LA RELATION AGITEE ENTRE MATHEMATIQUES ET CRYPTOGRAPHIE[1]

Neal KOBLITZ[2]
Traduction Marie-José DURAND-RICHARD et Philippe GUILLOT

Au cours des six mille premières années, jusqu'à l'invention des clés publiques dans les années 1970, les mathématiques utilisées en cryptographie n'étaient généralement pas très intéressantes. Même au vingtième siècle, les cryptographes utilisaient peu les concepts de pointe des mathématiques. En effet, les mathématiciens qui s'intéressaient à la cryptographie dans ces années-là auraient volontiers adhéré à la déclaration méprisante de Paul Halmos[3] : « les mathématiques appliquées sont de mauvaises mathématiques »[4].

Il y a cependant quelques exceptions. Dans les années 1940, Alan Turing, le père de la science informatique, a travaillé intensivement en cryptographie. Il a en particulier montré comment utiliser des techniques statistiques sophistiquées pour décrypter un code[5]. Claude Shannon, le père

---

[1] NdT. : la version originale de cet article a été publiée sous le titre « The Uneasy Relationship between Mathematics and Cryptography » dans *Notices of the AMS*, septembre 2007, vol. 54, n° 8, pp. 972-979. Nous tenons à remercier Neal Koblitz et l'AMS pour nous avoir gracieusement accordé le droit de publier cette traduction.

[2] Neak Koblitz est professeur de mathématiques à l'Université de Washington, Seatle. Son courriel est *koblitz@math.washington.edu.*

Cet article repose sur une conférence invitée donnée à la réunion de l'AMS au *Steven Institute of Technology* à Hoboken, NJ, le 14 avril 2007. Certaines parties sont extraites du chapitre sur la cryptographie de son ouvrage à venir *Random Curves : Journeys of a Mathematician*, à paraître chez Springer Verlag. [NdT. : Ce livre est paru en 2008].

[3] NdT. : Paul R. Halmos (1916-2006) est un mathématicien d'origine hongroise, émigré aux États-Unis en 1929, et spécialiste de la théorie des ensembles. Il est l'auteur d'une autobiographie intitulée *I Want to Be a Mathematician. Automathography* (1985).

[4] NdT. : *Applied Mathemathics is Bad Mathematics in* L. A. Steen (ed.), *Mathematics Tomorrow*, New-York, Springer Verlag, 1981.

[5] NdT. : Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » p. 59.

de la théorie de l'information, a travaillé sur les fondements de la cryptographie[6].

Dans la même décennie, G. H. Hardy a écrit, dans son *Apologie d'un mathématicien* :

> « À la fois Gauss et de moindres mathématiciens peuvent se réjouir qu'il y ait une science [la théorie des nombres] qui de toutes façons, et selon eux, devrait rester éloignée des activités humaines ordinaires, et rester noble et propre ».

Du temps de Hardy, la plupart des applications des mathématiques étaient militaires, et un pacifiste comme lui était heureux de constater que la théorie des nombres n'était pas étudiée pour son utilité pratique, mais seulement pour sa valeur esthétique intrinsèque.

Cette image d'une théorie des nombres « noble et propre » a eu un grand succès jusqu'en 1977, lorsque trois chercheurs en informatique du *Massachusetts Institute of Technology* – Ron Rivest, Adi Shamir et Len Adleman – ont inventé un système cryptographique radicalement nouveau. Un article paru dans *Scientific American* de Martin Gardner a décrit l'idée du RSA, expliqué sa signification, et provoqué un regain soudain d'intérêt populaire pour la cryptographie et la théorie des nombres[7].

Dans ces années-là, le RSA était la principale façon de réaliser ce qui allait devenir la « cryptographie à clé publique ». Les systèmes antérieurs pour brouiller les messages convenaient aux applications militaires ou diplomatiques, où seule une hiérarchie arrêtée de personnes était autorisée à connaître les clés secrètes. Mais dans les années 1970, de larges pans de l'économie se sont rapidement informatisés, les limites de la cryptographie classique devinrent manifestes. Supposons par exemple qu'un grand réseau de banques veuille pouvoir échanger des messages chiffrés pour autoriser les transferts d'argent. En cryptographie traditionnelle, deux banques doivent toujours s'accorder sur leur propre clé secrète pour échanger en toute confiance sur un service de messagerie. Le nombre de paires possibles atteint facilement les centaines de millions. Par conséquent, la cryptographie antérieure, dite « à clé privée » (ou « à clé symétrique »), devient extrêmement peu maniable.

En cryptographie à clé publique, la clé nécessaire pour embrouiller un message est une donnée publique. Chaque utilisateur du système (par exemple, chaque banque) dispose de sa propre clé publique, inscrite dans un annuaire un peu comme un numéro de téléphone. N'importe qui peut chiffrer

---

[6] NdT. : voir les chapitres « Du message chiffré au système cryptographique » pp. 127-142 et « Pourquoi et comment la cryptologie a envahi le domaine public ? » pp. 203-207.

[7] NdT. : voir le chapitre « Pourquoi et comment la cryptologie a envahi le domaine public ? » pp 209-216.

un message en utilisant cette clé publique. Toutefois, le processus de déchiffrement exige la connaissance d'une clé totalement différente, que le destinataire garde secrète. La procédure pour embrouiller un message est appelée une « fonction à sens unique avec trappe »[8]. Cela signifie qu'une fois que nous avons la clé publique de la banque, il est facile de calculer (à l'aide d'un ordinateur) le message chiffré à envoyer. Si toutefois, nous voulons aller dans l'autre sens – désembrouiller le message – cela est mathématiquement impossible, à moins de posséder une information supplémentaire, à savoir la clé secrète.

Rivest, Shamir et Adleman ont conçu un moyen ingénieux – et simple – pour réaliser une fonction à sens unique avec trappe, en utilisant la théorie élémentaire des nombres. Leur construction repose sur la multiplication de deux grands nombres premiers p et q pour obtenir un nombre composé $N = pq$. On peut supposer qu'il s'agit d'un processus à sens unique, en ce sens que factoriser N pour retrouver p et q est très difficile.

Ainsi, la sécurité de la cryptographie RSA est entièrement tributaire de la difficulté présumée de la factorisation de grands nombres entiers. Pour cette raison, l'invention du RSA a donné une impulsion considérable à l'étude des méthodes de factorisation des entiers, et aussi des méthodes pour produire aléatoirement de grands nombres premiers. Au début des années 1980, les points forts de la cryptographie mathématique étaient pour la plupart dans ce domaine – par exemple, le développement par Carl Pomerance de l'amélioration des techniques de crible pour les algorithmes de factorisation, et la preuve déterministe de primalité en temps quasi polynomial d'Adleman-Pomerance-Rumely à l'aide des sommes de Jacobi[9].

Dans une veine un peu différente, Don Coppersmith mit au point un algorithme qui pouvait trouver le logarithme discret dans le groupe multiplicatif de F_{2^n} en temps $\exp(n^{1/3+\varepsilon})$, ce qui est bien plus rapide que les méthodes antérieures de calcul de logarithme. Cela a également eu un impact en cryptographie, du fait qu'El Gamal a proposé une alternative au chiffrement RSA[10] reposant sur la difficulté présumée à inverser la fonction : $x \mapsto g^x$ (où g est fixé) dans un corps fini.

[8] NdT. : voir le chapitre « Les nouvelles orientations de la cryptographie » p. 192.

[9] NdE. : le lecteur trouvera de nombreuses références aux travaux de Carl Pomerance dans le chapitre « L'influence de la cryptologie moderne sur les mathématiques et l'université » notamment p. 267.

[10] NdT. : contrairement au RSA, le système fondé par Taher El Gamal n'a jamais été protégé par un brevet. Il est utilisé par le logiciel libre GNU *Privacy Guard*, par de récentes versions de PGP, et d'autre systèmes de chiffrement.

FACTORISATION ET COURBES ELLIPTIQUES[11]

En 1984, Hendrik Lenstra a diffusé en une page la description d'une nouvelle méthode qu'il avait développée pour factoriser les entiers en utilisant les courbes elliptiques[12]. L'algorithme astucieux et élégant était assez simple pour que je puisse le comprendre à partir d'une esquisse d'une page, même si une analyse détaillée de son temps d'exécution en a pris beaucoup plus. Ce fut la première fois que les courbes elliptiques étaient utilisées en cryptographie, et quand j'ai lu la page que Lenstra m'avait envoyée, j'ai senti qu'il avait d'un seul coup élevé les mathématiques de la cryptographie à un tout nouveau niveau de sophistication.

Peu de temps après, j'ai passé un semestre en Union Soviétique, où personne ne travaillait ouvertement sur la cryptographie. J'ai cependant continué à réfléchir sur ce sujet, et bientôt il m'est apparu qu'il devrait être possible d'utiliser les courbes elliptiques d'une manière tout à fait différente de ce que Lenstra avait fait, à savoir, pour construire des systèmes basés sur le problème difficile du calcul des logarithmes sur la courbe. Comme je ne connaissais personne en Union Soviétique avec qui je pouvais en parler, j'ai écrit une lettre à Andrew Odlyzko[13], puis aux *Bell Labs*, décrivant mon idée d'utiliser le groupe d'une courbe elliptique pour construire un cryptosystème. Odlyzko était alors un des rares mathématiciens à avoir produit un travail majeur à la fois dans les domaines théoriques et pratiques. Aujourd'hui, il n'est pas si inhabituel de concilier les mathématiques pures et appliquées, mais dans le milieu des années 1980, Odlyzko était le seul dans ce cas parmi les mathématiciens que je connaissais personnellement.

Les courriels n'existaient pas encore, et les lettres entre l'URSS et les États-Unis prenaient deux semaines dans chaque direction. Il a donc fallu attendre un mois pour recevoir une réponse d'Odlyzko. Il disait que mon idée de ce nouveau type de cryptographie était bonne, et en fait, dans le même temps, Victor Miller[14] d'IBM a proposé exactement la même chose. L'attrait de la cryptographie à courbe elliptique (ECC *Elliptic Curve Cryptosystem*) résidait dans ce que le problème du logarithme discret sur une courbe elliptique paraissait être (et semble l'être encore vingt-deux ans

---

[11] NdT. : les titres des paragraphes ne figurent pas dans l'article original.

[12] NdT. : voir le chapitre « L'influence de la cryptologie moderne sur les mathématiques et l'université » p. 273.

[13] NdT. : le mathématicien et informaticien Andrew Odlysko (né en 1949) fut responsable du *Digital Technology Center* de l'université du Minnesota. Il a abondamment publié en théorie analytique et en théorie algorithmique des nombres, ainsi qu'en théorie de la complexité et en cryptographie.

[14] NdT. : Victor S. Miller (né en 1947), co-inventeur de la cryptographie par les courbes elliptiques, travaille au Centre de Recherche en Communication de l'*Institute for Defense Analysis* à l'université de Princeton. Il est l'auteur de plusieurs algorithmes cryptographiques.

plus tard) un problème beaucoup plus difficile que celui de la factorisation des nombre entiers.

Dans un premier temps, ni Victor ni moi n'imaginions que l'ECC prendrait une importance commerciale, nous l'avions plutôt pensée comme une belle construction théorique. Rétrospectivement, le plus surprenant n'est pas que je ne pensais pas à commercialiser l'idée, mais que Victor Miller, qui travaillait chez IBM, ne pensait pas non plus en termes concrets. Il n'a même pas déposé de demande de brevet, même si à l'époque comme aujourd'hui à IBM, la politique était d'encourager vivement tous les employés à faire tout leur possible pour déposer des brevets, même sur le plus futile des sujets. Ainsi, la question de transformer l'ECC en un produit commercial aura attendu que d'autres personnes s'y intéressent.

LA LIBERTE DE TON DANS LES REUNIONS DE CRYPTOGRAPHIE

Après être revenu aux États-Unis, j'ai commencé à fréquenter les conférences de cryptographie. Les plus importantes étaient les réunions annuelles *Crypto* en août à Santa Barbara, en Californie. Dans les années 1980, j'ai trouvé l'atmosphère à *Crypto* rafraîchissante et stimulante. Les réunions étaient vraiment pluridisciplinaires, avec des participants venant de l'industrie, du gouvernement, et du milieu universitaire dans des domaines allant des mathématiques à l'informatique, et de l'ingénierie aux affaires.

Il y avait une sorte de « fruit défendu » dans la première décennie des conférences *Crypto*. Au début des années 1980, la *National Security Agency* (NSA) avait mené une tentative lourde (mais infructueuse) pour limiter la recherche ouverte en cryptographie. Ainsi, inaugurer les conférences *Crypto* en 1981 était en soi un acte de défiance.

La liberté de ton des réunions dans ces années reflète les personnalités hautes en couleur et excentriques de certains des premiers fondateurs et des chercheurs en cryptographie à clé publique. Tel a été Whit Diffie, un libertaire brillant, excentrique et imprévisible, qui avait co-écrit en 1976 (avec Martin Hellman) l'article le plus célèbre de l'histoire de la cryptographie[15]. Diffie avait l'habitude de donner des « sessions impromptues » *(rump sessions*), où les présentations informelles, irrévérencieuses, et souvent humoristiques étaient la norme. Il a été chahuté au point qu'on a dû imposer des restrictions sur ce qui pouvait être jeté à l'orateur (d'accord pour des canettes de bière vides, mais pas pleines).

L'influence des entreprises était alors beaucoup plus faible. Il s'est passé beaucoup de temps entre l'invention de la cryptographie à clé publique et

[15] NdT. : cet article est ici traduit au chapitre « Les nouvelles orientations de la cryptographie » p. 173.

son acceptation dans le monde commercial. Jusqu'à la fin des années 1980, les entreprises ne manifestaient généralement que peu d'intérêt pour la question de la sécurité des données. Presque aucun chercheur en cryptographie n'a jamais signé d'« accord de non divulgation » limitant ce qu'il pourrait dire publiquement – en fait, la plupart d'entre nous n'avions jamais entendu parler d'une telle chose.

C'est à *Crypto* que j'ai rencontré Scott Vanstone[16], un mathématicien de l'Université de Waterloo qui a dirigé un groupe pluridisciplinaire et amélioré les algorithmes pour l'arithmétique dans les corps finis. Avec cette expérience, il était bien outillé pour travailler sur l'ECC. Vanstone, avec deux autres professeurs de Waterloo, l'un en mathématiques et l'autre en ingénierie, ont formé une société, qui s'appelle maintenant la *Certicom Corporation*, pour développer et commercialiser l'ECC.

Les courbes elliptiques ne sont pas le seul type de courbes qui peut être utilisé pour la cryptographie. En 1989, j'ai proposé d'utiliser les groupes de jacobiennes des courbes hyperelliptiques. Ces dernières années, beaucoup de recherches, en particulier en Allemagne, ont été consacrées aux cryptosystèmes à courbes hyperelliptiques.

DES MATHEMATIQUES TOUJOURS PLUS SOPHISTIQUEES

Au début de septembre 1998, quelques jours avant de partir pour une année sabbatique à l'Université de Waterloo, j'ai reçu un e-mail de Joe Silverman[17], mathématicien à l'Université Brown, qui avait écrit un excellent manuel en deux volumes pour étudiants de troisième cycle sur les courbes elliptiques. Son message décrivait un nouvel algorithme, qui se proposait de résoudre le problème du logarithme discret elliptique, en un mot, de casser la cryptographie à courbe elliptique.

Silverman a appelé son algorithme « *xedni calculus* » comme « *index* » épelé à l'envers. Son idée générale était d'exécuter les étapes semblables à celles de l'algorithme de calcul du logarithme (*index calculus*), mais dans l'ordre inverse.

La raison pour laquelle Silverman pensait que son algorithme pouvait éventuellement être efficace reposait sur une relation profonde et difficile qu'on appelle la conjecture de Birch et Swinnerton-Dyer. Ironie du sort, dans un livre intitulé *Algebraic Aspects of Cryptography*, que j'avais publié quelques mois auparavant, j'avais inclus une discussion de cette conjecture

---

[16] NdT. : il est le co-auteur d'un important manuel de cryptologie, *Handbook of Applied Cryptography*.

[17] NdT. : Joseph H. Silverman (né en 1955), professeur de mathématiques à Brown University, a fondé la *NTRU Cryptosystems* en 1996 avec plusieurs collègues pour commercialiser leurs algorithmes cryptographiques.

dans une section que j'avais appelée « Bagage Culturel ». Mon ton était plein d'excuses envers mes lecteurs qui prenaient de leur temps pour lire des mathématiques qui, en dépit de leur grand intérêt pour les théoriciens, avaient peu de chances, disais-je, d'être jamais appliquées à la cryptographie. Puis, pendant une année, j'ai intensivement étudié l'attaque de Silverman sur l'ECC, qui reposait justement sur l'idée sous-jacente de cette conjecture. Cela montre qu'il est imprudent de prédire que certaines mathématiques ne seront jamais utilisées en cryptographie.

Scott Vanstone et ses collègues de Certicom étaient extrêmement inquiets de l'algorithme de Joe Silverman, parce qu'ils craignaient que les concurrents doutant de l'ECC, en particulier à la *RSA Company*, ne s'en emparent comme un argument contre l'utilisation des courbes elliptiques.

Les premiers mois de mon année sabbatique furent consacrés à une analyse approfondie de l'algorithme de Silverman. En octobre, j'ai trouvé un argument théorique, reposant sur le concept de « hauteur » de points, montrant que, pour des groupes de courbes elliptiques très grands, l'approche *xedni* serait extrêmement inefficace. Cependant, avec cette ligne générale de raisonnement, je ne pouvais pas être plus précis sur les tailles pour lesquelles l'algorithme ne serait pas applicable. Il était concevable, même si je le pensais peu probable, que l'algorithme ne soit pas totalement inapplicable pour les courbes dans la gamme de taille qui est utilisée en cryptographie.

Il est important de comprendre qu'une quelconque garantie de sécurité ne peut pas s'appuyer sur un résultat asymptotique, tel mon argument théorique établissant l'inefficacité de *xedni* comme limite lorsque la taille du groupe augmente. Il faut plutôt analyser l'algorithme pour les tailles de courbes elliptiques employées en cryptographie. L'argument asymptotique peut être utile comme un guide, et il nous a certainement fait espérer que nous serions en mesure de démontrer que *xedni* était impraticable pour les courbes réellement utilisées, mais il ne peut servir de substitut à une analyse concrète de sécurité. Il s'est avéré être beaucoup plus difficile et plus long de mener à bien cette analyse que cela ne l'avait été pour arriver au résultat asymptotique avec l'argument théorique.

Afin de répondre à la question cruciale de l'efficacité de *xedni* pour les courbes elliptiques utilisées en pratique, j'ai travaillé avec un groupe pluridisciplinaire de jeunes mathématiciens et informaticiens au Centre de Recherche Cryptographique Appliquée de Waterloo, en particulier avec Edlyn Teske, Andreas Stein, et Michael Jacobson. Nous étions en constante communication avec Joe Silverman, qui nous a donné des suggestions sur la meilleure façon de tester son algorithme. Finalement, vers la mi-décembre, nous avions fait assez de calculs et Silverman a convenu que son algorithme n'était pas applicable. En fait, c'est un euphémisme – il s'est avéré que son

algorithme est probablement le plus lent jamais imaginé pour trouver le logarithme discret sur une courbes elliptique.

C'était néanmoins une idée élégante, et notre étude sur *xedni* fut un projet stimulant. La tentative d'attaque de Silverman sur la cryptographie à courbe elliptique illustre l'utilisation croissante de l'arithmétique et de la géométrie algébrique en cryptographie à clé publique.

Dans les années 1990, un autre exemple de la plus grande sophistication de la cryptographie mathématique a été la proposition de Gerhard Frey[18] d'utiliser la descente de Weil[19] pour trouver les logarithmes discrets sur les courbes elliptiques. Des algorithmes sous-exponentiels pour les logarithmes discrets sur courbes hyperelliptiques de genre élevé avaient déjà été mis au point sur une idée d'Adleman et Huang, et l'idée de Frey était de transférer le problème du logarithme discret sur une courbe elliptique vers une courbe hyperelliptique de genre élevé. La proposition de Frey a été étudiée par Galbraith, Gaudry, Hess, Menezes, Smart, Teske, et d'autres, et il a été démontré que cela conduisait à un algorithme plus rapide dans un petit nombre de cas.

Des progrès ont été également accomplis dans la recherche de méthodes très rapides pour compter le nombre de points sur une courbe elliptique générée aléatoirement. La première étape dans ce sens a été accomplie par Schoof dans un document de 1985, utilisant les polynômes de division. Par la suite, de meilleurs algorithmes ont été mis au point en utilisant les formes modulaires et des techniques *p*-adiques.

Le rapport annuel des séries de conférences ECC, qui est maintenant dans sa onzième année (voir http://www.cacr.math.uwaterloo.ca), indique bien la quantité de recherche consacrée aux applications cryptographiques des courbes elliptiques ces dernières années.

Un tout nouveau type de cryptographie à courbe elliptique a été développé aux environs de l'année 2000, à la suite des idées d'Antoine Joux, Dan Boneh, et Matt Franklin. Il s'est avéré que les appariements de Weil et Tate sur les courbes elliptiques pourraient être utilisés pour réaliser des fonctionnalités cryptographiques qui n'étaient pas possibles auparavant (ou avaient été réalisées inefficacement), notamment, le chiffrement avec l'identité (où la clé publique est, disons, l'adresse e-mail) et des signatures numériques ultra-courtes. La cryptographie avec appariement a été un domaine actif de la recherche. En juillet 2007, la première d'une série de

[18] NdT. : Gerhard Frey (né en 1944) est un mathématicien allemand spécialiste de la théorie des nombres, qui a enseigné dans plusieurs universités des États-Unis. Ses recherches sur les courbes elliptiques ont alimenté la preuve de Wiles du grand théorème de Fermat.

[19] André Weil (1906-98) fut un des membres fondateurs du groupe Bourbaki, et initiateur de la cohomologie galoisienne. Ses importants travaux concernent essentiellement la géométrie algébrique et la théorie des nombres.

conférences entièrement consacrées à ce type de cryptographie à courbe elliptique a eu lieu au Japon[20].

LA DIVISION DE LA COMMUNAUTE MATHEMATIQUE

En dépit de ces merveilleux exemples d'applications de mathématiques intéressantes en cryptographie, il y a eu aussi un inconvénient, en fait, deux inconvénients. Ce sera l'objet de la suite de cet article.

Tout d'abord, il y a eu un effet d'entraînement. Un jour, dans les années 1990, le *Canadian Natural Sciences and Engineering Research Council* m'envoya une longue proposition à évaluer, émanant d'un groupe dirigé par un mathématicien de premier plan, affirmant que la recherche proposée serait importante en cryptographie. Après avoir lu la description du projet, il fut clair pour moi que (1) la proposition était solide d'un point de vue mathématique, et (2) ils ne connaissaient rien en cryptographie. Il est triste que sous la pression, certains mathématiciens éprouvent le besoin de présenter leurs recherches comme ayant un lien avec la cryptographie.

À la fin des années 1980, la NSA s'est rendu compte qu'elle avait commis une erreur en divisant la communauté mathématique plusieurs années auparavant, et elle voulait rétablir les relations. La meilleure façon de se réconcilier avec le milieu universitaire était de donner de l'argent. Ils ont donc mis en place un système de subventions qui est devenu une source majeure de financement dans certains domaines comme la théorie des nombres.

La plupart du temps, il est bénéfique que davantage d'argent arrive pour les mathématiques – quels que soient les motifs du donateur. Cependant, cela peut aussi engendrer de subtils effets négatifs. Il y a plusieurs années, William Thurston (NdT. : 1946-2012) et d'autres nous ont avertis des dangers d'une trop grande dépendance vis-à-vis du financement militaire. Et l'année dernière dans les *Notices,* David Eisenbud a écrit[21] ce que j'ai considéré comme une réfutation éloquente de l'argument (sur la base des avantages supposés de la collecte de fonds) en faveur d'un programme de bourses de l'AMS (*American Mathematical Society*).

Au début des années 1990, j'ai reçu une proposition de la NSA pour le financement d'une conférence sur les modules de Drinfeld. La conférence semblait être une bonne idée, et j'en ai fait un rapport positif dans son ensemble. Cependant, le ton d'une partie de la proposition m'ennuyait. Dans un paragraphe sur « l'effet de la conférence sur la compétitivité des

[20] NdT. : il s'agit de la conférence *Pairing* : http://www.pairing-conference.org/2007/.
[21] NdT. : Eisenbud, D., « Science or Politics at the AMS ? – A Divisive Proposal », august 2006, vol. 53, n° 7, pp. 757-758.

mathématiques américaines », les auteurs tentaient de diviser le terrain entre mathématiques américaines et non-américaines, et promouvaient la conférence au motif qu'elle augmenterait la position concurrentielle des premières. J'ai commenté :

> « Les mathématiques sont sans doute la plus internationale des disciplines intellectuelles. Interaction et travail en commun traversent facilement les frontières nationales. Ainsi, il est généralement impossible de déterminer – et il ne sert à rien de chercher à le faire – la proportion de crédit à attribuer à chaque pays. Un tel ton chauvin n'est pas en harmonie avec l'esprit coopératif et international de la profession mathématique... Qu'ils aient écrit cet article à partir d'une inquiétude sincèrement ressentie sur la « compétitivité des mathématiques américaines » ou que ce soit en réponse à ce qu'ils pensaient être l'état d'esprit à la NSA, j'espère vraiment que dans l'avenir, ils supprimeront de telles absurdités dans les appels à projets ».

Apparemment, la disponibilité de l'argent de la NSA avait eu un effet corrupteur sur certains mathématiciens, qui ont commencé à penser en termes nationalistes et chauvins, jusqu'à rédiger leur proposition d'une façon qui selon eux plairait à la NSA.

LES MATHEMATICIENS PRENNENT EN MARCHE LE TRAIN DE LA CRYPTOGRAPHIE

En même temps que les mathématiciens essayaient de prendre en marche le train de la crypto, les cryptographes ont découvert la puissance que l'aura de la certitude mathématique peut avoir dans les situations de compétition. Ils ont commencé à démontrer des théorèmes mathématiques censés garantir la sécurité de leur système, l'idée étant de convaincre les autres que leur système était sûr à 100 %. Il s'agit du deuxième « côté obscur » qui s'est développé dans la relation entre mathématiques et cryptographie, chaque groupe cherchant des moyens pour exploiter le statut de l'autre groupe afin de faire progresser son propre intérêt. Avant d'expliquer cette utilisation (ou mauvaise utilisation) des mathématiques plus en détail, je voudrais commenter un choc des cultures entre mathématiques et recherche cryptographique.

En 1996, j'ai été président du comité de programme de la conférence *Crypto*. Pour une personne de formation mathématique, ce fut une expérience troublante. Environ les deux tiers des soumissions sont arrivés par la poste dans les 48 heures avant l'échéance finale. Un bon nombre d’entre elles avait de toute évidence été élaboré dans la précipitation, pleines d'erreurs typographiques. Un auteur m'avait envoyé uniquement les pages

impaires. Quelques-uns avaient violé l'obligation d'anonymat (il y avait une politique de rapporter en double-aveugle). Plusieurs n'avaient pas tenu compte des lignes directrices qui avaient été mises à leur disposition. Et dans de nombreux cas, les documents étaient peu originaux, ils n'étaient que de légères améliorations de publications des mêmes auteurs l'année précédente ou une modification mineure du travail d'un autre.

À certains égards, la situation a encore empiré avec les soumissions électroniques. Alfred Menezes, le président de programme de *Crypto* 2007, m'a dit que sur 197 soumissions, 103 sont arrivées dans les onze heures précédant la date limite et 35 sont arrivées dans la dernière heure.

La publication de travaux mathématiques fonctionne différemment. Tout d'abord, la plupart des articles sont publiés dans des revues, pas dans des actes de conférences – et les revues n'ont pas d'échéance. En second lieu, les mathématiciens ont tendance à avoir une piètre opinion des auteurs qui se précipitent pour publier un grand nombre de petits articles – le terme péjoratif est LPU (*Least Publishable Unit*, plus petite unité publiable), plutôt que d'attendre d'être prêts à publier un traitement exhaustif du sujet dans un seul article.

Les départements de mathématiques pensent en général que :

CONJECTURE. *Pour le développement des mathématiques, il est préférable pour une personne de publier un excellent article en* n *années plutôt que* n *documents sans valeur en un an.*

Dans certains autres domaines scientifiques – y compris malheureusement la science informatique et la cryptographie – la conjecture similaire, bien que probablement tout aussi vraie, n'est généralement pas admise.

La cryptographie a été fortement influencée par la culture disciplinaire de la science informatique, qui est tout à fait différente de celle des mathématiques. Certaines explications de la divergence entre les deux domaines pourraient être une question d'échelle de temps. Les mathématiciens, qui héritent d'une riche tradition millénaire, perçoivent le temps qui passe à la manière d'un éléphant. Dans cette façon de voir, il y a peu de conséquences si leur grand article paraît cette année ou la suivante. La science informatique et la cryptographie, au contraire, sont influencées par le monde des entreprises de haute technologie, avec leur course frénétique pour être la première à apporter de nouveaux gadgets sur le marché. Les cryptographes voient ainsi le temps passer à la manière d'un colibri. Les meilleurs chercheurs s'attendent à ce que pratiquement toutes les conférences incluent un ou plusieurs documents vite faits par eux ou par leurs élèves.

Ces dernières années, Alfred Menezes et moi avons écrit une série de documents qui critiquent le domaine de la cryptographie connu sous le nom

de sécurité prouvable. (voir http://eprint.iacr.org/2004/152.pdf, http://eprint.iacr.org/2006/229.pdf, et http://eprint.iacr.org/2006/230.pdf). Bien que les documents aient été largement téléchargés et la plupart des réactions favorables, notre travail dans ce domaine n'a pas été bien accueilli par tout le monde. Beaucoup de spécialistes en cryptographie théorique ont mal perçu notre intrusion dans leur domaine.

Dans les années 1980, il semblait que tous les cryptographes étaient heureux de voir affluer les mathématiciens. Vingt ans plus tard, cependant, j'ai l'impression que certains d'entre eux préféreraient simplement nous voir partir.

L'idée de « sécurité prouvable » est de donner la preuve mathématiquement rigoureuse d'une garantie conditionnelle de la sécurité d'un protocole de chiffrement. Elle est *conditionnelle* en ce qu'elle est généralement de la forme « notre protocole n'est à l'abri d'une attaque de type X qu'à la condition que le problème mathématique Y soit calculatoirement difficile »[22].

Ici, le mot « protocole » désigne une suite particulière d'étapes qui se trouvent réalisé dans une application particulière de la cryptographie. Depuis les débuts de la cryptographie à clé publique, il est traditionnel d'appeler deux utilisateurs *A* et *B* du système par les noms d'« Alice » et de « Bob ». Donc, une description d'un protocole peut être : « Alice envoie à Bob ..., puis Bob répond avec ..., puis Alice répond avec ... », et ainsi de suite.

La forme que prennent les preuves de sécurité est vue comme une *réduction*. La réduction d'un problème à un autre survient implicitement tout au long des mathématiques ; en informatique, les réductions sont le principal outil utilisé pour comparer et classer les problèmes selon leur difficulté.

Dans les articles sur la sécurité prouvable, les auteurs tentent de prouver que le problème mathématique qui est généralement considéré comme difficile, tel que la factorisation des entiers ou la recherche du logarithme discret sur une courbe elliptique, est *réductible* à la réussite d'une certaine attaque contre leur protocole cryptographique. Cela signifie que toute personne qui pourrait briser leur cryptosystème peut aussi, avec seulement un peu plus d'effort, résoudre le problème mathématique supposé difficile. Comme par hypothèse, cela n'est pas possible, il est donc prouvé que le protocole est sûr.

Pour les mathématiciens qui étudient la littérature sur la sécurité prouvable, comme Menezes et moi l'avons fait, il y a plusieurs raisons d'être inquiets. De toute évidence, un théorème de sécurité prouvable s'applique uniquement aux attaques d'un genre spécifié et ne dit rien sur les attaques astucieuses qui pourraient ne pas être incluses dans le théorème. En outre, le

[22] Voir le chapitre « Les nouvelles orientations de la cryptographie » p. 192.

résultat est fortement conditionnel. Contrairement aux mathématiques, où une condition sur un théorème signifie habituellement quelque chose comme « en supposant que l'hypothèse de Riemann est vraie » (ce qui est presque certain), en cryptographie la condition est du type « en supposant que personne ne trouve d'amélioration pour un algorithme résolvant un certain problème de maths » ce qui est une totale énigme. L'histoire n'a pas été concluante pour ce dernier type d'hypothèse. Par exemple, à la fin des années 1980 et au début des années 1990, le développement de l'algorithme de factorisation du crible du corps de nombres pour un module RSA a entraîné une diminution drastique du temps d'exécution des algorithmes de calcul de logarithme et de factorisation de $\exp(\log(n)^{1/2+\varepsilon})$ à $\exp(\log(n)^{1/3+\varepsilon})$.

SECURITE PROUVABLE ?

Les résultats de sécurité prouvable sont souvent utilisés pour impressionner ceux qui sont étrangers au domaine et qui comprennent peu leur véritable signification. Supposons que certaines personnes utilisent la cryptographie à clé publique pour protéger des numéros de carte de crédit pour l'e-commerce, afin de préserver la confidentialité des dossiers médicaux, ou de créer des signatures numériques. Comment peuvent-elles être certaines que le système est sécurisé ? Pour les non-spécialistes, « sécurité prouvable » signifie qu'il y a une garantie à toute épreuve comme peut l'être une preuve du théorème de Pythagore. À notre avis, ceci est très trompeur.

Il y a aussi une difficulté qui vient de la culture disciplinaire de la cryptographie que j'ai commentée plus haut. Habituellement, des articles sont écrits sous la pression de l'échéance, davantage à la manière d'un journaliste que d'un mathématicien. Et ils ont rarement lu les articles d'autres auteurs avec soin. En conséquence, même les meilleurs chercheurs publient parfois des documents contenant des erreurs graves qui vont passer inaperçues pendant des années.

En 1994, deux des plus grands spécialistes dans ce nouveau domaine qu'est la sécurité prouvable, Mihir Bellare et Phillip Rogaway, ont proposé une méthode de chiffrement basée sur RSA qu'ils ont appelé OAEP[23] (le O est pour « optimal », un mot bien galvaudé dans le monde hyper branché de la *high-tech*). Ils ont estimé que les preuves de sécurité devaient être suffisamment détaillées pour obtenir des garanties concrètes pour des tailles

[23] NdT. : Bellare M., Rogaway P., *Optimal Asymmetric Encryption – How to encrypt with RSA*. Extended abstract in A. De Santis (ed.), *Advances in Cryptology - Eurocrypt '94 Proceedings*, Lecture Notes in Computer Science, vol. 950, New-York, Springer Verlag, 1995.

de clés et un choix de paramètres spécifiés. En partie grâce à la preuve de sécurité qui accompagnait OAEP, il a été adopté pour servir dans une nouvelle norme de cartes *Visa* et *MasterCard*. Il s'est avéré, cependant, que la preuve était fausse, comme Victor Shoup l'a découvert sept ans plus tard[24]. Ce fut un peu un scandale qui a conduit beaucoup de gens à s'interroger sur la qualité du contrôle des documents de sécurité prouvable.

Si un lecteur attentif et perspicace se livre à un examen sérieux – et Alfred Menezes est un tel lecteur –, alors les erreurs dans les preuves sont découvertes beaucoup plus rapidement. Une affaire qui à bien des égards est encore plus frappante que celle de OAEP est la panique récente autour d'un ensemble d'« améliorations » de protocoles d'échange de clés conçus par Hugo Krawczyk. En février 2005, Krawczyk, un chercheur de premier ordre en matière de sécurité prouvable qui travaille pour IBM, a présenté un document à *Crypto* 2005, dans lequel il prétendait avoir trouvé des failles dans le système d'échange de clés Menezes-Qu-Vanstone (MQV). Il l'a remplacé par une version modifiée (HMQV) qui selon lui, était à la fois plus efficace et prouvée sûre. Si ses revendications avaient été valides, cela aurait été une source d'embarras majeur, non seulement pour Menezes et ses co-auteurs, mais aussi pour la NSA, qui avait accordé une licence à MQV de *Certicom*, et que ses experts avaient étudié attentivement.

Krawczyk n'avait pas envoyé son papier à Menezes ni aux autres concepteurs de MQV avant de le soumettre, ce qui aurait été considéré comme une courtoisie standard dans le monde scientifique. Mais ce qui me semble plus scandaleux, c'est que personne non plus, au sein du comité de programme de *Crypto* 2005, ne l'avait fait. Ils se sont apparemment précipités pour accepter le papier après une simple lecture superficielle. Lorsqu'enfin Menezes a obtenu une copie du document – après qu'il ait été accepté par le comité de programme – il a tout de suite vu que les défauts que Krawczyk a listés dans MQV reposaient sur des malentendus ou étaient des points théoriques mineurs sans signification pratique.

Plus important encore, Menezes a constaté que le principal argument de l'article était fallacieux. Krawczyk a affirmé que dans son système d'échange de clé modifié, il pourrait augmenter l'efficacité en éliminant une certaine vérification de sécurité (appelée « validation de clé publique ») mise dans MQV pour empêcher des attaques connues. C'est sa « preuve » de sécurité qui lui a donné la confiance nécessaire pour le faire. Mais Menezes a rapidement constaté que certains des protocoles HMQV succombent aux mêmes attaques que MQV si ces contrôles de sécurité n'avaient pas été mis en place. Ensuite, voyant que quelques-unes des conclusions des théorèmes de Krawczyk étaient fausses, Menezes a commencé la lecture soigneuse de

[24] NdT. : Shoup, V., « OAEP reconsidered », 2001, *in Crypto '01 Proceedings of the 21rst Annual International Cryptology Conference on Adavances in Cryptology*, pp. 239-259.

la « preuve » jusqu'à ce qu'il tombe sur une lacune manifeste dans l'argumentation.

Krawczyk et les rapporteurs du comité de programme avaient été tellement hypnotisés par la « preuve » qu'ils n'ont pas réussi à utiliser le sens commun. Toute personne travaillant en cryptographie devrait réfléchir avec soin avant d'abandonner une étape de validation mise en place pour prévenir des problèmes de sécurité. Certes, quelqu'un ayant l'expérience et l'expertise de Krawczyk n'aurait jamais fait une telle bourde s'il n'avait pas été trop confiant en raison de sa « preuve » de sécurité. Comme beaucoup d'autres idées à la mode – des abris souterrains des années 1950 au bouclier anti-missile des années 1980 – les « preuves » de sécurité d'un protocole cryptographique donnent souvent une fausse confiance qui aveugle quant aux dangers véritables.

Dans notre premier article sur la sécurité prouvable, Menezes et moi nous sommes opposés à cette terminologie :

> « Il y a deux connotations malheureuses du mot « preuve » qui viennent des mathématiques et qui rendent le mot inapproprié dans les discussions sur la sécurité des systèmes cryptographiques. La première est la notion de certitude à 100 %. La plupart des gens qui ne travaillent pas dans une spécialité donnée voient un « théorème » qui est « prouvé » comme quelque chose qu'ils devraient accepter sans broncher. La seconde connotation est une suite compliquée et hautement technique d'étapes. D'un point de vue psychologique et sociologique, une « preuve d'un théorème » est une notion intimidante : c'est quelque chose que personne en dehors d'une élite étroite de spécialistes n'est susceptible de comprendre dans le détail ni de mettre en doute. Autrement dit, une « preuve » est quelque chose qu'un non-spécialiste ne s'attend pas vraiment à lire ni à examiner.
>
> Le mot « argument », que nous préférons ici, a des connotations très différentes. Un « argument » est quelque chose qui devrait être largement accessible. Et même un argument raisonnablement convaincant n'est pas supposé être à 100 % définitif. Contrairement à la « démonstration d'un théorème », un « argument à l'appui d'un énoncé » suggère quelque chose que toute personne bien éduquée peut essayer de comprendre, voire d'interroger ».

Menezes et moi avons également étudié certains des problèmes subtils d'interprétation des résultats de la sécurité prouvable. Même lorsque les preuves sont correctes, elles masquent souvent un grand saut d'« ajustement ». Cela signifie que dans l'argument de réduction, l'attaque sur le protocole doit être répétée des millions de fois pour résoudre le problème calculatoirement difficile. Dans ce cas, la garantie pratique que l'on obtient est très faible. Menezes a trouvé quelques exemples extrêmes de ce problème de « non ajustement » dans quelques cas bien connus d'articles sur des générateurs de nombres aléatoires. Dans un article, il s'est avéré que,

si vous suivez attentivement l'argument de l'auteur avec la valeur recommandée du paramètre, tout ce qu'il a vraiment prouvé, c'est qu'un attaquant aurait besoin d'au moins 10^{-40} nanosecondes pour casser le système. C'est beaucoup moins de temps que ce que met la lumière pour parcourir un micron.

Ce qui s'est passé, c'est que les valeurs des paramètres avaient été recommandées sur la base d'un théorème asymptotique. Ce théorème dit que, quand N tend vers l'infini, vous pouvez en toute sécurité générer $O(\log \log N)$ symboles binaires pseudo-aléatoires à chaque fois que vous effectuez une élévation au carré modulo le nombre N composite (ici, « en toute sécurité » signifie, *grosso modo*, que personne ne peut distinguer entre la séquence produite et une séquence vraiment aléatoire par un algorithme qui fonctionne dans un temps raisonnable). Cependant, comme je l'ai mentionné lors de la discussion du calcul *xedni* de Joe Silverman, il est fallacieux d'utiliser un résultat asymptotique comme une garantie pratique de sécurité. On a plutôt besoin d'effectuer une analyse détaillée pour une gamme réaliste de paramètres. Il est souvent beaucoup plus difficile (comme pour *xedni*) de mener à bien cette analyse concrète que de prouver le théorème asymptotique, et parfois les conclusions ne sont pas ce que l'on pourrait espérer. Dans le cas du générateur pseudo-aléatoire de symboles binaires, l'analyse (si l'on suppose que $\log_2 (\log_2 N)$ symboles binaires sont pris à chaque itération, comme recommandé) conduit à une minoration absurde de la quantité de temps dont un adversaire aurait besoin pour attaquer avec succès le générateur.

L'HYPOTHESE DE L'ORACLE ALEATOIRE

L'histoire de notre premier article sur la « sécurité prouvable » a une suite amusante. Juste avant de devoir paraître dans *Journal of Cryptology* et presque deux ans après avoir été accepté pour publication, un membre du comité de rédaction s'est fermement opposé à son acceptation par le journal. Bien qu'il ait été trop tard pour bloquer la publication, le rédacteur en chef avait été suffisamment inquiété pour écrire une préface dans l'édition de janvier 2007 où il justifiait sa décision de publier.

Le membre du conseil éditorial qui s'opposait à notre article était Oded Goldreich de l'Institut Weizmann, qui est l'un des chefs de file israélien en science informatique et un grand nom (certains diraient LE grand nom) de la cryptographie théorique. Lorsqu'il fut incapable d'empêcher la publication de notre article dans le *Journal of Cryptology*, il a posté sur le serveur de prépublications en cryptographie ePrint, un essai de 12 pages intitulé « La Cryptographie Postmoderne » qui s'en prenait à nous sur des positions

philosophiques (voir http://eprint.iacr.org/2006/461)[25]. Il a accusé Menezes et moi d'être « post-modernes » et « réactionnaires », car nos critiques de la sécurité prouvable « faisaient le jeu des adversaires du progrès ».

La partie de notre article qui semble avoir le plus irrité Goldreich, est notre explication de la raison pour laquelle nous n'avons pas été convaincus par certains arguments que lui et d'autres ont avancé dans le but de se débarrasser de la prétendue hypothèse de « l'oracle aléatoire ». L'hypothèse de l'oracle aléatoire concerne ce qu'on appelle les « fonctions de hachage » (de courtes chaînes de symboles qui agissent comme une sorte d'« empreinte digitale » d'un message). Cette hypothèse dit essentiellement que l'empreinte digitale donnée par une fonction de hachage, bien que construite, est en pratique impossible à distinguer d'un échantillon d'une chaîne aléatoire de symboles. Il s'agit d'une hypothèse intuitivement raisonnable, et dans notre document, nous avons fait valoir que toutes les tentatives visant à s'en débarrasser – même celles que les auteurs affirmaient être d'intérêt pratique – utilisaient en fait des constructions qui ne respectent pas les principes cryptographiques de base et donc n'ont aucun rapport avec la cryptographie du monde réel. Nous avons conclu notre discussion en disant que « notre confiance dans l'hypothèse de l'oracle aléatoire reste inébranlable ».

Goldreich a répondu à cela en ramenant sur nous la colère de l'Ancien Testament. Nous accusant de faire de l'oracle aléatoire un « fétiche », il a raconté une histoire de la Bible que notre article lui rappelait (dans ce qui suit, j'ai conservé la mise en forme, la casse, et l'orthographe de l'original) :

> « En effet, ce qui s'est passé avec le modèle de l'oracle aléatoire nous rappelle le récit biblique du Serpent d'airain, reproduit ci-après. (voir Nombres (21:4-8) et 2 Rois (18:4).). Pendant le voyage du peuple d'Israël dans le désert, le Seigneur a ordonné au prophète et dirigeant Moïse de réaliser un « serpent ardent » comme un moyen symbolique pour guérir les gens qui avaient été mordus par des serpents (qui avaient auparavant été envoyés par le Seigneur comme une punition pour un péché antérieur). Plusieurs centaines d'années plus tard, le serpent de bronze fabriqué par Moïse est devenu une idole objet d'un culte. Cela a conduit le roi juste Ezéchias (fils d'Achaz) à émettre l'ordre de réduire ce serpent de bronze en pièces. Laissez-nous affirmer que l'ordre du roi était *de détruire un objet qui a été construit sur l'instruction directe du Seigneur*, parce que cet objet est devenu un fétiche. En outre, cet objet ne sert plus le but pour lequel il a été construit. Cette histoire illustre le processus par lequel une bonne chose peut devenir un fétiche, et ce qu'il faut faire dans un tel cas.... Compte tenu du tournant que prend cette affaire, il nous semble bon d'abolir le modèle de l'oracle aléatoire ».

[25] NdT. : voir aussi Godereich, O., « On Post-Modern Crytpography », *Journal of Cryptology*, http://www.wisdom.weizmann.ac.il/.

Goldreich se voit comme le roi juste Ezéchias du vingt-et-unième siècle, défendant les chercheurs en sécurité prouvable contre les infidèles et post-modernes fétichistes comme Menezes et moi. Il est clair dans son essai qu'il n'avait pas lu notre article attentivement avant d'écrire sa réponse. Il ne semble pas non plus avoir été au courant de nos deux autres articles critiquant la sécurité prouvable. Mais bien sûr, il n'était pas nécessaire de lire vraiment les détails techniques de nos trois articles[26] pour nous dénoncer sur des bases religieuses et philosophiques.

Les réactions de colère de quelques chercheurs qui semblent percevoir notre travail comme une menace contre leurs intérêts ne sont pas le genre de choses qui se rencontre normalement en mathématiques théoriques[27], où habituellement les seules questions qui peuvent conduire quelqu'un à objecter un document sont une erreur ou une omission de la reconnaissance d'un travail antérieur (qui n'a été trouvée dans aucun de nos trois articles sur la sécurité prouvable). Mais loin d'être dérangé par les accusations formulées par Goldreich et d'autres, je me trouve encouragé par celles-ci, car elles montrent au moins que les gens y prêtent attention.

CONCLUSION

La cryptographie a ceci d'excitant d'être bien plus qu'un simple champ académique. Une fois, j'ai entendu un orateur de la NSA déplorer que les chercheurs universitaires puissent proposer de manière cavalière des cryptosystèmes non testés. Il a souligné que, dans le monde réel, si votre cryptographie échoue, vous perdez un million de dollars ou votre agent se fait tuer. Dans le milieu universitaire, si vous écrivez sur un cryptosystème, et que vous trouvez un moyen de le casser quelques mois plus tard, cela vous fait deux publications à ajouter à votre CV !

Drames et conflits sont inhérents à la cryptographie qui, en fait, peut être définie comme la science de la transmission et de la gestion des informations en présence d'un adversaire. La mentalité « espion contre espion », faite de compétition et de rivalité permanente s'étend à la culture

[26] NdT. :
– Koblitz N., Menezes A., J., « Another Look at 'Provable Security' », 2007, *Journal of Cryptology*, vol. 20, Issue 1, pp. 3-37,
– Koblitz N., Menezes A., J., « Another Look at 'Provable Security'. II », 2006, *Progress in Cryptology – INSOCRYPT 2006, Lecture Notes in Computer Science*, vol. 4329, pp. 148-175.
– Koblitz N., Menezes A., J., « Another Look at generic groups », *Advances in Mathematics of Communications (AMC)*, 2007, vol. 1, issue 1, pp. 13-28.

[27] NdT. : des débats métaphysiques ont pourtant eu lieu dans l'histoire des mathématiques, par exemple au sujet de la légitimité des nombres négatifs et des nombres imaginaires au 16e siècle, ou encore sur le caractère naturel des nombres entiers que Leopold Kroneker (1823-91) attribuait à Dieu, les autres ensembles numériques étant élaborés par l'homme.

du champ disciplinaire. Cela peut devenir excessif, et même enfantin à certains moments, mais cela explique aussi en partie pourquoi il peut être si amusant de faire de la recherche en cryptographie.