Press Conference

CNRS Gold Medal for 2006

Friday October 6, 2006

CNRS – Paris

PRESS FILE

Contact details - Medalist

Jacques Stern Tel. (33 0)1 44 32 20 34
Jacques.Stern@ens.fr

Contact details - Press relations

Martine Hasler Tel. (33 0)1 44 96 46 35
Martine.hasler@cnrs-dir.fr

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Press Conference
CNRS Gold Medal for 2006

Contents

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

The CNRS Gold Medal for 2006 has been awarded to Jacques Stern, Professor of Computer Science and French cipher expert

PRESS RELEASE – PARIS – OCTOBER 6, 2006 www.cnrs.fr/presse

The CNRS Gold Medal, France's highest distinction for scientific research, has been awarded this year to Jacques Stern, 57, Professor at the ENS *École normale supérieure* (ENS), Director of the ENS Computer Science Laboratory (a combined ENS/CNRS unit) and a researcher with a global reputation for his work in cryptology. The originator of 150 publications, very much a founding father of a school of cryptology that has put France at the forefront of the discipline in Europe, Jacques Stern began his career as a mathematician before becoming interested in computer science and moving on to cryptology. A summary which matches the recent development of this discipline …

Internet, bank accounts, online auctions, electronic voting, telephone communications … Although cryptology remained for many years a domain reserved for the military and diplomats, its extremely wide-ranging contemporary applications are highly important for the general public.

A world-renowned French specialist, Jacques Stern did groundbreaking work on cryptology in France, devoting 20 years to research in this field. Initially a mathematician (logic and set theory), he subsequently became interested in algorithmic complexity before setting out to do research in this area.

A graduate of the *École normale supérieure* and the holder of a science doctorate, Jacques Stern is now an ENS professor at the Rue d'Ulm in Paris, where he heads up the ENS Computer Science Laboratory (LIENS – a combined ENS/CNRS unit) and the Computer science department. He is the author of 150 scientific publications, a book entitled *La Science du Secret* [The Science of Secrecy] (published by Odile Jacob) and a report to the French government which led to new cryptography regulations. Awarded the CNRS Silver Medal in 2005, a *Chevalier* of the *Légion d'honneur*, Jacques Stern received the Lazare Carnot Prize in 2003 from the French *Académie des sciences* for his lifetime achievement in this field.

The recognition of 20 years of research symbolized by the award of the CNRS Gold Medal provides an opportunity to pay homage to a unique area of science which for many years, due to its very nature, sought meaning in secrecy but which, with digitization and the globalization of trade, now affects the vast majority of the population.

A novel scientific discipline

From the etymological standpoint, cryptology means “the science of secrecy”. The first “work” in this field dates back to a time several centuries BCE and with the passage of time cryptology has become a fully-fledged scientific discipline whose aim is to ensure the integrity of information, its authenticity and its confidentiality in terms of data and transactions. To accomplish this, it lays down “game rules” and techniques designed to resist the efforts of “opponents” who do not play by the rules. Examples: the encryption of diplomatic messages must counter the efforts of other countries’ intelligence services; a bank must be sure of the identity of a credit card holder, and so on.

The broad principles are straightforward. To exchange information whose confidentiality two protagonists (organizations or individuals) want to preserve, and for each to be sure of the identity of the other, each must have both a key to identify himself and a formula to encrypt and then decrypt the message. From this point on, things get more complicated. The concepts require the use of the most sophisticated mathematics. Modern researchers draw inspiration from the work of mathematicians such as Alan Turing who explored the outer limits of mathematical thinking in the 1930s, following in the footsteps of Kurt Gödel.

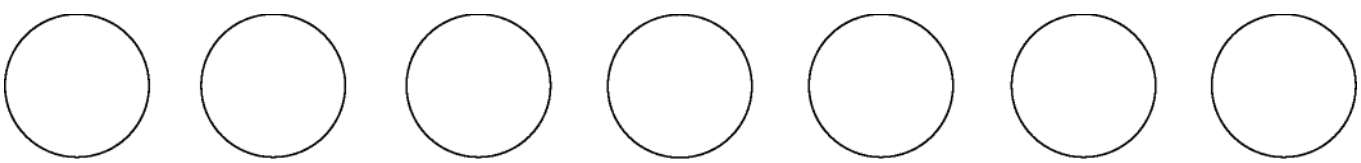
Technically speaking, cryptology has converged with computer science from the end of the World War II and scientists make intensive use of the computer as a tool to generate or “break” the most powerful encryption algorithms. Finally, from the standpoint of economics, this is a fast-growing sector due to the exponential spread of electronic communications.

Although the simplest terms such as “secret code number” or “PIN code” for the bank card and the “SIM” card for mobile telephones are used on daily basis by everybody, who knows what “secret key”, “public key”, “RSA”, etc. mean? Such terms hide a discipline that is currently boiling over with new ideas, one that has become indispensable, is often of strategic importance and holds great scientific riches.

Four major areas of work for modern cryptology

This award of the CNRS Gold Medial for 2006 pays homage first and foremost to the work of a researcher, but it also salutes the work done by his team, one that is at the cutting edge in Europe, enjoys a global reputation, and has made major breakthroughs in several fields possible in the space of twenty or so years, particularly in what are currently cryptology’s four major areas of work.

The design of algorithms gives rise to new cryptographic schemes that are constantly needed to meet new requirements (authentication, signatures based on smartcards). Jacques Stern and his team have for example been able to prove an authentication algorithm called “GPS” designed in conjunction with France Telecom, which became an ISO standard in 2005.



CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

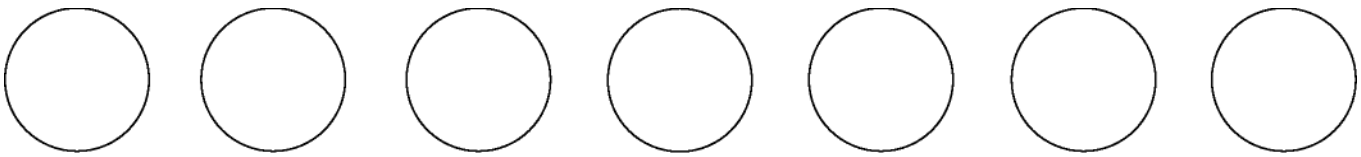
Cryptanalysis is used to “break” supposedly impenetrable ciphers. The ENS/CNRS team has for example proved how fragile reputedly robust or unbreakable algorithms can be; in 1998, the team was able to “break” an IBM algorithm intended as an alternative solution to RSA using mathematical tools provided by the geometry of numbers.

Proven security. It is not because an algorithm has withstood cryptanalysts’ efforts to break it that it is secure! Proof has to be provided, and that is for example what the ENS cryptology team were able to do when they helped “salvage” an encryption standard. In 1994, an American team published an algorithm that then became the standard for transactions over the Internet. In 2000, there was panic among Internet users when the rumor began to spread that the proof was incorrect. The ENS/CNRS team, in collaboration with Japanese researchers, were able to come up with one that is correct.

Applications and protocols. Electronic voting, online auctions on the Internet, 3G telephony, the French teams working with Jacques Stern have made their mark on new cryptographic schemes involving a multiplicity of actors. The word is that cryptology is now ubiquitous.

To find out more:

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



Glossary

Cryptology in 10 keywords

Authentication
A procedure for checking the identity of an entity or the origin of a message or file.

Key
The item of information needed by sender and receiver to send and receive confidential messages or data, or to authenticate their identity.

Cryptanalysis
This is the effort to break a cryptographic system, especially in order to evaluate the real degree of security it actually provides.

Cryptography
The design of cryptological mechanisms intended to guarantee security for the purposes of confidentiality, authentication and the protection of data integrity, as well as for other purposes such as assured anonymity.

Asymmetric cryptography (public key)
The algorithms are public, but each individual holds a pair of keys: one is secret and allows that individual to carry out procedures only he or she is supposed to be able to do (signatures and decryption), whereas the public key is disseminated in order to allow that individual to carry out reciprocal operations (signature verification or message encryption). The roles of the two keys are “asymmetric”, hence the term.

Symmetric cryptography (secret key)
The algorithms are public, but a secret piece of information shared by sender and receiver allows them to be used by more than one person. This system is said to be “symmetric” because the levels of information held by sender and receiver are identical.

Cryptology
From the Ancient Greek *kryptos* (hidden) and *logos* (science), "cryptology" literally means the "science of secrecy" and its purpose is to hide the information contained in a message. Its aim is threefold: to ensure confidentiality, to guarantee authenticity and to preserve the integrity of the information. This science, born several millennia ago but organized into a true discipline only over the last few decades, is essentially composed of two fields of study, cryptography and cryptanalysis.

Security Proofs
A methodology which supplements cryptanalysis by providing mathematical proofs that there are no flaws in the encryption scheme.

RSA
So-called for its inventors, Ron Rivest, Adi Shamir and Leonard Adleman, this was the first algorithm to be based on the public key principle.

Digital signature
An authentication service which has had legal force in France since the law of March 20, 2000. It enables verification of the identity a given entity or the origin of a message or file.

Jacques Stern

© CNRS photolibrary – Christophe Lebedinsky

Twenty years in the service of cryptology

or the man who made our communications and transactions more secure.

"I have always been attracted by near-horizon science. I like to see my ideas move on quickly to the application stage…". Talking to this calm, soft-voiced man using terminology that is precise, but above all concrete, one understands quickly why as a young teacher and researcher in mathematics (who graduated from the *École Normale Supérieure* at the age of 22 and started teaching at Caen University at 30) switched horses in the 1980s, at a time when computer science was beginning to take off, to become the standard-bearer for French cryptology. A need to have an impact on the real world.

But it was a smooth transition, not a radical break. The way was prepared by his earliest research work on logic, which is the closest mathematical specialty to computer science. Jacques Stern explains: *"I was interested impossibility results in set theory"*, talking in his very tidy office at the Rue d'Ulm in Paris, near which, down one corridor, the following could recently be seen posted up: *"la crypto c'est rigolo!"* [Cryptology is a gas!]. At the time his inspiration came from the mathematicians Kurt Gödel, Alan Turing and Paul Cohen. This was the same Turing who "broke" the ciphers used by the German army in the 1940s … *"When I looked at what happens at the outer limits of mathematical thinking I came across cryptology. I have always been fascinated by certain paradoxes encountered in logic, as well as in cryptology: how might it be possible to send secret correspondence without ever having previously met your correspondent?".*

So his mind was made up: the year was 1986, cryptology had become an academic field of study since the invention of the "public key" concept in 1976. The field was in its infancy in France, but *"this was an area of science in which I wanted to be a player".*

A French school of cryptology

Driven by the man who is a professor at ENS today, director of its Computer science department and the head of the ENS Computer Science Laboratory (LIENS, a combined ENS/CNRS unit), a genuine French school of cryptology came into being in the space of 20 years. The work done by him and his team at LIENS came to involve all the discipline's major fields: algorithm design, cryptanalysis (attempting to break systems proposed by other experts), security proofs, definition of standards for cryptographic systems, and, lastly, protocols and applications, especially in connection with the Internet and electronic voting in particular.

Recognition, internationally and at the highest levels, was quick to come for this scientist and his work, which were to generate over 150 publications and a large number of doctoral theses. Author of *La Science du secret* [The Science of Secrecy] (published by Odile Jacob), Jacques Stern was awarded the CNRS Silver Medal in 2005. He was also responsible for a report to the government on new cryptography regulations.

A *Chevalier* of the *Légion d'honneur*, Jacques Stern was awarded the Lazare Carnot Prize by the French *Académie des sciences* for his "lifetime achievement". Married and father of two, there is nothing excessive about him. While he does not lack modesty, you feel that he is proud in a way of having made our transactions more secure. His profoundly calm character cannot disguise the passion he feels for a discipline that demands a great deal of him. It leaves little time for his other favorite activity: opera. *"Classical opera, I have to say …".*

Jacques Stern

Born August 21, 1949 in Paris

Education and training: an academic background

- Secondary school studies at the *Lycée Michelet* and the *Lycée Louis-le-Grand* in Paris
- 1968: accepted for entrance to the *École Polytechnique* and the *École Normale Supérieure* (ENS)
- 1968-1972: student years at ENS
- 1971: passes the high-level *Agrégation* competitive examination in mathematics
- 1975: awarded a Doctorate in Science

Career: from mathematics to cryptology, taking in computer science on the way

- 1972-1978: teaching assistant, then assistant professor at Paris 7 University
- 1979-1986: professor at Caen University
- 1986-1992: professor at Paris 7 University
- 1986-1998: associate professor at the *École Polytechnique*
- 1992-1993: Research director at CNRS
- 1993 -: professor at ENS
- 1996 -: Director of the ENS Computer Science Laboratory (LIENS, ENS/CNRS)
- 1999 -: Director of the ENS Computer Science Department

Publications and books

- 150 scientific publications between 1975 and 2006
- 30 doctoral theses supervised
- A book: *"La Science du secret"* published by Editions Odile Jacob.

Prizes and honors

- *Chevalier* of the *Légion d'honneur*
- Awarded the Lazare Carnot Prize by France's *Académie des Sciences* in 2003
- Fellow of the IACR (International Association of Cryptology Research)
- CNRS Silver Medal for 2005
- CNRS Gold Medal for 2006

The importance of cryptology

The first faltering steps in cryptology were taken several millennia ago. Despite this, cryptology is a very young science which began to come into its own only with the arrival of digital computing and the spread of telecommunications. For many years a closed world reserved for the military and diplomats, it now affects everybody since the Internet's exponential take-off. What are its technical and societal issues, its resources and its future prospects? These questions can be answered with a look at the work done by the ENS/CNRS team.

What do the SIM card in your telephone, a bank card, and your favorite Internet online shopping sites have in common? The answer is in just one word: cryptology.

Indeed, the information society has made the use of cryptology an everyday affair. Mobile telephones, bank cards, transport documents, medical ID cards, cable and satellite TV decoders, the Internet ... countless items in our everyday lives incorporate security mechanisms. For instance, cryptographic algorithms guarantee that nobody can make a telephone call at your expense, intercept a bank card number on the worldwide web, access the confidential details on your medical ID card, and so on.

Once restricted to diplomatic and military usage, cryptology is now a fully-fledged scientific discipline whose applications are so wide-ranging that it is difficult to define what its precise boundaries might be in principle. Initially, its purpose was to study methods capable of providing guarantees of the integrity, authenticity and confidentiality of communications and information systems. Based on the use of encryption keys, it now covers the whole range of computerized processes that need to withstand the efforts of opponents who are not playing "by the rules".

What is cryptology?

Essentially, cryptology is the art of hiding information in an encrypted message. It is an art that is very ancient: the first ciphers date back to antiquity.

It has two major divisions:

- **cryptography** relates to the design of mechanisms intended to guarantee security notions.
- **cryptanalysis** involves attempts to penetrate cryptographic systems, especially in order to discover exactly what degree of real security it actually provides.

It must meet three needs:

- It serves to guarantee data integrity to ensure that the content of a message or file has not been modified with malicious intent.
- It serves to authenticate the identity of a given entity or the originator of a message or file. Where a file is concerned, and if the entity that created it is the only possible source of a guarantee of authenticity, this service is one of "non-repudiation". This is provided by a digital signature, which has legal force since the passing of the law of March 20, 2000.
- It serves to protect confidentiality, ensuring that the content of a message or file cannot be accessed by third parties. Confidentiality services are provided in many contexts, but especially in mobile telephony, pay television and Internet browsers using the SSL/TLS protocol.

The core concepts

Until the end of the 19th century, most cryptographic techniques based their security on the fact that the "algorithm" itself was kept secret, which meant that they were not suitable for use by large groups of individuals. It was for this reason that the mechanism was later personalized by means of a small item of information called a **secret key** shared by both sender and receiver. Later, the methods of such **secret-key symmetrical cryptography** improved, becoming more complex with the arrival of electronics and digital computers.

Cryptology underwent a radical transformation at the time Internet was coming into being, with the appearance on the scene of so-called **public-key** cryptography, which opened up a rich vein of research covering the whole range of practical security issues: authentication, confidentiality, commerce, e-voting, e-auctions and all the other forms of data exchange requiring integrity, non-repudiation or anonymity. Indeed, in 1976 two scientists, Whitfield Diffie and Martin Hellman, came up with the idea of making the entire encryption process completely public, not only the algorithms, but also the a key specific to the receiver, the public key. Only the decryption key would remain secret. This meant that each individual would hold a pair of keys, one public, to be used by his or her contacts to encode messages, and the other secret, used by that individual to decipher the messages received, and originally encrypted using that individual's public key. Such **asymmetric cryptography** also makes signature schemes possible. Decryption, which can be done only with knowledge of the secret key, thus becomes a signature algorithm. Conversely, the reciprocal operation, encryption, available to anybody, becomes a verification algorithm which must lead back to the initial message. This means that non-repudiation can be guaranteed.

This principle was applied as early as 1978 in the RSA algorithm invented by Ron Rivest, Adi Shamir and Leonard Adleman. When RSA is used, the security comes from the difficulty of computing the prime factors of a whole number containing at least several hundred digits: the record – which dates back to May 2005 –

is 200. In addition, where authentication is concerned, an RSA signature can be verified using the public key alone, whereas its creation requires the holder's secret key, which guarantees non-repudiation.

Such public-key cryptography provides solutions to make an electronic transaction impossible to repudiate and to protect its confidentiality, or the anonymity of a vote. But a warning is in order: the system's effectiveness is based on "trust", which must itself be underpinned by management of the public keys by a Certification Authority empowered to issue and sign keys (banks, tax authorities, corporations, government ministries for example). Furthermore, the security of these mechanisms is not unconditional, but dependent on mathematical hypotheses that need to be clearly identified if their validity is to be assessed. What is at stake here are two major problems that face both the public authorities and the scientific community in order to ensure that cryptography can provide protection for individual freedoms in a world where digital technology is omnipresent, but without running the risk of its misuse for dishonest purposes.

Over the last thirty years, research into cryptology has seen substantial development, focusing on the design and evaluation of symmetrical algorithms and public key systems. This research has gone hand in hand with an effort to define standards that has exceptionally deep roots in the most recent studies and is based on close collaboration between the academic and corporate sectors.

French research at the cutting edge

Without going into detail on all the work that has been done, we can mention here two promising avenues of research that have opened up in recent years and which are being pursued at the LIENS laboratory, under the leadership of Jacques Stern.

Proven security

The greatest stride forward made by asymmetric cryptography since its invention is the introduction of the provable security, or security proof, methodology, which complements cryptanalysis insofar as it provides real proof that there are no flaws in the protection. The first task is to model the security itself as such and then to construct cryptosystems whose security is proven within this model, on the basis of precise and credible mathematical hypotheses.

The security proof is based on a reductionist approach: the security notion is translated into a hypothesis as to the difficulty of using computation to resolve a problem that is both well-known and well-defined, such as integer factorization or computing discrete logarithms. If the hypothesis is verified, the system is secure. The main benefit of this approach is that it enables the assumption on which the security is based to be clearly identified, and its main drawback is that absolute proof is not obtained: all that has been achieved is that a complex expression has been replaced by a clearer hypothesis. What remains to be done is to monitor progress made on solving problems deemed to be difficult and to size the keys accordingly.

Unfortunately, in most practical asymmetric cryptosystems, and especially those that have been standardized, the translation of the complex expression into a clearer hypothesis is not necessarily relevant to keys of ordinary size. To overcome this problem, researchers have applied an idealization of the integrity functions, also called "hashing", which is known as the "random oracle" model. This boils down to positing an extra hypothesis that the code breaker will not make use of the intrinsic features of the hashing functions used. Using this ideal model, many effective cryptographic systems have been proven to be secure on the basis of plausible computational hypotheses.

Cryptography based on identity

Another major issue for asymmetric cryptography is how to manage the public keys – or to be more precise, how the authenticity of the keys is to be guaranteed. In the case of the Internet, this issue has been resolved at the present time by the certificates familiar to habitual users of online shopping sites. Identity-based asymmetric cryptography offers an alternative solution by enabling the public keys to be directly linked to the user's identity: any chain of characters, an email address for example, can potentially serve as a public key.

This is made possible by the intermediation of a Certification Authority trusted by all users: the Authority chooses public parameters and on each occasion that a user wishes to register a public key (arbitrarily chosen), the user sends it to the Authority, which then returns the corresponding secret key. Unlike the procedure followed in systems based on conventional public keys, the Authority has knowledge of all the secret keys.

Identity-based cryptography is spreading rapidly at the present time, despite the fact that it is not without its drawbacks. In addition, it has had to call on complex mathematical theories whose algorithmic dimension has not so far been subjected to in-depth research.

To find out more:

- Jacques Stern, *La science du secret,* Editions Odile Jacob, 1997.
- David Kahn, *The Codebreakers, The Story of Secret Writing* (Revised Edition, Scribner, 1996).
- *Paradigmes et enjeux de l'informatique* [Paradigms and issues in computer science], edited by Nicole Bidoit, Luis Farinãs del Cerro, Serge Fdida, Brigitte Vallée, Editions Lavoisier, 2005. Chapter 6: "La cryptologie: enjeux et perspectives" [Cryptology: current issues and future prospects]. Phong Q. Nguyen, Jacques Stern.
- David Pointcheval, *La cryptographie à l'aube du troisième millénaire* [Cryptography at the dawn of the third millennium], Revue de l'électricité et de l'électronique [Journal of electricity and electronics]. Volume 5, pages 28-34. In-depth dossier *La sécurité des systèmes d'information* [The security of information systems] SEE, May 2001.

Key dates

2,500 years of well-kept (or not so well-kept) secrets

Cryptology goes back in history as far as organized human societies have needed to keep secret certain items of information. History contains a wealth of highly original inventions for doing so. Until the arrival of digital computing – which changed everything.

5th century BCE
The Greek Skytale: a strip of papyrus that had to be wrapped around a wooden rod of known diameter for the message to be read.

Rome (1st century BCE)
Caesar's Cipher: a cryptographic system for the encryption of military messages in which each plaintext letter is replaced by another designated by a fixed shift along the alphabet.

9th century CE
Al Kindi, an Arab scholar and philosopher. He is the author of the first known manuscript devoted to cryptology.

15th century CE
Alberti's Wheel: a system of concentric disks.

16th century CE
The Cardan Grille: a grid-based system.

1863
A Prussian officer, Friedrich Kasiski, looks in *Ciphers and the Art of Decryption* at the statistics of the frequencies with characters recur in a text in a given language. He defines and introduces an invariant called the "index of coincidence", which makes codebreaking easier.

1883
Auguste Kerckhoffs, a Flemish linguist and cryptologist, sets out in his monograph *La cryptographie militaire* a number of fundamental principles for encryption, including the notable fact that it must be possible for the mechanism to *"fall into the hands of the enemy without inconvenience"* .

1919
Two patents are filed for the first "cipher" machines in this year: the Enigma, used later by the German army, and the Hagelin, adopted by the Allies.

1930
The work of Kurt Gödel and Alan Turing on the outer confines of mathematical thinking, leading to the concept of "concrete impossibility", which refers to the existence of statements that can be neither proved nor refuted.

1938
Alan Turing, a British mathematician, joins the GE&CS (Government Code and Cypher School).

1940
Turing "breaks" the German army's ciphers.

1945
The first digital computers.

1976
Asymmetric cryptology is born. Whitfield Diffie and Martin Hellman, in a paper entitled *New Directions in Cryptography,* make the encryption process entirely public, including the key specific to the receiver, called the public key. Only the decryption key must remain secret. This marks the invention of the public-key concept in cryptography.

1978
RSA: The first asymmetric encryption mechanism is designed by Ronald Rivest, Adi Shamir and Leonard Adleman.

1981
The first academic Cryptology Conference "Crypto" is held; it has taken place every year since in Santa Barbara in California.

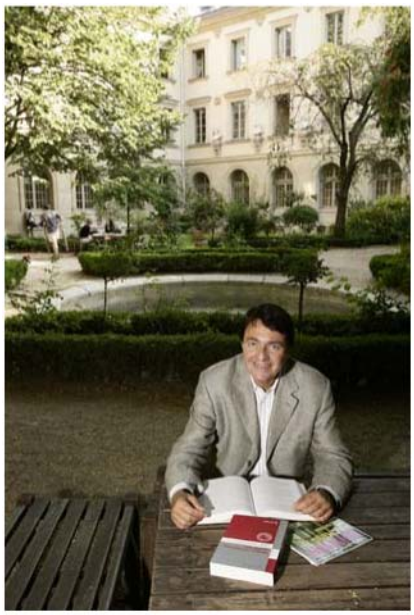
CNRS 2006 Gold Medal
Jacques Stern

© CNRS Photolibrary – Christophe Lebedinsky

Ref 01

Ref 02

Ref 03



Ref 04

Ref 05

Ref 06

Ref 07

Ref 08

Ref 09

Ref 10

The Engineering Department	**Information Science and Technology** **Science and Technology for Engineering**
	The Computer Science Laboratory of the *École Normale Supérieure* (LIENS – a combined ENS/CNRS unit), of which Jacques Stern is head, forms part of the CNRS Engineering Department
The Department 255 integrated or associated laboratories 1,910 researchers 6,256 teacher/researchers 3,134 engineers, technicians and administrative staff €28,390,000	**The Department** ➢ ***Its Philosophy*** The **Engineering Department** is the product of a merger between the Department of Engineering Sciences and the Department of Information Science and Technology. One of its core qualities is its open character: openness to other disciplines, openness to the corporate sector, openness to society at large, and so on. It offers a special interface. ➢ ***Its aims*** It primary aims are to build a scientific approach centered on the production of knowledge and on human beings – human beings and their needs, human beings and health, human beings and their products – and, as a consequence, it aims to develop a systemic approach to the design, production and application of systems that are more secure, communicate better, offer enhanced performance and are more environmentally friendly. These objectives are part of the overarching strategy of the CNRS which is to develop fundamental concepts and technologies, to be present at the cutting edge of knowledge and to bring to light new topics for study, in addition to responding to the major challenges facing society.
	➢ ***The main focuses of its research***
Information Science and Technology: computer science, automation, signals and communication 78 integrated or associated laboratories 465 researchers 3,000 teacher/researchers 750 engineers, technicians and administrative staff €8,492,000	Communications, the security and safety of hardware and software systems, mechanical systems, energy, engineering for the life sciences... the Engineering Department is focused on gaps in the information sciences and technologies and in engineering science and technology. To accomplish its aims, it sets out to provide synergy between disciplines while consolidating them individually: computer science, automation, signals and communication; micro- and nanotechnology, electronics, photonics, electromagnetism, electrical power; materials and structural engineering, solids mechanics, acoustics, biomechanics, biomaterials; the mechanics of heterogeneous fluid and reactive environments; characterization, transfer properties, processing techniques, and so on. The Department also wishes to adopt a common approach to the search for understanding: modeling and observation based on intensive simulation and experiment; for design and construction: the definition of specifications based on an expressed requirement and subsequently tracking back from those specifications to components and systems; for the control, optimization and management of the complexity linked to mobility, large masses of data and networks: Energy, the Life Sciences, the Human and Social Sciences; to generate new applications. The Engineering Department bases its approach on a proactive policy for development and interdisciplinary work with the Life Sciences, in the domains of energy and complex systems. It also relies on the building of partnerships with the corporate sector, centers of competitive excellence, the Carnot Institutes, thematic advanced research networks, etc. … but also including partnerships with universities, the high-level French *Écoles*… with the goal of enhancing an integrated approach and training through research. In addition, the Department also applies a policy directed at openness to Europe and the international community.