution à ce problème.

De façon générale, la CNIL estime que la cryptologie est un **outil majeur de protection des individus contre les dangers de l'informatique**. Face au risque d'une utilisation criminelle des moyens de cryptage, la justice dispose, dans le cadre de ses enquêtes et sur commission rogatoire, du droit d'accès à toute donnée informatique. Par ailleurs, l'usage d'outils cryptologiques importés de l'étranger doit avoir l'accord des autorités. Mais, en dehors de ces mesures, il n'y a aujourd'hui aucune restriction à l'usage de la cryptographie par quiconque et, par exemple, aucune limitation légale à la longueur des clés utilisées. On trouvera dans la Section 5 une présentation plus détaillée des activités de la CNIL.

## 2.7 Conclusions

Cette brève enquête nous a menés aux constatations et conclusions suivantes :

1) Il y a **peu de cryptologues purs en France aujourd'hui**. Si l'on entend par cryptologue une personne dont l'activité professionnelle principale est la mise au point de protocoles de cryptologie, que ce soit de façon industrielle, académique, ou dans des organismes d'état, leur nombre ne semble pas dépasser la centaine. Ainsi défini, ce métier ne propose donc pas beaucoup de débouchés, car les protocoles de cryptographie sont mis

au point de façon très centralisée. L'exemple des banques est frappant, et la cryptologie contraste nettement avec le domaine des mathématiques financières, qui emploie beaucoup plus de personnes très qualifiées.

2) Mais la cryptologie n'est qu'une partie, un des outils de **la sécurité informatique, où les besoins sont au contraire considérables**. Il y a donc lieu de développer la formation en cryptologie, tout en indiquant clairement aux étudiants que cette discipline ne sera probablement pas leur activité professionnelle principale.

3) **L'enseignement** fourni ne doit pas se limiter aux aspects théoriques et arithmétiques. Il doit être de nature interdisciplinaire (mathématiques, informatique et même électronique). Il doit favoriser une attitude critique vis-à-vis des méthodes existantes de cryptage, et comporter si possible une part de cryptanalyse, où l'on apprendra comment casser certains protocoles. Le niveau idéal auquel peut se faire cet apprentissage semble être la fin de la licence et le master. Les écoles d'ingénieurs sont sans doute aussi très bien adaptées pour enseigner la cryptologie à leurs élèves. Il ne paraît pas indispensable d'avoir effectué un travail original de recherches pour devenir cryptologue, mais il faut par contre être capable de suivre l'évolution des connaissances, et surtout être capable d'implémenter concrètement des protocoles.

On notera enfin que le profil des étudiants qui aborderont ce sujet est a priori relativement rare, puisqu'il s'agit soit d'informaticiens ayant un haut niveau en mathématiques, soit de mathématiciens prêts à écrire des logiciels, soit d'électroniciens que n'effraient pas les théories abstraites. Nous avons appris que certains centres de formation ont eu du mal à trouver des étudiants ces deux dernières années. Il faut donc éviter un déséquilibre entre l'offre d'enseignements et la demande.

4) La **qualité exceptionnelle de la recherche en théorie des nombres**, et, plus spécifiquement, en théorie des nombres effective, fait que la France a toutes les raisons de devenir un pays leader en cryptologie théorique, ce qu'elle n'est pas tout à fait aujourd'hui. Il faudra veiller à ce que cette discipline ne devienne pas une sorte de « bulle académique », mais qu'elle débouche sur la solution des vrais problèmes posés par la sécurité informatique.

5) Il faut donc continuer à **développer la culture en cryptologie**, comme cela se fait déjà un peu dans l'enseignement des classes préparatoires.

### 3. Algorithmes et cryptologie

(J.-M. Couveignes, Professeur de mathématiques, Université de Toulouse II)

Un article fameux de Claude Shannon, publié en 1949, distingue sécurité inconditionnelle et sécurité calculatoire. La *sécurité inconditionnelle* protège d'un adversaire disposant d'une capacité de calcul illimitée. Le coût de la sécurité inconditionnelle est souvent prohibitif. La longueur de la clé secrète utilisée pour le chiffrement doit être au moins égal à la longueur du message. Et pour chaque nouveau message, il faut convenir d'une nouvelle clé. Son coût extrêmement élevé cantonne la sécurité inconditionnelle aux

applications les plus sensibles. La sécurité calculatoire protège contre un adversaire disposant d'une capacité de calcul limitée. Cette limitation (budgétaire ou technologique dans la pratique) est quantifiée par la *théorie de la complexité*. L'objet de cette théorie est d'évaluer le nombre d'opérations élémentaires nécessaires à la résolution algorithmique d'un problème appartenant à une famille donnée. Par exemple, la complexité de la multiplication est le nombre d'opérations élémentaires requises pour multiplier deux nombres entiers (en fonction de la taille de ces deux nombres). Si cette théorie établit que la cryptanalyse d'un système de chiffrement requiert un nombre d'opérations élémentaires plus grand que le rapport entre l'âge de l'univers et la durée d'un phénomène physique élémentaire, on s'estime suffisamment prémuni contre des attaques réelles. Au contraire, si la résolution d'un problème requiert un nombre d'opérations élémentaires polynomial en la taille de ce problème, ce problème est considéré comme facile. On dit qu'il est *polynomial en temps* et on ne peut fonder un système de chiffrement sur ce problème. La théorie de la complexité s'est remarquablement développée depuis Turing. Malheureusement, ses énoncés les plus remarquables sont *relatifs*. Ils établissent que si un algorithme efficace existe pour résoudre un certain problème, alors il existe des algorithmes efficaces pour toute une classe de problèmes. Un résultat très important de cette nature a été obtenu récemment par Miklos Ajtai : le problème appelé SVP, qui consiste à trouver le *vecteur le plus court* (pour la norme usuelle) dans un réseau entier, est un problème NP-complet. Cela signifie par exemple, que si ce problème était polynomial en temps, alors la factorisation des entiers, la recherche de solutions aux formules booléennes, les problèmes de coloration de graphes et un grand nombre de problèmes difficiles d'optimisation combinatoire, seraient polynomiaux en temps, et donc plutôt faciles. La célèbre hypothèse  $P \neq NP$  serait alors fausse, ce qui est très improbable. Ajtai a inventé un système de chiffrement dont la sécurité calculatoire repose sur la difficulté du problème SVP. Donc ce système est sûr si SVP n'est pas polynomial. Et si SVP est polynomial alors l'hypothèse  $P \neq NP$  est fausse. Ce système offre le meilleur niveau de sécurité conditionnelle accessible à ce jour puisque la condition de sécurité ( $P \neq NP$ ) est très largement considérée comme vraie, bien qu'elle ne soit pas mathématiquement prouvée. Malheureusement, ce système est un peu trop lourd à mettre en oeuvre pour envisager des applications à court terme. Les systèmes de chiffrement réellement utilisés reposent sur des hypothèses un peu plus fortes. Certains d'entre eux, dérivés du système RSA inventé par Rivest, Shamir et Adleman, font reposer leur sécurité sur la difficulté de factoriser certains entiers. Plus précisément, si P et Q sont deux grands nombres premiers (de l'ordre de  $10^{150}$  par exemple), le produit  $N=PQ$  se calcule aisément (calculer le produit de deux entiers est un problème polynomial en temps, et c'est même l'un des plus faciles parmi les problèmes polynomiaux). En revanche, si l'on connaît l'entier N, il est difficile (et même impossible en l'état actuel des connaissances) de calculer P et Q dans un temps raisonnable (significativement plus petit que l'âge de l'univers). La *factorisation* n'est pas un problème NP-complet mais c'est un problème réputé très difficile. Il existe des systèmes de chiffrement efficaces en pratique, dont la sécurité est conditionnée à la difficulté de la factorisation. Un petit nombre de problèmes d'algorithmique mathématique joue ainsi un rôle essentiel en cryptologie. Outre la factorisation des entiers et la recherche du vecteur le plus court d'un réseau, on peut citer le décodage aux limites des codes correcteurs d'erreur et le *logarithme discret*. Ce dernier problème consiste en la donnée d'un groupe fini G et de deux éléments g et h

de ce groupe tels que  $h$  appartienne au sous-groupe de  $G$  engendré par  $g$ . On demande alors un entier  $x$  tel que  $h$  soit égal à  $g^x$ . La question a un sens pour une grande variété de groupes  $G$  et est supposée difficile pour nombre d'entre eux. Ueli Maurer a montré récemment que, pour un *groupe générique*, le logarithme discret n'est pas résoluble en temps polynomial, mais il est difficile de prouver qu'un groupe déterminé est générique ... Notons aussi que si l'on se donne  $g$  un élément du groupe  $G$  et  $x$  un entier naturel, il est aisé de calculer  $h=g^x$  par la méthode dite de *l'exponentiation rapide*. La correspondance qui à  $(g, x)$  associe  $(g, h)$  est donc un candidat au titre de *fonction asymétrique*, c'est-à-dire de correspondance biunivoque facile à calculer mais difficile à inverser. Le logarithme discret joue un rôle croissant en cryptologie. Il simplifie considérablement la *gestion des clés* car il permet à deux opérateurs distants de convenir d'un secret partagé en communiquant seulement à travers un canal non sécurisé. Le problème du logarithme discret permet aussi *l'identification sans divulgation de connaissance* : il est ainsi possible de prouver son identité en démontrant que l'on détient une information personnelle, sans rien dévoiler de cette information.

Ces quelques exemples de problèmes algorithmiques (RSA, SVP, logarithme discret) et de fonctionnalités cryptologiques (chiffrement, identification, échange de clé) ne rendent pas compte de la richesse de ce domaine mais permettent d'introduire quelques une des préoccupations essentielles de la recherche en algorithmique pour la cryptologie :

- évaluer la difficulté algorithmique des principaux problèmes algorithmiques mobilisés par la cryptologie. Par exemple, on cherche des algorithmes aussi efficaces que possible pour factoriser des entiers. L'implémentation soignée de ces algorithmes donne une mesure concrète de leur efficacité et permet de spécifier des longueurs de clés optimales pour les applications. On peut chercher aussi des bornes inférieures pour la complexité de ces problèmes, en particulier par des techniques de *réduction* (ramener un problème à un autre). Ces recherches en mathématique et informatique fondamentale mobilisent des connaissances pointues et soulève des questions profondes en arithmétique, géométrie algébrique, mathématiques discrètes.
- évaluer la sécurité des *primitives cryptographiques*. Ces primitives sont les briques de base de la sécurité informatique. Leur sécurité repose sur la difficulté de certains problèmes algorithmiques mais il convient de *prouver* que la *difficulté* du problème algorithmique implique la *sécurité* de la primitive. Ces recherches connaissent un développement rapide. Elles permettent aussi de détecter les primitives non sûres. La notion de preuve est au centre de ces recherches. Il faut prouver la sécurité et donner un sens précis au terme de preuve dans ce contexte.
- évaluer la sécurité des *systèmes d'information*. Ces systèmes peuvent assembler un grand nombre de *briques de bases*. De la sécurité des briques de base et de l'architecture du système, peut on déduire la sécurité de l'ensemble ? Les *méthodes formelles* mobilisées pour étudier la sécurité des systèmes ont du mal à prendre en compte les propriétés particulières des briques de bases : par exemple la brique RSA a des propriétés *homomorphiques* (le produit de deux chiffrés est le chiffré du produit des deux messages clairs) qui peuvent compromettre la sécurité d'un vaste système d'information. Mais il est très difficile de prendre en compte cette propriété dans l'analyse formelle du système.

## **4. La cryptographie quantique : un bref état des lieux en 2005**

(Philippe Grangier, Institut d'Optique, Orsay)

### **4.1 Introduction**

La plupart des moyens de communications actuels (téléphones mobiles, réseaux informatiques...) seraient difficilement utilisables sans des méthodes de cryptage destinées à protéger la confidentialité des messages. Les systèmes de cryptographie les plus utilisés actuellement pour des utilisations militaires ou civiles sont appelés systèmes "algorithmiques", et répondent aux exigences de sécurité des communications, en mettant en oeuvre toute une constellation de méthodes mathématiques pour établir et transmettre une clé, chiffrer et déchiffrer un message, identifier et authentifier les deux partenaires, signer et assurer l'intégrité d'un message ou d'une transaction. Toutefois, leur sécurité reste conditionnée par la puissance informatique d'un adversaire éventuel, et par la possibilité de développement d'algorithmes de décryptage efficaces.

Le développement des systèmes de cryptographie quantique se présente comme une alternative permettant de se prémunir contre cette vulnérabilité, ou même contre le danger d'effondrement total des méthodes cryptographiques algorithmiques, qui pourrait être consécutif au développement de nouveaux moyens de calculs, ou de nouveaux algorithmes.

### **4.2 Les principes et l'état de l'art de la cryptographie quantique**

La cryptographie quantique est basée sur le codage d'information sur des propriétés physiques "quantiques" de faisceaux lumineux, par exemple sur la phase ou la polarisation de photons individuels, ou sur les corrélations quantiques entre des paires de photons. De nombreuses équipes en Europe, au Japon, en Australie et aux USA travaillent actuellement sur les technologies requises pour donner des débouchés commerciaux ou militaires à ces méthodes de cryptage. Sur un plan plus général, la cryptographie quantique est le volet "appliqué" d'un champ de recherche très actif appelé "Information quantique", donc l'objectif est d'utiliser les lois de la mécanique quantique pour améliorer certains aspects de la transmission et du traitement de l'information.

La cryptographie quantique est passée du statut d'idée théorique [1] à la réalisation d'expériences de faisabilité au début des années 90, puis à un niveau quasi opérationnel à l'heure actuelle. Une revue du domaine en 2002 est présentée dans [2]. La cryptographie quantique en fibres optiques atteint actuellement (2005) une portée supérieure à 100 km, et des systèmes très robustes vis-à-vis des perturbations extérieures ont été développés [2]. Des expériences en espace libre (20 km) ont été réalisées [3], ainsi que des démonstrations utilisant des sources de photons intriqués [2], de photons uniques [4], ou des variables quantiques continues [5]. Les premiers systèmes de cryptographie quantique ont été commercialisés en 2001 par la compagnie "IdQuantique" basée à Genève (<http://www.idquantique.com/>), suivi par MagiQ basé à New York et Boston (<http://www.magiqtech.com/>). Des grandes compagnies japonaises (NEC, Toshiba) et américaines (BBN) sont aussi très actives dans le domaine. En Europe, ces recherches

sont actuellement coordonnées par le "Projet Intégré" SECOQC (<http://www.secoqc.net/>).

Le concept de téléportation d'un état quantique a aussi été démontré [6], et peut ouvrir la voie à la cryptographie quantique à très longue distance. De tels "répéteurs quantiques" utilisent des portes logiques quantiques, et des mémoires capables de "stocker" un état quantique. Ils font l'objet d'études très actives, mais sont encore loins d'une mise en oeuvre "sur le terrain".

- [1] C.H. Bennett and G. Brassard, Proc. IEEE Int. conf. on computers, systems and signal processing, p.175. (1984)
- [2] "Quantum cryptography", N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002)
- [3] "Quantum cryptography: A step towards global key distribution", C. Kurtsiefer et al, Nature 419, 450 (2002)
- [4] "Single photon quantum cryptography", A. Beveratos et al. , Phys. Rev. Lett. 89, 187901 (2002)
- [5] "Quantum key distribution using gaussian-modulated coherent states", F. Grosshans et al., Nature 421, 238 (2003)
- [6] "Experimental quantum teleportation", D. Bouwmeester et al, Nature 390, 575 (1997)

### **4.3 Avis sur l'évolution du domaine**

Il existe actuellement trois principaux types de protocoles quantiques d'échange de clé, qui ont des statuts différents. Le plus ancien [1, 2] est basé sur le codage d'un bit d'information sur un photon, et il est maintenant bien compris, à la fois théoriquement et expérimentalement. Le deuxième type de protocole est basé sur la production de paires de photons intriqués, et il a été démontré expérimentalement plus récemment [2]. Une troisième voie, apparue encore plus récemment, utilise des variables continues, comme l'amplitude et la phase d'un faisceau laser, et non des photons individuels [5]. Ce type de protocole permet de s'affranchir des problèmes liés au comptage de photon, sa sécurité a été établie par des travaux théoriques récents, et sa faisabilité a été démontrée expérimentalement en 2003 au LCFIO. Les mérites comparés des divers protocoles dépendront alors des performances des sources et des détecteurs utilisés, ainsi que de choix liés aux conditions d'utilisation (transmission par fibres optiques ou en espace libre, éventuellement avec un relai satellite). De telles études "comparatives" sont actuellement en cours.

Dans une vision à plus long terme, il existe actuellement de nombreuses propositions de protocoles de transmission plus complexes, qui ne sont pas encore validés expérimentalement. Les buts poursuivis sont en particulier la correction des erreurs de transmission, ou la réalisation de répéteurs pour la cryptographie quantique à grande distance. Les concepts utilisés sont la distribution ou le transfert d'intrication (entanglement sharing, entanglement swapping), et la téléportation quantique. Sur le plan expérimental, les méthodes proposées utilisent des portes logiques quantiques, et des transferts quantiques d'information entre photons et atomes (mémoires quantiques). Ces études à long terme font que le domaine est très actif sur le plan scientifique, mais il est clair que certains des objectifs poursuivis ne seront pas atteints avant de nombreuses années.

Des crédits relativement importants sont actuellement consacrés à ces études. D'après diverses sources, le financement global actuel consacré à l'Information Quantique par les diverses agences civiles et militaires aux USA (NSF, NSA, DARPA, MITRE, etc) est de l'ordre de 30 à 50 M\$ par an. Un exemple d'objectif qui semble en bonne voie d'achèvement à moyen terme est la transmission quantique de clés dans des petits réseaux (quelques dizaines de km), en utilisant des fibres optiques ou des transmissions en espace libre. Un exemple d'objectif plus futuriste est la réalisation d'un système de "téléportation quantique" d'une portée supérieure à 100 km.

#### **4.4 Conclusions**

Le développement actuel de l'information quantique, qui est le domaine scientifique qui englobe la cryptographie quantique, implique de nombreux échanges interdisciplinaires, qui vont des problèmes mathématiques fondamentaux (algorithmique) aux technologies de télécommunications optiques, en passant bien sûr par l'optique quantique. La réalisation de démonstrateurs implique des développements scientifiques très récents, testés dans des laboratoires de recherche. Les équipes européennes sont actuellement très bien placées dans la compétition internationale dans ce domaine, particulièrement en Angleterre, en Autriche, en Suisse et en France. Plusieurs groupes français (LCF/IO Orsay, LKB/ENS Paris, LPN Bagneux, U. Nice, ENS Cachan, GTL Metz) sont impliqués dans ces recherches, ainsi qu'un industriel (Thales TRT).

Le bilan des travaux effectués depuis une dizaine d'années en cryptographie quantique montre que plusieurs problèmes qui semblaient initialement insurmontables ont été résolus un par un. Sur le plan des applications, les défis actuels sont d'une part d'améliorer les performances (distance, débit...), et d'autre part de dépasser la notion de "liaison quantique point à point", pour atteindre celle de "réseau quantique", ce qui est l'objectif central du projet "SECOQC".

L'objection majeure qui subsiste contre la cryptographie quantique est celle du "maillon faible" : il est généralement admis que le point faible des systèmes de sécurité actuels n'est en fait pas le cryptage lui-même, mais plutôt les interfaces (accès, authentification, stockage...). On peut donc objecter que la cryptographie quantique se contente de renforcer le point le plus fort, ce qui est inutile puisque la vulnérabilité est ailleurs. Cependant, cette objection s'applique surtout aux liaisons point à point, et ignore l'apport potentiel d'un réseau global de gestion de clé quantique. Il semble donc encore un peu tôt pour conclure, et comme il est probable que les progrès se poursuivront dans les années à venir, l'évolution du domaine doit être suivie avec attention.

### **5. La Commission nationale de l'informatique et des libertés**

(Yann Le Hegarat, Commission nationale de l'informatique et des libertés, CNIL)

Créée en 1978, la CNIL est une autorité administrative indépendante (comme l'ARCEP, l'ART ou la Commission des marchés financiers), comportant 85 agents et 17

commissaires, qui est chargée de la régulation de la collecte et de l'usage des données personnelles.

Une grande partie des activités de la CNIL est dédiée au contrôle a priori et a posteriori de ces traitements d'information. Elle donne des avis sur les décrets d'application du gouvernement et peut aussi alerter le Parlement.

Entre autres tâches, elle mène des études de prospective technologique concernant l'équilibre entre l'informatique et les libertés. Elle pourra prochainement délivrer des labels à des procédures et des produits renforçant la protection des données personnelles.

Les sujets sensibles à forte implication technologique sont actuellement :

- les capacités de profilage des internautes (salariés ou non) naviguant sur Internet ,
- la rétention de toutes les données de connexion (toute forme de téléphonie, ou d'usage de l'un des nombreux protocoles Internet) concernant un individu, quand elle s'étend sur une période très longue (3 ans ?) ;
- l'utilisation abusive des fichiers liés à la défense et à la protection contre le terrorisme ;
- les problèmes posés par la diffusion des RFID (Radio Frequency Identification) ;
- la géolocalisation (dans le cas, par exemple, de telle ou telle compagnie d'assurance anglaise qui baisse les tarifs de ceux de ses clients qui se meuvent dans des zones à moindre risque) ;
- l'usage et la protection des signatures électroniques ;
- le vote électronique ;
- la biométrie ;
- les questions posées par le « peer to peer » ;
- enfin, tout système d'identification et d'authentification.

On estime que chaque individu figure dans un nombre de fichiers situé entre cent et cinq cents, chacun de ces fichiers contenant des informations partielles (qui peuvent être éventuellement religieuses, politiques, commerciales... ou médicales). Pour se protéger contre l'usage abusif de ces informations, l'usage de la cryptographie est largement libéré depuis 2002. D'autres outils de protection sont par exemple :

- les signatures électroniques
- le PGP
- les protocoles de connexion SSL-128 bits
- l'identification fédérée (exemple : le protocole *Liberty Alliance* proposé par un consortium initié par Sun Micro Systemes)
- le double hashage à clef secrète
- les protocoles dits « zero knowledge »

ainsi que des méthodes et technologies en cours de développement, regroupées sous le terme de PETs (Privacy Enhancing Technologies).

On assiste donc à une explosion de la communication de données sous toutes ses formes. L'utilisation future de « smart objets », dans une société où l'informatique est omniprésente, posera de nouveaux problèmes éthiques, qui seront certainement complexes. La CNIL pense pouvoir y faire face. Mais il est clair que la répression de la

fraude et des traitements illégaux de données personnelles pourrait s'avérer plus difficile à l'avenir.

Du point de vue de la technologie, la CNIL identifie parfois des problèmes qui relèvent encore de la recherche (nous avons mentionné la valeur et l'usage de la signature électronique sur le long terme et le rapprochement de plusieurs bases de données sans en faire la fusion).

## **6. Les principaux débouchés professionnels en cryptographie**

(Philippe Gaborit et Thierry Berger, université de Limoges)

### **6.1 L'industrie des cartes à puces**

Ce travail est avant tout un travail de développement logiciel dans un contexte cryptographique: assembleur pour cartes à puces, programmation orienté objet, méthodes formelles. Il s'agit souvent de mettre en oeuvre les dernières normes, par exemple celles concernant l'utilisation des courbes elliptiques. Il ne s'agit pas d'un travail de recherche sur les algorithmes cryptographiques, mais il est indispensable d'avoir compris le fonctionnement pour réaliser l'implantation.

### **6.2 L'industrie de la défense et de la sécurité**

Il s'agit essentiellement de grands groupes qui proposent des solutions sécurisées pour des applications grand public ou de la défense. Les compétences recherchées peuvent aller de compétences pointues en cryptographie à des connaissances plus générales pour des applications logicielles.

### **6.3 L'industrie des services informatiques et du conseil**

L'activité dans ce secteur en cryptographie est surtout orientée vers la gestion des PKI (Public Key Infrastructure) et l'architecture des systèmes sécurisés. Les compétences demandées sont la compréhension des mécanismes de gestion des clés, la connaissance des normes ainsi que des compétences en programmation, langage C ou java pour adapter des solutions existantes à des architectures particulières.

### **6.4 L'industrie des télécommunications et les éditeurs de solutions de protection de documents multimédia**

Il s'agit d'intégrer aux solutions proposées des techniques cryptographiques nouvelles ou connues tout en les adaptant au contexte de l'application envisagée. Ce type de débouchés nécessite une bonne connaissance des techniques liées à l'application concernée: télécom, formats d'images, etc.

### **6.5 Les établissements publics**

DGA, certains ministères.

### **6.6 Les laboratoires de recherche institutionnels**

Université, INRIA, CNRS. Ces débouchés restent très limités.

## 7. Annexe

### Le codage RSA<sup>3</sup>

Supposons que A veuille communiquer avec B sans que C puisse lire.

A traduit son message en un nombre  $m$ , par exemple en remplaçant chaque lettre par sa position dans une table ; avec la table de numérotation de l'alphabet « a » devient 01, « b » devient 02... « z » devient 26.

B choisit 2 nombres premiers  $p$  et  $q$  tels que  $n=p.q > m$  et choisit aussi un nombre  $e$  qui n'a pas de facteur commun<sup>4</sup> avec  $(p-1).(q-1)$  ; puis il calcule  $d$  tel que<sup>5</sup>  
 $d.e=1 \text{ mod } (p-1).(q-1)$ .

Le nombre  $d$  est la « clef privée » et le nombre  $e$  est la clef publique. La longueur  $n$  est connue de tous. Codage : A demande donc à B la clef  $e$ , calcule  $c = m^e \text{ mod } n$  et envoie  $c$  à B

Décodage : B reconstruit  $m$  par  $m = c^d \text{ mod } n$ , puis rétablit le message par la table en regroupant<sup>6</sup> les chiffres 2 par 2.

La méthode est fondée sur le (petit) théorème de Fermat :

$$m^{ed} = m \text{ mod } p = m \text{ mod } q = m \text{ mod } pq$$

La sûreté de la méthode est basée sur le fait qu'il n'est pas possible de deviner  $d$  en un temps  $t$  petit même en connaissant  $m$ ,  $n$  et  $e$  car cela reviendrait à pouvoir trouver les facteurs premiers de  $n$  (i.e.  $p$  et  $q$ ) en un temps de l'ordre de  $t$ , donc petit, ce qui est considéré (mais non démontré) comme infaisable. Actuellement il faut 3 mois pour factoriser un nombre de 640 bits ; un prix est donné à celui qui fait mieux !

Exemple : Pour coder « ab » la table de l'alphabet donne  $m=102$ ; en choisissant  $p=13$  et  $q=11$ , soit  $n=143$ , on a  $(p-1).(q-1)= 120$  on peut donc prendre  $e= 13$  et  $d=37$  car  $13 \times 37 = 120 \times 4 + 1$ . Alors A calcule  $c = (102^{13} \text{ mod } 143) = 115$  qui est envoyé à B . Puis B effectue  $(115^{37} \text{ mod } 143)$  qui vaut bien 102. B complète à gauche par zéro pour avoir un nombre pair de chiffres et traduit 0102 en « ab ».

---

<sup>3</sup> R. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21 (2), pp.120–126. 1978.

<sup>4</sup> On dit que  $z$  et  $y$  ont un facteur commun  $z$  si  $z > 1$  et  $x$  et  $y$  sont divisibles par  $z$ .

<sup>5</sup>  $z \text{ mod } y$  est le reste de la division de  $z$  par  $y$ , c'est à dire  $r < y$  tel que  $x = s.y + r$ , pour  $s$  entier.

<sup>6</sup> Dans la pratique on utilise la table ASCII plutôt que la table de l'alphabet et une codification hexadécimale.

**Personnalités rencontrées**

Jacques Stern (ENS-Ulm)  
Christian Peskine (CNRS)  
Philippe Grangier (CNRS)  
David Lubicz (CELAR)  
Gilles Lachaud (CNRS, Luminy)  
Philippe Elbaz-Vincent (Montpellier)

Michel Bouthier (CSD)  
Nicolas Sendrier (INRIA)  
Yann Le Hegarat (CNIL)  
Christine Bachoc (Bordeaux)  
Robert Rolland (Luminy)

**Personnalités consultées**

Eric Brier, Marie-Pierre Malherbe, Nathalie Feyt (Gemplus)

**Principaux rapports consultés**

- PITAC (*President's Information Technology Advisory Committee*)  
*Cyber Security: a crisis of prioritization*  
février 2005  
<http://www.nitrd.gov>
- Rapport du Comité Science et Défense, 2005