Conférence de presse

Médaille d'or 2006 du CNRS

Vendredi 6 octobre 2006

CNRS – Paris

DOSSIER DE PRESSE

Contact médaillé
Jacques Stern
T 01 44 32 20 34
Jacques.Stern@ens.fr

Contact presse
Martine Hasler
T 01 44 96 46 35
Martine.hasler@cnrs-dir.fr

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Conférence de presse
Médaille d'or 2006 du CNRS

Sommaire

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

La médaille d'or 2006 du CNRS décernée à Jacques Stern, professeur d'informatique, spécialiste français des codes secrets

COMMUNIQUÉ DE PRESSE – PARIS – 6 OCTOBRE 2006 www.cnrs.fr/presse

La Médaille d'or du CNRS, plus haute distinction pour des travaux de recherche scientifique en France, est décernée cette année à Jacques Stern, 57 ans, professeur à l'Ecole normale supérieure (ENS), directeur du laboratoire d'informatique de l'ENS (unité mixte ENS/CNRS) et chercheur mondialement connu pour ses travaux sur la cryptologie. A l'origine de 150 publications, véritable père fondateur d'une école de cryptologie classant la France aux avant-postes de l'Europe dans la discipline, Jacques Stern a débuté sa carrière comme mathématicien avant de s'intéresser à l'informatique puis à la cryptologie. Un résumé de ce qui est aussi l'évolution récente de cette discipline…

Internet, comptes bancaires, enchères en ligne, vote électronique, communications téléphoniques… Alors que la cryptologie est restée très longtemps un domaine réservé aux militaires et aux diplomates, ses applications aujourd'hui très vastes touchent largement le grand public.

Spécialiste français mondialement reconnu, Jacques Stern a ouvert la voie de la cryptologie en France et y a consacré 20 années de travaux de recherche. D'abord mathématicien (logique et théorie des ensembles), il s'est ensuite tourné vers la complexité algorithmique avant de se lancer dans ce domaine de recherche.

Ancien élève de l'Ecole normale supérieure et docteur ès-sciences, Jacques Stern est aujourd'hui professeur à l'ENS rue d'Ulm à Paris où il dirige le laboratoire d'informatique de l'ENS (LIENS - unité mixte ENS/CNRS) et le département d'informatique. Il est l'auteur de 150 publications scientifiques, d'un ouvrage intitulé « *La science du secret* » (Editions Odile Jacob) ainsi que d'un rapport au gouvernement qui a été suivi d'une nouvelle réglementation de la crytographie. Médaillé d'argent du CNRS en 2005, chevalier de la Légion d'honneur, Jacques Stern s'est vu décerner en 2003 le prix Lazare Carnot de l'Académie des sciences pour l'ensemble de ses travaux dans le domaine.

Cette reconnaissance de 20 ans de recherche par la Médaille d'or du CNRS est l'occasion d'honorer une science singulière, qui a longtemps - par nature - cultivé le sens du secret mais qui, avec la numérisation et la mondialisation des échanges, concerne aujourd'hui le plus grand nombre.

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Une nouvelle discipline scientifique

Etymologiquement, cryptologie signifie « science du secret ». Les premiers « travaux » remontent à plusieurs siècles avant Jésus-Christ et au fil du temps, la cryptologie est devenue une discipline scientifique à part entière dont le but est d'assurer l'intégrité d'une information, son authenticité et sa confidentialité dans les données et les échanges. Pour ce faire, elle établit des « règles du jeu » et des procédés pour résister aux « adversaires » qui ne les respecteraient pas. Exemples : le codage des messages diplomatiques doit lutter contre les services de renseignements d'autres pays ; une banque doit s'assurer de l'identité du porteur d'une carte de crédit, etc.

Les grands principes sont simples. Pour échanger une information que deux protagonistes (organisations ou individus) veulent conserver confidentielle, et pour s'assurer de leur identité respective, chacun doit posséder à la fois une clé pour s'identifier et une formule afin de coder puis de décoder le message. A partir de là, tout se complique. Les concepts font appel aux mathématiques les plus sophistiquées. Les chercheurs contemporains puisent leur inspiration dans les travaux de mathématiciens tel Alan Turing qui, dans les années 1930, a exploré à la suite de Kurt Gödel, les limites de la pensée mathématique.

Techniquement, la cryptologie a rejoint l'informatique depuis la fin de la deuxième guerre mondiale, et les scientifiques utilisent massivement l'ordinateur comme outil pour générer ou « casser » les algorithmes de codage les plus puissants. Sur le plan économique, enfin, c'est un secteur en pleine expansion du fait de l'explosion des communications électroniques.

Si les termes les plus simples, comme « code secret » ou « code PIN » pour la carte bancaire et la « carte SIM » pour les téléphones mobiles, sont dans la bouche de tous, qui connaît « clé secrète », « clé publique », « RSA », etc…? Derrière ces mots se cache une discipline en pleine effervescence, devenue indispensable, souvent stratégique et d'une grande richesse scientifique.

Quatre grands chantiers de la cryptologie moderne

A travers la Médaille d'Or 2006 du CNRS, c'est d'abord l'œuvre d'un chercheur qui est saluée, mais aussi les travaux de son équipe qui sont en pointe en Europe, se distinguent au plan mondial et ont permis en une vingtaine d'années des avancées majeures dans plusieurs domaines, en particulier dans quatre grands chantiers actuels de la cryptologie.

La conception d'algorithmes donne naissance à de nouveaux schémas cryptographiques, dont on a sans cesse besoin pour répondre à de nouveaux besoins (authentification, signature au moyen d'une carte à puce). Jacques Stern et son équipe ont, par exemple, pu faire la preuve d'un algorithme d'authentification, dit « GPS », élaboré avec France Télécom et devenu une norme ISO en 2005.

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

La cryptanalyse permet de « casser » des codes secrets prétendus inviolables. L'équipe de l'ENS/CNRS a notamment prouvé la fragilité d'algorithmes pourtant réputés solides voire inviolables ; en 1998, elle a pu « casser » un algorithme d'IBM qui se voulait une solution alternative à RSA fondée sur des outils mathématiques de la géométrie des nombres.

La sécurité prouvée. Ce n'est pas parce qu'un algorithme a résisté aux attaques des cryptanalystes qu'il est sûr ! Il faut en apporter la preuve, et c'est par exemple ce qu'a fait l'équipe de cryptologie de l'ENS en participant au « sauvetage » d'une norme. En 1994, une équipe américaine a publié un algorithme qui est devenu une norme d'échanges sur l'Internet. En 2000, un vent de panique a soufflé chez les utilisateurs, devant une rumeur selon laquelle sa preuve était fausse. L'équipe ENS/CNRS, en collaboration avec des chercheurs japonais, a pu trouver une preuve correcte.

Les applications et les protocoles. Vote électronique, enchères en ligne sur Internet, téléphonie 3 G, les équipes françaises autour de Jacques Stern ont apposé leur signature sur de nouveaux schémas cryptographiques qui concernent une multitude d'acteurs. On parle d'ubiquité de la cryptologie.

Pour en savoir plus :

http://www.di.ens.fr/CryptoTeam.html.fr
http://www.di-ens.fr/~stern/

Glossaire

La cryptologie en 10 mots clés

Authentification
Action de s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication ou d'un fichier.

Clé
Information nécessaire à l'émetteur et au destinataire pour envoyer ou recevoir un message ou des données confidentielles, ou pour s'authentifier.

Cryptanalyse
Consiste à tenter d'attaquer un système cryptographique, notamment pour en étudier le niveau de sécurité effectif.

Cryptographie
Conception de mécanismes cryptologiques destinés à garantir les notions de sécurité à des fins de confidentialité, d'authenticité et d'intégrité de l'information, mais aussi pour d'autres notions comme l'anonymat.

Cryptographie asymétrique (clé publique)
Les algorithmes sont publics, mais chaque individu possède un couple de clés : l'une secrète lui permettant d'effectuer les opérations que lui seul est sensé être en mesure de faire (signature ou déchiffrement), tandis que sa clé publique est diffusée afin de permettre à ses interlocuteurs de mettre en œuvre les opérations réciproques (vérification de signature ou chiffrement de message). Les deux clés ont un rôle « asymétrique », d'où la terminologie.

Cryptographie symétrique (clé secrète)
Les algorithmes sont publics, mais une information secrète commune à l'émetteur et au destinataire permet leur usage entre plusieurs personnes. On dit « symétrique » car émetteur et destinataire ont le même niveau d'information.

Cryptologie

Du grec *kryptos* (caché) et *logos* (science), « cryptologie » signifie littéralement science du secret et a pour objet de cacher les informations d'un message. Son but est triple : assurer la confidentialité, garantir l'authenticité et conserver l'intégrité des informations. Cette science, née il y a plusieurs millénaires mais organisée en discipline depuis quelques décennies seulement, comprend principalement deux champs d'étude, la cryptographie et la cryptanalyse.

Preuve de sécurité

Méthodologie qui complète la cryptanalyse par des preuves mathématiques d'absence de failles.

RSA

Du nom de ses inventeurs Ron Rivest, Adi Shamir et Leonard Adleman, premier algorithme qui utilise le principe de clé publique.

Signature numérique

Service d'authenticité, ayant une valeur juridique depuis la loi du 20 mars 2000, et qui permet de s'assurer de l'identité d'une entité donnée ou l'origine d'une communication ou d'un fichier.

Jacques Stern

© CNRS Photothèque – Christophe LEBEDINSKY

20 ans au service de la cryptologie

ou l'homme qui a rendu nos échanges plus sûrs.

« J'ai toujours été attiré par la science à temps court. J'aime que mes idées passent rapidement au stade des applications… ». On comprend vite, face à cet homme calme, à la voix douce, aux termes précis et surtout concrets, pourquoi le jeune enseignant et chercheur en mathématiques (sorti de l'Ecole normale supérieure à 22 ans et professeur à l'université de Caen à 30) a changé son fusil d'épaule à l'orée des années 80 pour devenir, en même temps que l'informatique prenait son essor, le chantre de la cryptologie française. Un besoin de peser sur le réel.

Mais une évolution, pas une rupture. Ses premiers travaux de recherche sur la logique, spécialité des mathématiques la plus proche de l'informatique, préparaient le terrain. *« Je m'intéressais aux résultats d'impossibilité en théorie des ensembles »,* explique Jacques Stern dans son bureau bien rangé de la rue d'Ulm, à Paris, près duquel, dans un couloir, on pouvait lire, il y peu, sur une affichette : *« la crypto c'est rigolo ».* Les mathématiciens Kurt Gödel, Alan Turing et Paul Cohen sont alors ses inspirateurs. Le même Turing qui, au début des années 1940, « casse » les codes de l'armée allemande… *« En allant voir ce qui se passe aux limites de la pensée mathématique, je suis arrivé à la cryptologie. J'ai toujours été attiré par certains paradoxes que l'on rencontre en logique, mais aussi en cryptologie : comment transmettre une correspondance secrète sans s'être jamais rencontrés ? »*

Dès lors le choix est fait : nous sommes en 1986, la cryptologie est devenue un domaine académique aux Etats-Unis depuis qu'a été inventé le concept de « clé publique » en 1976. La France balbutie en la matière, mais *« je voulais devenir un acteur de cette science ».*

Une école de cryptologie française

Sous l'impulsion de celui qui est aujourd'hui professeur à l'ENS, directeur de son département d'informatique et directeur du laboratoire d'informatique de l'ENS (LIENS, unité mixte ENS/CNRS), c'est une véritable école de cryptologie française qui va se créer en 20 ans. Les travaux poursuivis par le chercheur et son équipe du LIENS toucheront aux grands domaines de la discipline : conception d'algorithmes, cryptanalyse (attaque des systèmes proposés par d'autres), preuves de sécurité, normalisation de systèmes cryptographiques, et enfin protocoles et applications notamment dans le domaine de l'Internet avec en particulier le vote électronique.

La reconnaissance est vite internationale et aux plus hauts niveaux, pour le scientifique et ses travaux qui vont produire plus de 150 publications ainsi qu'une grande quantité de thèses. Auteur du livre « La science du secret » (chez Odile Jacob), Jacques Stern a obtenu la Médaille d'argent du CNRS en 2005. Il est également à l'origine d'un rapport au gouvernement sur la nouvelle réglementation de la crytographie.

Chevalier de la Légion d'honneur, Jacques Stern s'est vu décerner en 2003 le prix Lazare Carnot de l'Académie des sciences pour l'ensemble de son « œuvre ». Marié et père de deux enfants, l'homme n'est en rien exubérant. S'il n'est pas immodeste, on le sent fier d'avoir d'une certaine façon rendu nos échanges plus sûrs. Son grand calme dissimule mal la passion pour une discipline qui lui prend beaucoup. Mais lui laisse un peu de temps pour son autre inclination : l'opéra. *« Classique, j'insiste… ».*

Jacques Stern

Né le 21 août 1949 à Paris

Formation : un cursus académique

- études secondaires au lycée Michelet et au lycée Louis-le-Grand à Paris
- 1968 : reçu à l'Ecole Polytechnique et à l'Ecole Normale Supérieure (ENS)
- 1968-1972 : élève à l'ENS
- 1971 : agrégé de mathématiques
- 1975 : docteur ès sciences

Carrière : des mathématiques à la cryptologie, en passant par l'informatique

- 1972-1978 : assistant puis maître-assistant à l'université Paris 7
- 1979-1986 : professeur à l'université de Caen
- 1986-1992 : professeur à l'université Paris 7
- 1986-1998 : maître de conférences à l'Ecole polytechnique
- 1992-1993 : directeur de recherche au CNRS
- 1993 - : professeur à l'ENS
- 1996 - : directeur du laboratoire d'informatique de l'ENS (LIENS, ENS/CNRS)
- 1999 - : directeur du département d'informatique de l'ENS

Publications et ouvrages

- 150 publications scientifiques entre 1975 et 2006
- 30 directions de thèses
- un livre : *« La science du secret »*. Editions Odile Jacob.

Prix et distinctions

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

Les enjeux de la cryptologie

Elle a connu ses premiers balbutiements il y a plusieurs millénaires. Pourtant la cryptologie est une science très jeune qui a véritablement éclos avec l'avènement de l'informatique et la généralisation des télécommunications. Longtemps fermée, réservée aux militaires et à la diplomatie, elle touche tout le monde depuis l'explosion d'Internet. Quels sont ses enjeux techniques et sociétaux, ses moyens et ses perspectives ? Réponses à travers les travaux de l'équipe de l'ENS/CNRS.

Qu'y a-t-il de commun entre la carte SIM de votre téléphone, une carte bancaire, vos sites Internet préférés d'emplettes ? Un mot les relie : cryptologie.

En effet, dans la société de l'information, l'usage de la cryptologie s'est banalisé. Téléphones mobiles, cartes bleues, titres de transports, cartes vitales, décodeurs, Internet, on ne compte plus les objets de la vie courante qui incorporent des mécanismes de sécurité. Des algorithmes cryptographiques assurent par exemple que personne ne peut téléphoner à vos frais, intercepter un numéro de carte de paiement sur la Toile, accéder aux données confidentielles d'une carte vitale, etc.

Jadis restreinte aux usages diplomatiques et militaires, la cryptologie est maintenant devenue une discipline scientifique à part entière dont les applications sont si vastes aujourd'hui qu'il est difficile de définir *a priori* ce qui en relève. Initialement, elle avait pour objet l'étude des méthodes permettant d'assurer les services d'intégrité, d'authenticité et de confidentialité dans les systèmes d'information et de communication. Reposant sur l'utilisation de clés, elle recouvre désormais l'ensemble des procédés informatiques qui doivent résister à des adversaires ne respectant pas les « règles du jeu ».

Qu'est-ce que la cryptologie ?

La cryptologie a pour essence l'art de cacher une information au sein d'un message chiffré. C'est un art très ancien : les premiers codes secrets remontent à l'antiquité.

Elle se divise en deux branches :

- la **cryptographie** concerne la conception de mécanismes destinés à garantir les notions de sécurité.
- la **cryptanalyse** consiste à tenter d'attaquer un système cryptographique, notamment pour en étudier le niveau de sécurité effectif.

Elle doit répondre à trois enjeux :

- Un service d'intégrité pour garantir que le contenu d'une communication ou d'un fichier n'a pas été modifié de façon malveillante.
- Un service d'authenticité pour s'assurer de l'identité d'une entité donnée ou l'origine d'une communication ou d'un fichier. Lorsqu'il s'agit d'un fichier et que l'entité qui l'a créé est la seule à avoir pu apporter la garantie d'authenticité, il s'agit de la non-répudiation. Ce service est réalisé par une **signature numérique**, qui a une valeur juridique depuis la loi du 20 mars 2000.
- Un service de confidentialité pour garantir que le contenu d'une communication ou d'un fichier n'est pas accessible aux tiers. Des services de confidentialité sont offerts dans de nombreux contextes, notamment en téléphonie mobile, en télévision à péage et dans les navigateurs Internet par l'intermédiaire du protocole SSL/TLS.

Les principaux concepts

Jusqu'à la fin du XIX^{e} siècle, la plupart des techniques cryptographiques faisaient reposer leur sécurité sur le secret même de l' « algorithme » et n'étaient pas adaptées à un usage au sein d'un grand groupe de personnes. C'est pourquoi on a ensuite personnalisé le mécanisme avec une information de petite taille, appelée **clé secrète,** commune à l'émetteur et au destinataire. Puis ces méthodes de **cryptographie symétrique** à clé secrète se sont améliorées et complexifiées avec l'arrivée de l'électronique et de l'informatique.

La cryptologie a connu une mutation importante, au moment même où Internet se préparait, avec l'apparition de la cryptographie dite à **clé publique**, qui a ouvert un domaine de recherche très riche avec tous les problèmes pratiques de sécurité : authentification, confidentialité, commerce, vote, enchères et toutes autres formes d'échange de données nécessitant intégrité, non-répudiation ou anonymat. En effet en 1976, deux scientifiques, Whitfield Diffie et Martin Hellman ont imaginé de rendre tout le processus de chiffrement entièrement public, non seulement les algorithmes, mais encore une clé spécifique au destinataire, la clé publique. Seule la clé de déchiffrement doit rester secrète. Ainsi, chaque individu possède un couple de clés, l'une publique qui sert à ses interlocuteurs pour chiffrer des messages, l'autre secrète qui lui sert à déchiffrer les messages reçus, chiffrés à l'aide de sa clé publique. Cette **cryptographie asymétrique** permet également de concevoir des schémas de signature. Le déchiffrement, accessible uniquement à qui connaît la clé secrète, devient l'algorithme de signature. En revanche, l'opération réciproque de chiffrement étant accessible à tous devient l'algorithme de vérification qui doit conduire au message initial. La non-répudiation peut alors être garantie.

Ce principe a été mis en œuvre dès 1978 dans l'algorithme **RSA** inventé par Ron Rivest, Adi Shamir et Leonard Adleman. Dans le RSA, la sécurité est liée à la difficulté de calculer les facteurs premiers d'un nombre entier de plusieurs centaines de chiffres au moins : le record – qui date de mai 2005 –

est de 200 chiffres. De plus, en matière d'authenticité, une signature RSA est vérifiable avec la seule clé publique tandis que sa création nécessite la clé secrète de son titulaire, ce qui garantit la non-répudiation.

Cette cryptographie à clé publique apporte des solutions pour la non-répudiation d'une transaction électronique et sa confidentialité, ou l'anonymat d'un vote. Mais attention : l'efficacité du système repose sur la « confiance », qui elle-même doit s'appuyer sur la gestion des clés publiques par une autorité de certification habilitée à délivrer et à signer des clés (banque, administration des impôts, entreprise, ministère, etc...). De plus, la sécurité des mécanismes n'est pas inconditionnelle, mais dépend des hypothèses mathématiques qu'il faut identifier clairement afin d'évaluer leur validité. Il s'agit des deux problèmes majeurs posés à la fois aux pouvoirs publics et à la communauté scientifique pour que la cryptographie puisse assurer la protection des libertés individuelles, dans un monde envahi par le numérique, sans risquer d'être détournée à des fins malhonnêtes.

Dans les trente dernières années, la recherche en cryptologie a connu un considérable développement, se concentrant sur la conception et l'évaluation d'algorithmes symétriques et à clé publique. Cette recherche s'est accompagnée d'un effort de normalisation exceptionnellement enraciné dans les recherches les plus récentes et fondé sur un rapprochement entre la recherche académique et le monde industriel.

La recherche française en pointe

Sans revenir sur tous les travaux qui ont été réalisés, évoquons ici deux axes de recherche prometteurs apparus dans les dernières années et étudiés au laboratoire LIENS, dirigé par Jacques Stern.

La sécurité prouvée

Le plus grand progrès qu'ait connu la cryptographie asymétrique depuis son invention est la méthodologie de la sécurité prouvée, ou **preuve de sécurité**, qui complète la cryptanalyse par de véritables preuves d'absence de failles. Il s'agit dans un premier temps de modéliser la notion même de sécurité, puis de construire des cryptosystèmes prouvés sûrs dans ce modèle, sous des hypothèses mathématiques précises et plausibles.

La sécurité prouvée met en œuvre une approche réductionniste : on traduit la sécurité en une hypothèse sur la difficulté de résoudre par le calcul un problème bien connu et bien défini, comme la factorisation ou le logarithme discret. Si l'hypothèse est satisfaite, le système est sûr. Le principal avantage de cette approche est que l'on peut clairement identifier l'hypothèse sur laquelle repose la sécurité, le principal inconvénient étant que l'on n'obtient pas de preuve absolue : on a juste remplacé un énoncé complexe par une hypothèse plus claire. Reste à suivre les progrès dans la résolution des problèmes supposés difficiles et à dimensionner la taille des clés en conséquence.

Malheureusement, dans la plupart des cryptosystèmes asymétriques pratiques, notamment ceux qui sont normalisés, la traduction de l'énoncé complexe en une hypothèse plus claire n'est pas nécessairement pertinente pour les tailles de clés courantes. Pour contourner ce problème, les chercheurs ont opéré une idéalisation des fonctions d'intégrité dites aussi de « hachage », connue sous le nom de modèle de « l'oracle aléatoire ». La méthode revient à faire l'hypothèse supplémentaire que l'attaquant n'exploitera pas les spécificités intrinsèques des fonctions de hachage utilisées. Dans ce modèle idéal, de nombreux systèmes cryptographiques efficaces ont pu être prouvés sûrs, sous des hypothèses calculatoires plausibles.

La cryptographie fondée sur l'identité

Un autre grand problème de la cryptographie asymétrique est la gestion des clefs publiques, et plus précisément la façon de garantir l'authenticité de ces dernières. Dans le cas d'Internet, ce problème est actuellement résolu à l'aide de certificats, bien connus des habitués des sites marchands. La cryptographie asymétrique fondée sur l'identité propose une solution alternative en permettant aux clefs publiques d'être directement reliées à l'identité des utilisateurs : toute chaîne de caractères, par exemple une adresse électronique, est une clef publique potentielle.

Cela est rendu possible par l'intermédiaire d'une autorité de certification en laquelle tous les utilisateurs ont confiance : l'autorité choisit des paramètres publics, et à chaque fois qu'un utilisateur souhaite enregistrer une clef publique (de valeur arbitraire), l'utilisateur l'envoie à l'autorité, qui lui retourne la clef secrète correspondante. Contrairement à ce qui se passe dans les infrastructures de clés publiques traditionnelles, l'autorité a connaissance de toutes les clés secrètes.

La cryptographie à base d'identité est en plein essor, mais elle n'est donc pas sans inconvénient. De plus, elle a dû faire appel à des théories mathématiques complexes dont l'aspect algorithmique n'a pas encore fait l'objet de recherches approfondies.

Pour en savoir plus :

- Jacques Stern, *La science du secret,* Editions Odile Jacob, 1997.
- David Kahn, *La guerre des codes secrets,* Paris, InterEditions, 1980.
- *Paradigmes et enjeux de l'informatique*, sous la direction de Nicole Bidoit, Luis Farinãs del Cerro, Serge Fdida, Brigitte Vallée, Editions Lavoisier, 2005. Chapitre 6 : La cryptologie : enjeux et perspectives. Phong Q.Nguyen, Jacques Stern.
- David Pointcheval, *La cryptographie à l'aube du troisième millénaire.* Revue de l'électricité et de l'électronique. Volume 5, pages 28-34. Dossier spécial *La sécurité des systèmes d'information*, SEE, mai 2001.

Les dates clés
2500 ans de secrets bien (ou mal) gardés

La cryptologie remonte aussi loin que des sociétés organisées ont eu besoin de conserver secrètes un certain nombre d'informations. L'histoire est riche d'inventions toutes aussi originales les unes que les autres. Jusqu'à l'arrivée de l'informatique qui a tout changé.

V^e siècle av JC
Scytale lacédémonienne : ruban de papyrus qui nécessitait d'être enroulé autour d'une baguette de bois de diamètre connu pour être lue.

Rome (I^er siècle av JC)
Code de César : système cryptographique pour coder les messages militaires par décalage alphabétique de chaque lettre.

IX^e siècle
al Kindi, savant et philosophe arabe. Il rédige le premier manuscrit connu sur la cryptologie.

XV^e siècle
Cadran d'Alberti : système à base de disques concentriques.

XVI^e siècle
Grille de Cardan : système à base de quadrillages.

1863
Friedrich Kasiski, officier prussien, étudie dans son ouvrage *Les Chiffres et l'art du décryptement* la statistique des fréquences des caractères d'un texte dans une langue particulière. Il définit et introduit un invariant, appelé « indice de coïncidence », qui facilite les attaques.

1883
Auguste Kerckhoffs, linguiste et cryptologue flamand**,** énonce, dans son essai *La cryptographie militaire*, un certain nombre de principes fondamentaux pour le chiffrement, avec notamment le fait que le mécanisme de chiffrement doit *« pouvoir tomber sans inconvénient entre les mains de l'ennemi ».*

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

1919
Deux brevets sont déposés pour les premières machines « chiffrantes » : **Enigma** qui équipera l'armée allemande, puis **Hagelin** adoptée par les alliés.

1930
Kurt Gödel et Alan Turing, travaux sur les limites de la pensée mathématique, menant à « l'impossibilité concrète », c'est-à-dire à l'existence d'énoncés qui ne peuvent être ni prouvés, ni réfutés.

1938
Entrée d'Alan Turing, mathématicien britannique, au GE&CS (Government Code and Cypher School).

1940
Turing « casse » les codes de l'armée allemande.

1945
Premiers ordinateurs.

1976
Naissance de la cryptologie asymétrique. Whitfield Diffie et Martin Hellman, dans un article intitulé *New Directions in Cryptography*, rendent le processus de chiffrement entièrement public, y compris la clé spécifique au destinataire alors appelée clé publique. Seule la clé de déchiffrement doit rester secrète. Le concept de cryptographie à clé publique était inventé.

1978
RSA : Premier mécanisme de chiffrement asymétrique par Ronald Rivest, Adi Shamir et Leonard Adleman.

1981
Première conférence académique de cryptologie « Crypto » qui se tient depuis, chaque année, à Santa Barbara en Californie.

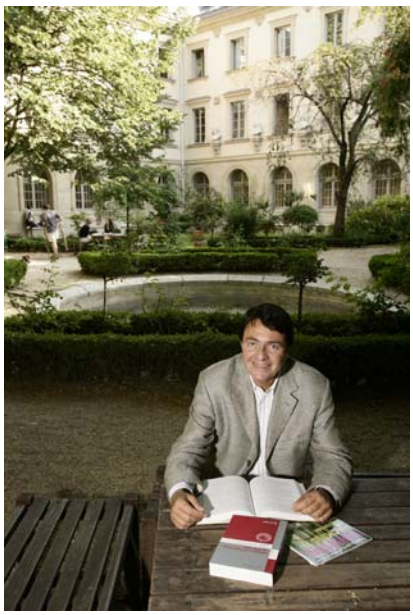
Médaille d'or 2006 du CNRS
Jacques Stern


Ref 01


Ref 02


Ref 03

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE



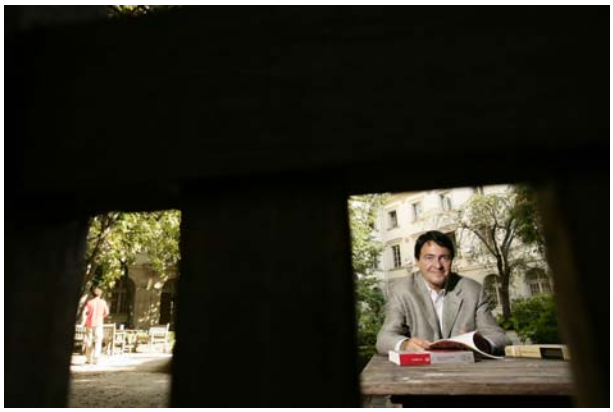
Ref 04

Ref 05

Ref 06

Ref 07

Ref 08



Ref 09

Ref 10

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE