



MÉDAILLE D'OR



CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

La Médaille d'or du CNRS distingue chaque année, depuis sa création en 1954, l'ensemble des travaux d'une personnalité scientifique qui a contribué de manière exceptionnelle au dynamisme et au rayonnement de la recherche française.

JACQUES STERN

Autrefois réservée aux seuls champs militaire et diplomatique, la cryptologie, ou l'art de coder et décoder des informations, est aujourd'hui partout dans notre quotidien. Grâce en partie à un homme, Jacques Stern, fondateur de la nouvelle école française de cryptologie, et à ses recherches impressionnantes. En toute logique, le directeur du Laboratoire d'informatique de l'ENS se voit aujourd'hui remettre la Médaille d'or 2006 du CNRS, la plus haute distinction scientifique française. À cette occasion, revivez le parcours de ce chercheur d'exception et partez à la découverte de ses nombreux travaux. Sans oublier un petit détour par l'histoire fascinante et millénaire de la science du secret.



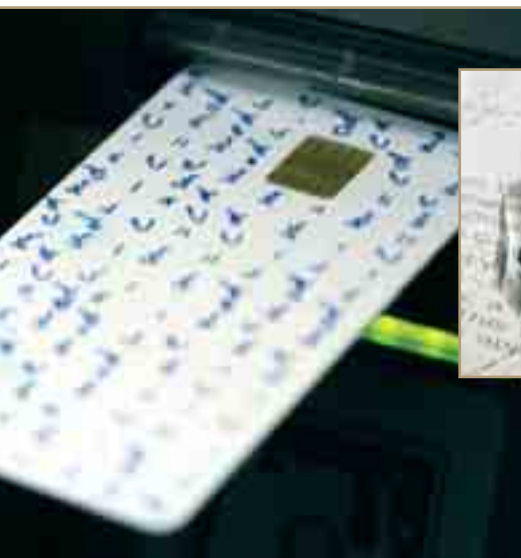




LE GARDIEN DU SECRET

D'ordinaire, pour protéger certaines informations, l'homme au regard pétillant jongle plutôt avec les chiffres et les algorithmes. Mais lorsqu'il s'agit de préserver ses jardins secrets, Jacques Stern, 57 ans, apôtre français de la cryptologie, sait tout aussi bien manier le verbe. Ainsi, dans son antre parisien où la lumière du jour peine à s'introduire, c'est avec aisance que le tout frais médaillé d'or du CNRS vous retrace son parcours en sinuant autour de ses zones interdites. Secret, l'élégant directeur du Laboratoire d'informatique de l'ENS (Liens) qui fait aussi partie du département Sciences et technologies de l'information et de l'ingénierie (ST2I) du CNRS ? Pas exactement. Discret, peut-être. Pudique, assurément. De l'arrivée en France de ses grands-parents à la fin du XIX^e siècle, de ses parents « *aux professions non intellectuelles* » qui lui ont « *assuré une enfance heureuse et sans problème, après les heures noires qu'ils avaient traversées* » et qui ont toujours valorisé ses études, l'on saura donc peu de choses. Juste l'essentiel : cette histoire l'aura mené au sommet de son art, la cryptologie. Qui en réalité rassemble deux disciplines : la cryptographie, qui s'évertue à modifier la forme d'un message pour le rendre étanche aux indiscretions, et la cryptanalyse qui consiste à décoder un message ou, plus généralement, à trouver les failles d'un code secret. Opérations bancaires, achats sur Internet, télépéages ou encore messageries électroniques... Dans les puces de téléphones portables, de cartes vitales et de cartes bleues, la crypto est désormais partout.

Tout comme les travaux de notre homme, génial inventeur et perceur de coffres-forts virtuels. Et père fondateur – la « racine de l'arbre » selon son ancien élève David Pointcheval, aujourd'hui chercheur CNRS au Liens – de l'école moderne française de cryptologie, la meilleure en Europe. Mais comment devient-on le chantre français d'une discipline si obscure, auteur de près de cent cinquante publications, quand on ne s'y convertit qu'à l'âge de trente ans ? La réponse se cache dans le parcours d'exception d'un homme très décidé. Décryptage.



© CNRS Photothèque - Christophe Lebedinsky.

LA CRYPTOLOGIE, UNE RECONVERSION LOGIQUE

Fin des années soixante : après de brillantes études dans deux des meilleurs lycées de la capitale, Jacques Stern a le choix du roi... En effet, l'École normale supérieure et l'École polytechnique lui tendent les bras. Lui opte pour la première dont il sort en 1972, un an après avoir également obtenu l'agrégation de mathématiques. Il rejoint alors l'université Paris-VII où il consacre sa thèse à une branche des mathématiques très proche, même s'il l'ignore encore, de l'informatique : la logique. Son dada ? Des résultats d'impossibilité en théorie des ensembles, des travaux faisant suite à ceux des célèbres Gödel ou Turing. En clair : « *Je travaillais sur les limites de ce que peut faire la théorie des mathématiques* » traduit Jacques Stern, de sa voix douce et posée. Premiers succès, et premier tournant en 1979 : l'université de Caen lui propose la chaire de professeur. « *À l'époque, les jeunes qui brillaient pouvaient grimper très vite. C'est ainsi que je suis arrivé à seulement 30 ans à un grade qui me libérait de tout souci de carrière pendant au moins dix ans !* »

Au-delà de ce confort administratif, notre logicien a pris de l'avance dans ses recherches et dispose dans ses tiroirs de nombreux travaux mathématiques à publier... Autant dire que le futur médaillé a un peu de temps pour réfléchir à la suite de son parcours. En Normandie, il va en profiter pour faire sa mue. Et retrouver le plaisir scientifique qui, cette fois, ne le quittera plus.

Sa reconversion débute par une question : suis-je dans la bonne démarche scientifique ? La réponse fuse, négative : « *Mes recherches consistaient essentiellement à démontrer que telle ou telle chose mathématique était impossible*, précise Jacques Stern. *Bref : aucune application à l'horizon... Moi, j'étais attiré par les sciences au tempo rapide, où les recherches trouvent rapidement des prolongements concrets.* » Heureusement, à l'impossible mathématique, nul n'est tenu... Le déclic ? Il provient du parcours d'un de ses illustres prédécesseurs en matière de logique : le célèbre Alan Turing, souvent présenté comme l'inventeur de l'ordinateur, embauché par les Alliés pour casser les codes allemands durant la seconde guerre mondiale. Car en cryptologie, l'impossibilité est toujours la bienvenue : « *Nous souhaitons tous qu'il soit impossible pour un cambrioleur de pénétrer dans notre domicile. C'est aussi ce que visent les cryptologues, mais pour protéger des informations* » note-t-il. Son choix est fait, conforté par l'émergence de la cryptologie dans le domaine académique depuis 1976 et par l'invention du concept de clef publique (voir *Des résultats à foison*, p. 9), passeport de la cryptologie pour notre quotidien. Les six années suivantes, outre ses cours à l'université

normande, le professeur va les passer à se former, seul, à sa discipline d'accueil et à combler quelques lacunes handicapantes : il apprend à programmer, travaille la théorie des nombres, transite par la « complexité algorithmique », une branche de l'informatique théorique. Et, détail qui vous classe un homme, potasse l'histoire de sa nouvelle science : « *Il me semblait important de me situer dans une dynamique historique. Dans toutes les disciplines, les résultats qui tombent chaque jour s'inscrivent dans une histoire, s'appuient sur une foule de travaux antérieurs. Et en cryptologie, nous avons une histoire multimillénaire derrière nous !* » (voir *3 600 ans de messages cryptés*, p. 14). Le scientifique en tirera d'ailleurs un ouvrage remarquable, *La science du secret*, publié en 1998¹.

¹ *La Science du secret*, Jacques Stern, éd. Odile Jacob, 1998.



© COSMOS

■ Le parcours du mathématicien britannique Alan Turing a certainement inspiré Jacques Stern. Pendant la seconde guerre mondiale, ce logicien fut recruté par le gouvernement de son pays pour décrypter les messages ennemis. Cette vaste opération de cryptanalyse, connue sous le nom d'opération *Ultra*, occupait près de sept mille personnes à la fin de la guerre. Et ne fut pas étrangère au succès final des Alliés.

UNE CARRIÈRE EN OR

1986 : les efforts paient. Son tout premier travail de recherche en lien avec la cryptologie est très remarqué et lui vaut à 37 ans une invitation à son premier colloque international. La suite ? Jacques Stern retourne mener ses recherches à l'université Paris-VII jusqu'en 1992, puis devient pendant un an directeur de recherche au CNRS en détachement à l'École normale supérieure. « *Depuis mon retour à Paris, j'avais régulièrement été invité à l'ENS où je donnais quelques cours : j'étais en quelque sorte le squatter de l'École !* » Il ne va pas le rester longtemps : le retour



© CNRS Photothèque - Christophe Lebedinsky.

officiel au bercail de la rue d'Ulm a lieu en 1993, en tant que professeur. L'enseignement ? « *Une activité essentielle,* répond celui qui fut aussi maître de conférence à l'École polytechnique de 1986 à 1998, *où l'on voit les générations se former, et qui force un chercheur à clarifier ses idées.* » Et dont notre homme tire une de ses plus grandes fiertés, celle d'avoir essaimé un nombre incalculable d'étudiants et thésards aussi bien dans la cryptologie civile que militaire.

En 1996, Jacques Stern prend logiquement la tête du Laboratoire d'informatique de l'ENS, commun au CNRS et à l'ENS, puis celle du département informatique en 1999. Car au fil des ans et des résultats brillants, il s'est naturellement imposé comme le chef de file de la cryptologie française, elle-même leader en Europe.

Ce qui a évidemment un prix... « *En période de création, l'esprit d'un chercheur est mobilisé à temps plein. Combien de fois répondais-je 'oui, oui' à ma femme sans même m'en rendre compte ?* » raconte notre chercheur l'air contrit. Tout juste

le virtuose de la cryptologie trouve-t-il, dans un emploi du temps saturé, un moment pour s'adonner à son autre passion, l'opéra. Et là aussi, le goût est affirmé et se porte sur les œuvres les plus classiques, de Mozart à Puccini en passant par Verdi. « *J'adhère moins à ce qui se fait de plus récent, et même à certaines adaptations modernes qui laissent plus de place à la création qu'à l'interprétation... C'est mon côté conservateur !* »

Dans son domaine, en revanche, Jacques Stern va toujours de l'avant. Une preuve ? Il a participé à une avancée importante pour la société française : la libéralisation de la cryptologie dans l'Hexagone.

En clair, depuis la réglementation adoptée en 1999 et dans laquelle l'expertise de Jacques Stern a beaucoup pesé, tout un chacun a le droit d'utiliser des systèmes cryptographiques comme ceux qui peuplent nos ordinateurs. Jusqu'alors, tout cela nécessitait une autorisation de l'État qui considérait la discipline comme stratégique pour la Défense nationale.

Opportunisme d'un scientifique propulsé expert par l'actualité ? Tout le contraire : Jacques Stern s'est depuis longtemps impliqué dans les relations entre sa science et la société. Parmi ses multiples casquettes, et sans parler de ses travaux pour la Défense française – il a été membre du Conseil scientifique de défense – l'homme appartient toujours au Conseil stratégique des technologies de l'information et à l'Observatoire de la sécurité des cartes de paiement. L'occasion ou jamais de demander à un connaisseur s'il est risqué de faire ses achats en ligne. L'expert botte en touche : « *Des systèmes comme la banque à distance font appel à tout l'arsenal de la cryptologie... Mais Internet reste la zone de tous les dangers. Globalement, la chaîne de sécurité est mesurée par son maillon le plus faible, et ce n'est pas la cryptologie : c'est souvent l'utilisateur naïf, qui par exemple ne met pas à jour régulièrement son système d'exploitation ! Ainsi, de nombreuses solutions de cryptologie ne s'imposent pas aujourd'hui à cause des internautes* », explique notre prudent médaillé en pianotant deux mots de passe successifs juste pour allumer son ordinateur. « *Mais la cryptologie va sûrement évoluer vers de nouveaux concepts pour combler cette faille humaine* » reprend-il aussitôt, avec un regard malicieux. On peut faire confiance à cet homme visionnaire qui a su se tourner vers une discipline avant même son explosion née de l'avènement d'Internet et des nouvelles technologies de l'information et de la communication. Le nez fin ? Pas toujours, pourtant, selon ses propres aveux. Car déjà chevalier de la Légion d'honneur et lauréat du prix Lazare Carnot

2003 de l'Académie des sciences entre autres¹, Jacques Stern avoue ne pas avoir senti le souffle de la Médaille d'or : « *J'avais reçu en 2005 la Médaille d'argent ! Alors autant dire que je n'y pensais même pas...* » Contraint une nouvelle fois

de sortir de l'ombre, l'homme en serait presque gêné. De la même pudeur, peut-être, qui le pousse à ne pas intervenir, malgré sa fierté paternelle, dans la conduite de la start-up de cryptographie montée par ses deux fils et l'un de ses anciens thésards. Ce n'est pourtant un secret pour personne : premier informaticien au palmarès de la Médaille d'or du CNRS, Jacques Stern est définitivement à sa juste place.

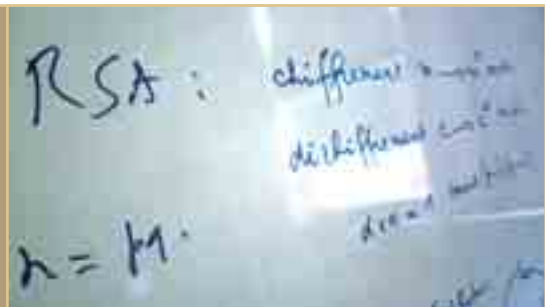
¹ Parmi ses nombreuses distinctions, Jacques Stern a été nommé *Fellow of the International Association for Cryptologic Research* en 2005.

DES RÉSULTATS A FOISON

En 1976, c'est la révolution au pays de la crypto. Avec l'invention de la clef publique (voir *La crypto à clef publique*, ci-dessous), un domaine scientifique nouveau et prometteur s'est ouvert. De plus, les applications bancaires et industrielles s'annoncent légion. Réactive, une communauté de recherche se crée alors. Dans cette émulation, Jacques Stern s'impose rapidement parmi les ténors mondiaux, et entraîne bientôt son laboratoire dans son sillage. Retour sur quelques faits d'armes d'un seigneur de la crypto, dans quatre grands chantiers de la discipline.

LA CRYPTO À CLEF PUBLIQUE

Pendant des millénaires, pour échanger des messages cryptés, deux protagonistes devaient d'abord se rencontrer en cachette pour convenir d'un code (cryptographie symétrique). En 1976, l'invention de la clef publique par Whitfield Diffie et Martin Hellman met un terme à cette pratique : désormais, seule la lecture du message codé nécessite une clef confidentielle (ou cryptographie asymétrique). Un exemple ? Alice veut communiquer en secret avec Bernard et Ève. Elle va alors générer deux clefs de codage complémentaires. La première clef, Alice la donne à qui la veut, sans précaution particulière. Bernard et Ève vont alors s'en servir pour coder leur message. Que seule Alice pourra lire grâce à sa seconde clef, qu'elle a gardée confidentielle. Notons que le premier système de code à clef publique, le RSA créé en 1978, reste pratiquement le seul utilisé à l'heure actuelle.



$$dxe = 1 \pmod{p-1}$$

TROUVER LES FAILLES DANS LES CODES DES AUTRES

« *Partie la plus amusante et la plus confortable de la cryptologie* » selon Jacques Stern, la cryptanalyse est un perpétuel concours de bras de fer. En effet, chaque équipe présente, lors des congrès internationaux, ses nouveaux codes au reste de la communauté mondiale. Sans complaisance, celle-ci va tenter par tous les moyens d'en trouver les failles, avant que ces procédés ne soient mis en service et ne deviennent éventuellement la proie de personnes ou d'organisations pratiquant la cryptanalyse dans un but frauduleux. Et de l'avis général, Jacques Stern est un expert des plus redoutés par tous les inventeurs de codes. Son premier résultat notable, qui lui valut l'admiration immédiate de ses pairs, fut

d'ailleurs dans ce registre. Pour le comprendre, il faut savoir que de nombreuses méthodes

de chiffrement impliquent de tirer un nombre au hasard, un aléa, pour sécuriser davantage le code. En 1987, fraîchement débarqué en terre de crypto, Jacques Stern démontre que la méthode la plus courante pour tirer un aléa dans un programme informatique, appliquée sans problème dans des simulations de phénomènes physiques, n'était pas sûre ! La solution vient alors d'autres méthodes déterministes, issues de constructions mathématiques plus élaborées, qui permettent de tirer un nombre au hasard sans affaiblir le code. Notre homme est d'ailleurs à l'origine de l'une d'entre elles.

Autre illustration de ses qualités de briseur de codes, dans un domaine phare de la cryptologie contemporaine, la recherche d'alternatives au système de chiffrement à clef publique le plus répandu, le RSA (voir *La crypto à clef publique*, p.9), aujourd'hui en situation de quasi-monopole. De nombreuses équipes de par le monde planchent sur des systèmes alternatifs. Jacques Stern et son équipe s'appliquent à en casser une multitude. Leur arme secrète ? Des outils issus de diverses branches des mathématiques. « *Lorsque vous essayez d'attaquer un code, vous cherchez à mettre en évidence ce que les mathématiciens appellent des invariants, c'est-à-dire des éléments dont il reste toujours une trace même après les opérations de codage. Mais vous ignorez a priori le type d'invariant que vous allez rencontrer : statistique, algébrique, voire un mélange des deux.* » Pour surmonter cette difficulté, Jacques Stern a en particulier systématisé l'utilisation de la géométrie des nombres en cryptanalyse. Paradoxalement, cette partie des mathématiques, qui étudie les structures

régulières comme celles rencontrées dans la physique des cristaux, est ainsi devenue une arme de choix entre les mains des cryptanalystes. « Signature » de notre médaillé et de son équipe, elle a fait l'objet de plusieurs thèses, dont celle de Phong Nguyen, actuellement chargé de recherche CNRS au Liens.

Un exemple de victime parmi des dizaines : en 1997, une équipe d'IBM publie un nouvel algorithme qu'elle qualifie d'inviolable. Quelques mois plus tard, l'équipe de Jacques Stern casse ce code grâce à son savoir-faire de perceur de coffre-fort. « *Et pourtant, tout le monde avait raison*, note le logicien, magnanime. *Sur le*

papier, les chercheurs d'IBM ne s'étaient pas trompés, il s'agissait même d'un beau résultat mathématique... Mais inapplicable pour faire entrer les

algorithmes dans la pratique informatique ! » Ne vous méprenez pas pour autant : ceux qui tentent de casser le travail de leurs voisins vont aussi soumettre leurs créations à la vindicte revancharde – mais visiblement bon enfant – de leurs collègues. Jacques Stern n'y déroge pas et a aussi présenté une multitude de codes à sa communauté.



(9-1)

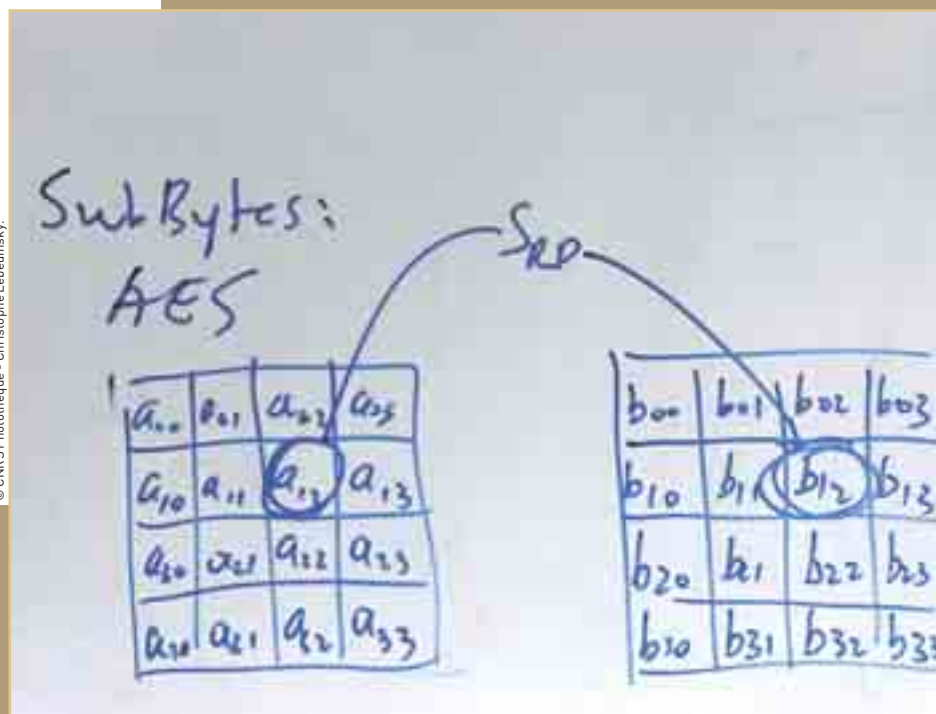
CRÉER DE NOUVELLES MANIÈRES DE CHIFFRER

Le médaillé est également concepteur de nombreux procédés de cryptographie. Face à la difficulté de trouver un remplaçant au RSA, et ce malgré les efforts de la communauté scientifique, Jacques Stern a par exemple développé une approche originale : « Pour certaines applications, sur Internet notamment, il n'est pas nécessaire de coder l'ensemble des informations, explique-t-il. On peut souvent se borner à réaliser une authentification, c'est-à-dire à garantir que chaque protagoniste est certain de l'identité de son interlocuteur. » En se fixant cet objectif plus restreint, on rencontre l'étonnant concept de *zero knowledge* ou « non divulgation ». Issu de la théorie de la complexité, celui-ci permet en effet de réaliser un bien étrange paradoxe : il est possible de prouver son identité à l'aide d'une donnée secrète, sans révéler la moindre information sur ce secret... une alternative bien plus élaborée que les mots de passe habituels. « Il n'y a guère qu'une dizaine de méthodes d'authentification à clé publique qui ont cette propriété de non divulgation et Jacques Stern a laissé son nom à deux d'entre elles », relève David Naccache, professeur à l'université Paris-II, et collègue du médaillé au sein du Liens. La particularité de ces deux méthodes est de s'appuyer sur des mathématiques qui ne relèvent pas de la théorie des nombres, et d'offrir ainsi une réelle alternative au RSA contrairement à la quasi-totalité des autres systèmes proposés.

Mais l'équipe du Liens s'est aussi illustrée dans la création de systèmes à clé publique plus traditionnels, c'est-à-dire s'appuyant sur la théorie des nombres. Elle a ainsi deux systèmes à son actif, qui présentent notamment des propriétés d'additivité. Autrement dit, on peut faire la somme de quantités codées sans avoir à les décoder ! « Si le premier système n'offre pas des performances comparables à celles de RSA en termes de temps de calcul, le second est plus prometteur et ouvre la voie à de nombreuses applications », précise le chercheur.

Toujours dans ce domaine, Jacques Stern et ses collaborateurs ont aussi contribué, entre autres, à la mise au point d'un système d'authentification pouvant s'utiliser « à la volée », par exemple à bord d'une voiture franchissant un télépéage. Il semblerait même que ce système puisse trouver place dans un dispositif sans microprocesseur (de type RFID), ce qui le rendrait particulièrement attractif en termes de coût. De quoi gagner du temps sur la route... et en toute sécurité.

© CNRS Photothèque - Christophe Lebedinsky.



PROUVER LA SÉCURITÉ DES ALGORITHMES

Avant le milieu des années quatre-vingt-dix, le seul critère de sécurité d'un code tenait au fait... que personne n'arrivait à le casser ! Avec l'émergence du concept de « sécurité prouvée », introduit en Europe par l'équipe de Jacques Stern, il s'agit de prouver qu'il n'est pas attaquable. Pour cela, les chercheurs ramènent le problème à une réalité mathématique, par exemple l'impossibilité – en l'état actuel des connaissances – de factoriser des nombres entiers de plusieurs centaines de chiffres. Rien de très surprenant dans le fait qu'un ancien logiciel ait développé cette méthode de preuve. Celle-ci a largement contribué à la notoriété de l'équipe du Liens et a fait l'objet de plusieurs thèses sous la direction de Jacques Stern, dont celle de David Pointcheval, désormais chargé de recherche au CNRS et membre du Laboratoire de l'ENS.

Ainsi, dès 1996, Jacques Stern et son équipe parviennent à prouver la sécurité d'un système de signature numérique, très employé sur Internet. Un tel mécanisme permet de certifier l'identité de l'auteur de messages électroniques en utilisant une clef publique.

« Ainsi, une seule personne peut apposer sa signature – celle qui dispose de la clef privée correspondante – mais tout le monde peut en vérifier l'authenticité. »

Ce succès en appelle d'autres et les chercheurs du Liens étendent leurs recherches au domaine de la monnaie électronique, rencontrant une problématique analogue mais plus complexe. Pour imiter le fonctionnement de la monnaie fiduciaire (pièces et billets), on avait imaginé d'émettre des pièces virtuelles, simples numéros de série signés. La difficulté : s'assurer que personne ne puisse fabriquer de fausse monnaie, par exemple en arrivant à combiner dix signatures reçues pour en créer une onzième. L'équipe du Liens résout le problème en mettant au point le premier système de pièces de monnaie virtuelles à la sécurité prouvée.

Citons encore une autre ligne du palmarès de la sécurité prouvée, commune cette fois aux chercheurs du Liens et à une équipe japonaise : en 2000, la norme OAEP (*Optimal Asymmetric Encryption Padding*), largement utilisée pour « formater » les messages avant de les chiffrer par RSA, est sur la sellette : « Un chercheur venait de montrer, non qu'OAEP fût attaquable, mais que la preuve de son inviolabilité était incorrecte. » L'inquiétude monte sur Internet, dans les forums de discussion. Mais pas longtemps car en peu de temps, nos chercheurs franco-japonais apportent une nouvelle preuve – plus élaborée – établissant que la norme est sûre, sans qu'aucune modification ne soit nécessaire ! Le monde de la cryptologie leur en est encore reconnaissant. D'une manière plus générale, les travaux menés par Jacques Stern et son équipe sont régulièrement cités comme des éléments qui contribuent à la confiance requise pour le développement du commerce électronique et des communications sur Internet.



PROTÉGER LES COMMUNICATIONS SUR LES RÉSEAUX

Son parcours le prouve : le médaillé d'or 2006 sent les grandes tendances à venir. « L'évolution technologique majeure des dix dernières années est la convergence de l'informatique et des télécoms. C'est ce phénomène qui produit les changements majeurs que nous observons : téléphone portable, Internet, numérisation et stockage massif des données, etc. Ce changement pose à la recherche en cryptologie un formidable défi, qui est d'assurer, dans ce contexte nouveau, la confidentialité des communications, l'authenticité des transactions et de protéger les informations personnelles », explique-t-il. Toujours en pointe, Jacques Stern et les chercheurs

de son équipe participent activement aux recherches sur la sécurité des réseaux. C'est ainsi qu'à la demande d'un organisme de normalisation européen, ils ont évalué les algorithmes proposés pour le codage des communications dans la téléphonie mobile dite de troisième génération. Sans déceler de faille ! Conclusion : nous pourrions échanger nos secrets en toute sécurité via les téléphones 3G. Une autre preuve ? Ses travaux, menés avec ses collaborateurs, sur ce qu'il nomme la cryptologie multi-acteurs. « Dans les réseaux, le paradigme traditionnel de la cryptologie – qu'elle soit à clef publique

ou conventionnelle – avec deux partenaires isolés du reste du monde n'est plus approprié. » Les scénarios d'Internet impliquent en effet une multitude d'acteurs, par exemple dans le cas des enchères en ligne. Cela tombe bien : avec son équipe, Jacques Stern a mis au point une méthode d'enchères anonymes sur le Web, qui garantit la confidentialité des informations, et notamment le montant des enchères proposées par les autres participants que le vainqueur. Autre résultat remarqué par la communauté, l'amélioration des schémas de signature collective : « *Ceux-ci correspondent à la possibilité pour chaque participant de signer au nom d'un groupe, de manière anonyme* », précise Jacques Stern. Mais ses travaux les plus prometteurs dans ce domaine concernent le vote électronique, une application où le niveau de garantie en termes de sécurité, d'authenticité, d'anonymat et de secret doit être très élevé. Là encore, les recherches de notre médaillé font référence dans le monde entier. Et ce ne sont que des exemples... Quid de la suite ? Quand on l'interroge sur l'avenir de sa discipline, le médaillé d'or répond avec enthousiasme : « *Il y a une véritable ubiquité de la cryptologie : elle est déjà présente dans les téléphones portables, dans les cartes bancaires, sur Internet, mais elle va aussi intervenir de manière cruciale pour protéger les contenus,*

notamment multimédia, ou pour contrôler l'accès à nos données personnelles, médicales en particulier. La cryptologie n'est donc plus seulement la science du secret mais la science de la confiance. Et un élément essentiel à la défense de nos libertés. »

LE TRIPTYQUE DU CRYPTOLOGUE

Intégrité, authenticité et confidentialité sont les trois piliers de la cryptologie. Intégrité car le contenu d'un message ne doit pas pouvoir être modifié de manière indésirable. Authenticité pour que chaque partie soit sûre de l'origine des messages reçus. Confidentialité, enfin, pour qu'un tiers indelicat ne puisse s'immiscer dans la communication.

UNE RICHE DESCENDANCE

On l'a dit, Jacques Stern est l'incontestable père fondateur de la nouvelle cryptologie française. Ainsi, parmi ses descendants directs, à savoir ceux devenus informaticiens qui l'ont eu pour directeur de thèse de doctorat, d'habilitation ou les deux, on compte aujourd'hui dix universitaires, trois chercheurs au CNRS, quatre ingénieurs de l'armement et cinq chercheurs ou ingénieurs dans l'industrie. Par ordre alphabétique : Emmanuel Bresson, Florent Chabaud, Jean-Sébastien Coron, Jean-Bernard Fischer, Pierre-Alain Fouque, Louis Goubin, Louis Granboulan, Étienne Grandjean, Antoine Joux, Salah Laballah, Gwenaëlle Martinet, David Mraïhi, David Naccache, Phong Nguyen, Jacques Patarin, David Pointcheval, Thomas Pornin, Guillaume Poupard, Miklos Santha, Christophe Tymen, Brigitte Vallée et Serge Vaudenay. Une liste qui n'a pas fini de s'allonger, puisque d'autres thèses sont en cours sous la direction du médaillé. Difficile, par contre, de recenser tous ses « petits-enfants », au-delà du premier d'entre eux Marc Girault, autrement dit tous ceux qui ont fait carrière après avoir soutenu leur thèse avec l'une des personnes citées ici. Et l'arbre généalogique n'en est pourtant qu'à ses premières branches...



© CNRS Photothèque - Christophe Lebedinsky.



© CNRS Photothèque - Christophe Lebedinsky.

3 600 ANS DE MESSAGES CRYPTÉS



Quelque part en Mésopotamie, seize siècles av. J.-C. Pour conserver le secret d'un vernis qu'il avait créé, un potier babylonien en inscrit la recette sur une tablette d'argile en y enlevant des consonnes et en modifiant l'orthographe : le premier document crypté de l'humanité était né. Suivront trente-six siècles de cryptographie où les méthodes évoluent au rythme des avancées mathématiques et, faut-il le souligner, des impératifs militaires. Cette histoire, Jacques Stern la connaît mieux que personne. Au visiteur, il montre ainsi avec fierté une réédition du premier traité de cryptologie, écrit par le savant et philosophe al-Kindi au IX^e siècle. Passionné par le sujet, notre homme a même retracé les grandes étapes de cette histoire millénaire dans son ouvrage *La science du secret*. L'occasion de rappeler que la cryptographie n'est pas apparue avec les premiers ordinateurs, mais a suivi un long chemin que le médaillé a découpé en trois âges.

1 Érudits arabes dans une bibliothèque à Bassora. Au IX^e siècle, le philosophe al-Kindi fut aussi un savant des plus complets. Il a notamment rédigé le premier traité connu de cryptologie, retrouvé il y a vingt ans dans les archives ottomanes d'Istanbul.

L'ÂGE ARTISANAL

Dès les premiers pas de l'écriture, les hommes trouvent le besoin de dissimuler certains messages : « On discerne ainsi les prémices de la cryptographie dès l'apparition des hiéroglyphes égyptiens ou des textes cunéiformes », rappelle Jacques Stern. Certes, les cachottiers d'alors se contentent souvent d'utiliser des signes rares, limitant ainsi l'accès du texte aux initiés. Mais la volonté de transformer le texte et celle de le garder secret, bases de la cryptographie, sont déjà là. Une autre voie largement explorée consiste alors à cacher l'existence même du message : « Hérodote raconte ainsi comment un certain

Histiée, voulant prendre contact avec son gendre pour se révolter contre les Perses, rase la tête d'un esclave dévoué, y tatoue le message secret, et attendit la repousse des cheveux avant d'envoyer l'esclave avec l'instruction de lui raser le crâne », écrit ainsi Jacques Stern. Autre exemple

célèbre, la scytale lacédémonienne utilisée au V^e siècle av. J.-C. : une baguette en bois autour de laquelle est enroulé, en spires, un ruban de papyrus. Déroulé, celui-ci ne donne plus à voir qu'une galaxie de lettres désassemblées. Seuls les destinataires du message connaissent le diamètre de la baguette sur laquelle enrouler le message.

LA CRYPTOGRAPHIE N'EST PAS APPARUE AVEC LES PREMIERS ORDINATEURS, MAIS A SUIVI UN LONG CHEMIN QUE LE MÉDAILLÉ A DÉCOUPÉ EN TROIS ÂGES.

Mais rendons à César ce qui lui appartient, à savoir le premier véritable système de cryptographie au sens propre. Dans ce procédé romain, outre le redécoupage des mots, chaque lettre est remplacée

par celle située trois rangs après dans l'alphabet. Par exemple, le mot « consul » devient « frqvxv ». Ce principe de substitution va occuper une place centrale dans l'histoire de la cryptologie, même si les méthodes vont bien évidemment se complexifier au fil des siècles.

Les mathématiciens des XVI^e et XVII^e siècles, tels Jérôme Cardan, François Viète, fondateur de l'algèbre moderne, ou encore le Britannique John Wallis jouent ainsi un rôle important dans cette évolution. Peu à peu émerge alors une véritable théorie de la cryptographie en lieu et place de ce qui se limitait jusque-là à un savoir-faire, aussi complexe soit-il. Une illustration ? En 1883, le linguiste Auguste Kerckhoffs expose dans sa *Cryptographie militaire* les six qualités indispensables¹ à un système de chiffrement militaire, qui servent encore aujourd'hui d'idéal en la matière.

Néanmoins, à l'orée du XX^e siècle, la cryptographie reste une discipline bien limitée. Deux mécanismes sont encore les plus utilisés : la substitution et la transposition qui change, quant à elle, l'ordre des lettres d'un texte. En parallèle, les techniques de chiffrement, qui consistent à remplacer mots et phrases par des groupes de quatre ou cinq chiffres fournis par une table spécifique, sont aussi relativement fiables. Mais toutes ces techniques de chiffrement manuel deviennent de plus en plus risquées car elles doivent lutter contre la montée en puissance de l'art de déchiffrer, la cryptanalyse. Grâce notamment à l'apparition de techniques d'analyse statistique des

textes. Un exemple ? En français, la proportion de E est de 18,2 %. À partir de nombreuses observations de ce type, des règles efficaces avaient été érigées par les déchiffreurs : « *Ainsi, deux caractères successifs que l'on soupçonne d'être des voyelles et qui suivent un caractère rarement employé forment sans doute la particule que* », illustre Jacques Stern. Aussi, les cryptanalystes commencent à prendre sérieusement l'avantage sur les cryptographes. L'exemple le plus connu date de la première guerre mondiale, avec le « télégramme Zimmermann », un message allemand dont le décryptement par les services britanniques précipite l'entrée en guerre des États-Unis en 1917. Au sortir de la guerre, un heureux événement a lieu pour les fabricants de secret : la réapparition des machines à chiffrer... dont les prototypes dataient tout de même du XV^e siècle ! Leur entrée en lice sonne le glas de l'âge artisanal et la naissance de l'âge technique.



L'ÂGE TECHNIQUE

En 1919, deux brevets de machines chiffantes marquent le début d'une nouvelle ère. L'une d'elles, développée en Allemagne, est restée célèbre : la machine Enigma, basée sur des méthodes complexes de substitution, qui propose plusieurs centaines de millions de combinaisons et autant de manières de coder un message. « *Plus tard, allaient apparaître des machines encore plus complexes, affranchies des contraintes alphabétiques : c'est l'alphabet Baudot des téletypewriters, composé de 32 symboles, qui servait de base* », raconte Jacques Stern. Autant dire que la partie s'annonçait difficile pour le camp des Champollion... C'est dans ce contexte que survient la seconde guerre mondiale. Dès 1939, le gouvernement britannique réunit les plus grands spécialistes, dont le mathématicien Alan Turing, pour intercepter et décrypter les messages ennemis. Un effort, allié à la confiance aveugle des Allemands en leur machine Enigma, qui s'avère payant : grâce à de grandes avancées conceptuelles et technologiques, sous l'impulsion de Turing, les Alliés déchiffrent nombre de messages ennemis, un avantage qui a sûrement une grande part dans l'issue de la guerre. En outre, cet effort de guerre permet une cristallisation de la pensée logique en une forme mécanique : l'informatique est alors près de naître. Au sortir de la guerre, les banques, compagnies



© COSMOS
2

2 Ici la célèbre machine Enigma utilisée par l'armée allemande lors de la seconde guerre mondiale.



© COSMOS
3

3 Un système de rotors permet de procéder à une suite d'opérations trop nombreuses et complexes pour être réalisées manuellement.

d'assurance, administrations et autres institutions éprouvent un besoin croissant de protéger leurs données et s'arrachent les cryptographes. Résultat ? En 1977 apparaît la première norme de cryptage purement civile : le DES (*Data Encryption Standard*), descendant sophistiqué des méthodes traditionnelles de chiffrement mais adapté à l'informatique, et offrant 2^{56} clefs possibles ! Mais l'évènement majeur de cette période a eu lieu un an avant, et marque les débuts d'une nouvelle ère, dans laquelle nous sommes toujours aujourd'hui.

L'ÈRE MODERNE

1976, « une rupture décisive en cryptographie » selon Jacques Stern. Deux chercheurs, Whitfield Diffie et Martin Hellman, inventent la cryptographie à clef publique (voir *La crypto à clef publique*, p.9). Le premier système robuste basé sur ce concept fut créé en 1978. Le RSA², c'est son nom, permit ainsi à la cryptologie de se propager dans d'innombrables applications civiles, du téléphone portable au commerce sur Internet. Depuis, et malgré les efforts d'une communauté scientifique active, personne n'a jamais réussi à casser ce code qui utilise l'arithmétique des grands nombres entiers. Pour en venir à bout, il faut en effet passer par la factorisation d'un très grand nombre. Et même si la puissance de calcul des ordinateurs ne cesse de croître, la norme RSA a encore du temps devant elle. N'allez pas croire pour autant que la cryptologie a stagné depuis la naissance du RSA : elle a même connu d'autres bonds de géant conceptuels, tels que l'invention de la notion de non divulgation ou le développement des méthodes de sécurité prouvée (voir *La crypto à clef publique*, p.9). De plus, la discipline s'est aussi consacrée aux applications dont l'essor exponentiel semble aujourd'hui sans limite, avec l'explosion des nouvelles technologies de l'information et de la communication. À travers le parcours remarquable de Jacques Stern, ce sont aujourd'hui une discipline millénaire et une communauté précieuses pour la société qui se voient aussi honorées par la Médaille d'or 2006 du CNRS.



© CNRS Photothèque - Christophe Lebedinsky.

¹ Les qualités indispensables d'un système de chiffrement sont les suivantes.

- Il doit être matériellement, sinon mathématiquement, indécryptable.
- Il doit pouvoir tomber sans inconvénient entre les mains de l'ennemi.
- La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée et modifiée au gré des correspondants.
- Il doit pouvoir être applicable à la correspondance télégraphique.
- Il doit pouvoir être portatif, et son maniement ne doit pas exiger le secours de plusieurs personnes.
- Il doit être d'usage facile.

² Acronyme regroupant les initiales de ses inventeurs : Ronald Rivest, Adi Shamir et Leonard Adleman.

UNE AFFAIRE DE FAMILLE

Un invariant dans la longue histoire de la cryptologie : l'existence récurrente de dynasties. Vers la fin du xvi^e siècle, les Argenti se succédèrent ainsi aux côtés du souverain pontifical, qui disposait à l'époque de la crème de la discipline. De même, les Rossignol furent les experts attirés à la cour de Louis XIII puis Louis XIV et « furent à l'origine de la grande tradition française ». Clin d'œil de l'histoire : aujourd'hui, les deux enfants du médaillé d'or 2006 dirigent Cryptolog, une start-up de cryptographie qu'ils ont montée en 2001 avec un des anciens thésards de Jacques Stern. À n'en pas douter, une éventuelle nouvelle dynastie aurait des bases pour le moins solides.



© CNRS Photothèque - Christophe Lebedinsky.


 A portrait of Jacques Stern, a man with dark hair, wearing a light-colored striped shirt, sitting at a desk. The background is dark with some blurred lights.

JACQUES STERN

Né le 21 août 1949 à Paris

FORMATION : UN CURSUS ACADÉMIQUE

- 1975 : docteur ès sciences
- 1971 : agrégé de mathématiques
- 1968-1972 : élève à l'ENS
- 1968 : reçu à l'École polytechnique et à l'École normale supérieure (ENS)
- Études secondaires au lycée Michelet et au lycée Louis-le-Grand à Paris

CARRIÈRE : DES MATHÉMATIQUES À LA CRYPTOLOGIE, EN PASSANT PAR L'INFORMATIQUE

- 1999 - : directeur du département d'informatique de l'ENS
- 1996 - : directeur du laboratoire d'informatique de l'ENS (Liens, CNRS ST2I/ENS)
- 1993 - : professeur à l'ENS
- 1992-1993 : directeur de recherche au CNRS
- 1986-1998 : maître de conférence à l'École polytechnique
- 1986-1992 : professeur à l'université Paris-VII
- 1979-1986 : professeur à l'université de Caen
- 1972-1978 : assistant puis maître-assistant à l'université Paris-VII

PUBLICATIONS ET OUVRAGES

- Un livre : *La science du secret*, éditions Odile Jacob, 1998.
- 30 directions de thèses
- 150 publications scientifiques entre 1975 et 2006

PRIX ET DISTINCTIONS

- Médaille d'or 2006 du CNRS
- Médaille d'argent 2005 du CNRS
- *Fellow of the IACR (International Association of Cryptologic Research)* en 2005
- Lauréat du prix Lazare Carnot de l'Académie des sciences en 2003
- Chevalier de la Légion d'honneur

LES LAURÉATS DEPUIS 1954

- 2005 • Alain Aspect, physique
- 2004 • Alain Connes, mathématiques
- 2003 • Albert Fert, physique
- 2002 • Jean Jouzel, glaciologie
 - Claude Lorius, glaciologie
- 2001 • Maurice Godelier, anthropologie
- 2000 • Michel Lazdunski, biochimie
- 1999 • Jean-Claude Risset, informatique musicale
- 1998 • Pierre Potier, chimie
- 1997 • Jean Rouxel, chimie
- 1996 • Claude Cohen-Tannoudji, physique
- 1995 • Claude Hagège, linguistique
- 1994 • Claude Allègre, physique du globe
- 1993 • Pierre Bourdieu, sociologie
- 1992 • Jean-Pierre Changeux, neurobiologie
- 1991 • Jacques Le Goff, histoire
- 1990 • Marc Julia, chimie
- 1989 • Michel Juvet, biologie
- 1988 • Philippe Nozières, physique
- 1987 • Georges Canguilhem, philosophie
 - Jean-Pierre Serre, mathématiques
- 1986 • Nicole Le Douarin, embryologie
- 1985 • Piotr Slonimski, génétique
- 1984 • Jean Brossel, physique
 - Jean-Pierre Vernant, histoire
- 1983 • Évry Schatzman, astrophysique
- 1982 • Pierre Joliot, biochimie
- 1981 • Jean-Marie Lehn, chimie
 - Roland Martin, archéologie
- 1980 • Pierre-Gilles de Gennes, physique
- 1979 • Pierre Chambon, biologie
- 1978 • Maurice Allais, économie
 - Pierre Jacquinot, physique
- 1977 • Charles Fehrenbach, astronomie
- 1976 • Henri Cartan, mathématiques
- 1975 • Raymond Castaing, physique
 - Christiane Desroches-Noblecourt, égyptologie
- 1974 • Edgar Lederer, biochimie
- 1973 • André Leroi-Gourhan, ethnologie
- 1972 • Jacques Oudin, immunologie
- 1971 • Bernard Halpern, immunologie
- 1970 • Jacques Friedel, physique
- 1969 • Georges Chaudron, chimie
- 1968 • Boris Ephrussi, génétique
- 1967 • Claude Lévi-Strauss, ethnologie
- 1966 • Paul Pascal, chimie
- 1965 • Louis Néel, physique
- 1964 • Alfred Kastler, physique
- 1963 • Robert Courrier, biologie
- 1962 • Marcel Delépine, chimie
- 1961 • Pol Bouin, physiologie
- 1960 • Raoul Blanchard, géographie
- 1959 • André Danjon, astrophysique
- 1958 • Gaston Ramon, immunologie
- 1957 • Gaston Dupouy, physique
- 1956 • Jacques Hadamard, mathématiques
- 1955 • Louis de Broglie, physique
- 1954 • Émile Borel, mathématiques

Cette plaquette de la collection Talents est éditée
par la Direction de la communication (Dircom) du CNRS.

Responsable du pôle Éditions - Relations avec la presse - Multimédia : Françoise Harrois-Monin

Rédaction : Matthieu Ravaud

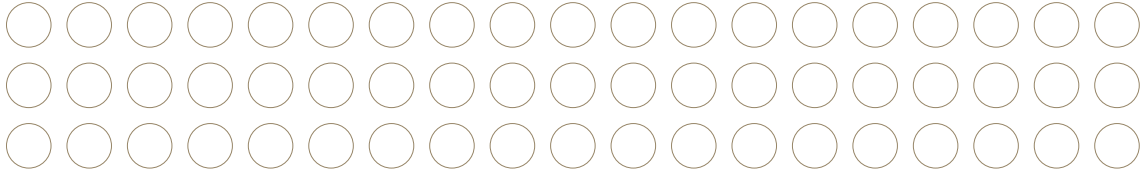
Conception graphique : Sarah Landel

Adaptation graphique et mise en page : Clément Prats

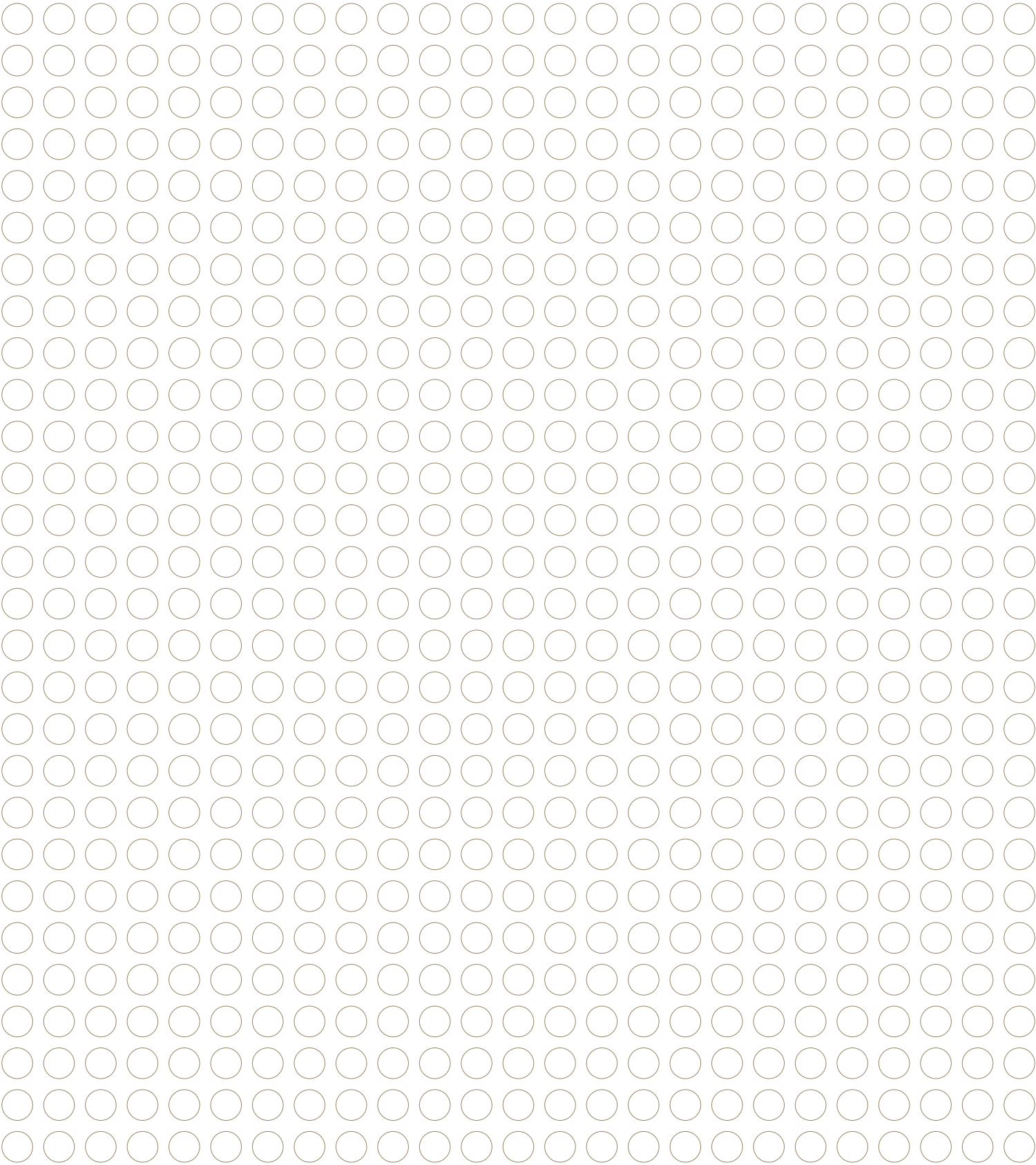
Coordination iconographique : Christelle Pineau (CNRS images-Photothèque)

Impression : Jouve
Décembre 2006

ISSN 1777-0378



www.cnrs.fr



CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE
3, RUE MICHEL-ANGE 75794 PARIS CEDEX 16 • TÉL. 01 44 96 40 00 • TÉLÉCOPIE 01 44 96 53 90

