Discours prononcé le 13 décembre 2006 lors de la remise de la médaille d’or du CNRS

Monsieur le ministre,
Madame la présidente du CNRS,
Monsieur le directeur général du CNRS,
Monsieur le maire,
Monsieur le recteur,
Chers collègues, chers amis,

1954.

En 1954, la médaille d'or du CNRS était décernée pour la première fois au mathématicien français Emile Borel. La même année, le mathématicien britannique Alan Turing mettait fin à ses jours, victime de ce qu'on appellerait aujourd'hui un lynchage juridico-médiatique. Si j'évoque les noms de Borel et de Turing, ce n'est évidemment pas pour opposer la science française à la science britannique : le savoir ne connaît pas de frontière. Ce n'est pas non plus pour inviter le médaillé d'or que je vais devenir aujourd'hui à la modestie, en l'amenant à observer que le destin des savants est divers: les honneurs pour Borel, l'opprobre pour Turing. Ce n'est ni le moment, ni le lieu. Non, si j'en appelle à Borel et à Turing, c'est tout simplement que, par le hasard de la science, certains de mes premiers travaux, appelons les mes travaux de jeunesse, s'inscrivaient dans le prolongement des leurs. En témoigne le titre d'un de mes

articles de l'époque: "Partitions effectives de la droite réelle en ensembles boréliens de rang borné". Le mot effectif renvoie à Turing et le mot borélien à Borel bien sûr.

Ces premiers travaux, ce ne sont pas ceux qui me valent la médaille d'or du CNRS. Je voudrais cependant en dire un mot en essayant de répondre à trois questions:

- en qui consistaient-ils?
- pourquoi les avais-je entrepris?
- en étais-je satisfait?

En qui consistaient-ils ? J’étais logicien et je démontrais, en particulier, ce qu'on nomme des résultats d'indécidabilité. En d'autres termes, j'essayais de montrer que tel ou tel problème est au delà des limites de ce que peuvent atteindre les mathématiques, qu'il est donc impossible de le résoudre.

Pourquoi les avais-je entrepris ? Parce que je pensais - et je pense toujours - que les résultats les plus profonds des mathématiques du vingtième siècle sont précisément les résultats d'impossibilité obtenus par Kurt Gödel en 1930 et par Alan Turing en 1936. Le théorème de Gödel, c'est le paradoxe du menteur: quel sens donner à l’assertion "je mens" ? En effet, en disant "je mens" ou bien je mens réellement, et alors je dis la vérité, ou bien je dis en fait la vérité mais c'est donc que je mens. Le tour de force de Gödel est d'avoir, pour reproduire le paradoxe du menteur,

su rendre les mathématiques capables de parler d'elles mêmes, ce qu'on nomme parfois l'arithmétisation de la syntaxe. Le pas suivant, celui de Turing est la mécanisation de l'activité mathématique par la notion de machine de Turing, ordinateur avant l'heure.

En étais-je satisfait? Oui et non. Oui, car il est fascinant de participer à la continuation d'une grande aventure intellectuelle. Non, car rien de concret ne me semblait pouvoir découler d'un résultat d'impossibilité de plus.

Il me fallait donc changer.

Je voyais que c'était possible. Les travaux dont je viens de parler m'avaient valu une certaine reconnaissance et l'occasion de devenir un assez jeune professeur à l'Université de Caen : dans ces conditions, je pouvais faire le choix de prendre des risques.

Je voyais aussi que ce n'était pas facile. Les communautés scientifiques sont constituées de telle manière que celui qui prend le risque de changer a le sentiment diffus, à tort ou à raison, d'être considéré par les uns comme un transfuge et pas les autres comme un intrus. Rétrospectivement, mes craintes étaient excessives: je crois avoir gardé l'estime des mathématiciens et, après un temps, j'ai été chaleureusement accueilli par une communauté regroupant nombre de collègues de ma génération qui avaient fait, avant moi,

le choix de l'informatique. Je ne peux les citer tous, mais je voudrais évoquer ici le nom de Gilles Kahn, qui nous a quitté au début de l'année et dont le charisme et la clairvoyance nous manquent.

Qu'elles qu'aient été les difficultés, réelles ou supposées, j'avais, dans mes projets de changement une confiance sereine, qui venait du soutien que je recevais de ma femme et de mes enfants. Je les remercie, mais je ne voudrais pas donner l'image d'un chercheur tourmenté en proie au doute et réconforté par sa famille. Non, si je remercie ma femme c'est pour ce qu'elle est, dans les premiers rangs de sa spécialité, le droit international. Elle pourrait certainement être aujourd'hui à ma place et, en étant ce qu'elle est, elle m'a permis de donner le meilleur de moi-même. Je remercie également mes enfants pour ce qu'ils sont, mais j'aurai l'occasion d'en reparler.

La voie du changement m'a conduit à la cryptologie. J'ai réalisé en effet que les machines de Turing étaient à la base de la théorie de la complexité algorithmique, qui classifie les problèmes informatiques en fonction du temps de calcul nécessaire à leur solution. J'ai réalisé que cette théorie servait elle-même de fondement à la science du secret, la cryptologie. En rejoignant ce domaine, par un autre hasard de la science, je mettais encore une fois mes pas dans ceux de Turing. En effet, en 1938, après sa thèse aux Etats-Unis,

à l'université de Princeton, avec le logicien Alonzo Church, ce dernier avait rejoint Bletchley Park. Bletchley était le lieu où le *Government Code & Cipher School* avait réuni des centaines de mathématiciens et de linguistes avec pour but de décrypter les codes secrets de l'armée allemande. Turing et ses collègues firent des prouesses : en 1942, les Alliés lisaient les messages secrets des Allemands.

S'agissant de mes travaux en cryptologie, ceux pour lesquels je suis récompensé aujourd'hui, j'ai envie de répondre aux trois mêmes questions que celles que j'avais posées tout à l'heure concernant mes travaux de logique.

- en qui consistent-ils?
- pourquoi les ai-je entrepris?
- en suis-je satisfait?

En quoi consistent-ils? La cryptologie est la science des messages secrets. C'est aussi aujourd'hui, à l'heure de l'Internet, l'ensemble des méthodes qui assurent l'authenticité des transactions et la confidentialité des communications. Ces méthodes sont mises en place par des programmes informatiques, lesquels reposent sur une sorte de trame mathématique, que nous appelons un algorithme. Ainsi, un algorithme de chiffrement transforme-t-il un texte en langage clair en un texte incompréhensible et un algorithme de déchiffrement fait-il l'opération inverse. Ce que je fais, c'est donc concevoir de nouveaux algorithmes, mais aussi les évaluer.

Cette activité d'évaluation repose sur la cryptanalyse, c'est-à-dire la tentative de mettre en défaut la confidentialité que l'algorithme est censé garantir. La défense et l'attaque en somme, auxquelles s'ajoute toutefois ce qui est une spécificité des recherches que j'ai menées, la preuve qu'un algorithme est capable de résister aux attaques des cryptanalystes. C'est un peu le retour à mes premiers travaux, montrer des résultats d'impossibilité, mais dans un cadre à la fois moins absolu et plus quotidien que celui ouvert par Gödel : moins absolu, car la cryptographie ne protège que compte tenu de limites prescrites à la puissance de calcul de l'adversaire ; plus quotidien, car ce sont les secrets et les transactions de tout un chacun qu'il s'agit de protéger.

Pourquoi les ai-je entrepris? Parce que la science du secret a radicalement changé il y a une trentaine d'années, avec l'invention de la cryptologie à clef publique. Cette invention a été l'œuvre de plusieurs chercheurs dont j'évoque les noms avec d'autant plus de plaisir qu'ils sont aussi des amis : Diffie, Hellman, Rivest, Shamir, Adleman. Elle permet entre autres, d'adresser un message secret à quelqu'un que l'on n'a jamais rencontré et avec qui on ne s'est pas préalablement accordé. Partant de leurs travaux, j'ai pu renouer avec une tradition qui avait été présente en France jadis : il suffit pour s'en convaincre d’ouvrir *le Traité des chiffres et secrètes manières d'écrire*, de Blaise de Vigenère, publié en 1586. En fait, cette tradition n'avait

pas disparu : elle était simplement maintenue par des chercheurs, militaires et civils, qui avaient choisi de travailler dans l'ombre, dans les univers de la défense et de la diplomatie, et auxquels je souhaite rendre hommage. J'ai la chance, en ce qui me concerne, de pouvoir faire de la cryptologie en pleine lumière dans le monde de la recherche académique, puisque la science du secret est devenue - ou redevenue - une activité scientifique ouverte.

En suis-je satisfait? Oui, car - tout comme pour mes premiers travaux - j'ai le sentiment de vivre une grande aventure intellectuelle, que je partage cette fois avec de nombreux élèves. Oui, aussi parce que cette aventure ne se déroule pas seulement dans un univers de théorie, mais qu'elle a prise sur le réel. Lorsque je restaure la preuve, reconnue incorrecte, d'une norme de chiffrement largement utilisée, lorsque j'invalide un algorithme en voie d'être normalisé, lorsque j'évalue les algorithmes cryptographiques de la téléphonie cellulaire 3G, qui succède au GSM, lorsque je donne mon avis sur la sécurité des cartes bancaires, je participe non seulement à l'avancement des connaissances, mais aussi à la mise en œuvre de la sécurité des communications et des transactions. Je me sens parfaitement à l'aise dans cette verticalité allant de la théorie à la pratique. Cette verticalité est d'ailleurs ce qui définit le département ST2I du CNRS, sciences et technologies de l'information et de l'ingénierie,

auquel appartient le Laboratoire d'informatique de l'Ecole normale supérieure que je dirige.

1954.

En 1954, l'année de la première médaille d'or du CNRS, j'avais cinq ans et j'entrais à l'école maternelle. Un peu tardivement au regard des normes actuelles, mais mes parents avaient sans doute voulu me garder un peu plus longtemps auprès d'eux après les épreuves de la guerre. Ce début de scolarité à cinq ans s'est révélé suffisant : j'ai appris à lire et à compter, et une trajectoire rectiligne m'a ensuite conduit de l'école maternelle à l'Ecole normale supérieure avec les constants encouragements de mes parents, que je remercie. Mon père est présent ce soir ; c'est une joie pour moi. Je regrette l'absence de ma mère, son état de santé ne lui permettant pas de se déplacer ; cette cérémonie l'aurait remplie de bonheur.

Le chemin de l'école maternelle à l'Ecole normale m'a conduit une première fois en ces lieux, dans ce grand amphithéatre de la Sorbonne. C'était en 1965 ; j'avais quinze ans, j'étais en classe de première et j'y ai reçu un prix des mains du Premier ministre de l'époque, Georges Pompidou. J'étais, tout comme je le suis aujourd'hui impressionné par la majesté de cet amphithéatre; j'étais intrigué par les fresques de Puvis de Chavannes; enfin j'étais fier - comme aujourd'hui - de la distinction qui

m'était remise. Peut-être cette cérémonie a-t-elle joué un rôle dans le choix que j'ai fait trois ans plus tard d'entrer à l'Ecole normale supérieure.

L'Ecole normale, j'y suis en fait entré deux fois. En 1968, comme élève et vingt ans plus tard pour y donner d'abord un cours, puis y devenir professeur. Comme élève, j'ai été parfaitement heureux à l'Ecole. C'était un espace d'absolue liberté. Le professeur responsable des mathématiques exerçait un magistère lointain mais bienveillant : nous étions donc libres de nos choix scientifiques, quoiqu'il les désapprouvât parfois. En ce qui me concerne, je crois bien que mon choix de la logique ne lui plaisait guère, mais il n'a pas cherché à s'y opposer.

Comme professeur, j'ai été et je reste comblé par l'environnement de l'Ecole. Fier également, en particulier, de deux projets que j'ai pu mener à bien. Le premier est l'installation rue d'Ulm d'une équipe de recherche en cryptologie. J'en ai déjà parlé mais je voudrais redire à quel point je mesure le privilège que j'ai eu d'accueillir des jeunes gens et des jeunes filles tous extrêmement brillants et à quel point j'ai apprécié l'atmosphère d'émulation intellectuelle que nous avons créée ensemble. Le second, c'est la mise en place en 1999 d'un département d'informatique: avec mes collègues, nous pensions que l'informatique devait prendre son envol et que nous devions proposer aux normaliens un cursus spécifique.

C'était une décision logique et sans doute inéluctable, mais je suis heureux d'en avoir pris la responsabilité.

1954.

En 1954, l'informatique était à ses débuts. Le premier ordinateur avait en effet été construit moins de dix ans auparavant. Il y a d'ailleurs une compétition pour le titre de "premier ordinateur". On considère souvent que ce titre revient à l'ENIAC (*Electronic Numerical Integrator and Computer*) construit en 1946 aux Etats-Unis. Cette énorme machine était composée de 19000 tubes et pesait 30 tonnes. Elle était capable d'effectuer environ 330 multiplications par seconde, ce qui - ramené à son poids -, constitue une bien modeste performance au regard des normes actuelles. L'autre candidat, que les cryptologues mettent en avant, est le Colossus, construit en Angleterre en 1944, sur la suggestion de Turing lui-même. Cette machine là, tout aussi gigantesque, ne savait même pas faire une multiplication, mais elle était capable de briser certains codes secrets de l'armée allemande. C'est peut-être en pensant à ces premiers calculateurs qu'on appréhende le mieux la nature de l'informatique. Elle est fille des mathématiques, science de l'abstraction, et de la physique, science de la matière. Son objet est précisément la mécanisation de l'abstraction. Autour de ce but, une communauté scientifique active s'est constituée et a, dans les soixante dernières années, développé un ensemble de

concepts rigoureux et de méthodes structurées. Pour la première fois, la médaille d'or du CNRS est décernée à un membre de cette communauté scientifique et, très clairement, au delà de moi, c'est toute la communauté des informaticiens qui est honorée.

Dans les soixante dernières années, les usages de l'informatique se sont également développés, jusqu'à modifier radicalement notre vie quotidienne. Cette véritable mutation a été la conséquence de progrès nombreux, où la double filiation de l'informatique est apparue en permanence. L'invention du transistor en 1947, celle du circuit intégré en 1958, puis celle du microprocesseur dix ans plus tard portent clairement la marque de la physique, tandis que celle de la compilation dès 1947, des langages de programmation, des algorithmes permettant le traitement efficace ou la compression de l'information, celle encore de la cryptologie à clef publique en 1976, révèlent leur origine mathématique. Dans certains cas cependant, la filiation est moins claire: la souris est-elle d’abord un objet physique ou un dispositif symbolique de pointage? L'Internet est-il principalement un ensemble de protocoles abstraits ou une agrégation de réseaux physiques? En tous cas, toutes ces inventions dessinent, en ce début du vingt et unième siècle, un monde différent, un monde de communication et de connaissance instantanés.

Dans ce monde, c'est une évidence de l'affirmer, la recherche joue un rôle essentiel. D'abord, parce que c'est elle qui est le moteur de la connaissance mais aussi, et c'est particulièrement vrai de la recherche en informatique, parce que l'innovation est source de compétitivité et donc de richesse. La recherche comme moteur de la connaissance, c’est celle que je connais le mieux, celle qui est portée par les universités, par les grandes écoles, comme la mienne, par les grands organismes, au premier rang desquels se trouve le CNRS, mais aussi l'INRIA qui, dans le domaine de l'informatique, joue un rôle également éminent. Fondamentale ou appliquée, elle est irremplaçable. La recherche comme source de richesse, c’est le processus par lequel l'innovation se diffuse dans le tissu économique. Je n'ai pas directement participé à l'émergence ni à la consolidation d'une stratégie industrielle : les exigences de la recherche ne sont sans doute pas faciles à concilier avec la vie d’un capitaine d'industrie. Par contre, j'ai eu bien sûr, dans ma carrière, de nombreux contacts avec le monde de l'entreprise et certains de mes élèves ont franchi le pas. Mes deux enfants également, jeunes entrepreneurs talentueux au sein d'une entreprise informatique, dont ils sont parmi les fondateurs. Cette proximité me permet de comprendre que les défis de l’innovation industrielle ne sont pas moindres que ceux de la création scientifique.

Dans le monde de la connaissance, quelle est aujourd'hui la place de la cryptologie? Elle était intimement liée à l'informatique des commencements, on l'a bien vu. Elle reste présente dans l'agora virtuelle constituée par l'Internet et le WEB, à tel point qu'on peut véritablement parler d'ubiquité de la cryptologie. Chacun d'entre nous l'utilise - sans le savoir - dans nombre de gestes de la vie quotidienne : en téléphonant avec son portable, en payant avec sa carte bancaire, en faisant des achats sur le Net. A l'heure où sont envisagés la création d'identités numériques et l'archivage massif de nos données personnelles, notamment médicales, elle est aussi appelée à jouer un rôle essentiel pour la protection de nos libertés, afin que ces données ne soient accessibles qu'à ceux qui ont le besoin d'en connaître. Elle n'est plus seulement la science du secret mais aussi la science de la confiance.