

Cryptography in Financial Transactions: Current Practice and Future Directions
by Professor Jacques STERN

In this talk I will briefly describe the history of cryptography and explain how it became an area of scientific research, served by a strong community both in academia and in the industry.

Next I will cover two case studies.

The first is related to banking cards and payment terminals and the second to Internet banking. In both cases, I will show how cryptographic tools crafted within the research community in the past thirty years entered the picture and how cryptographers were able to provide stronger and stronger levels of security.

While applications are now stable in the first area, there is more to come in the second.

Jacques STERN is Director of the Computer Science Department (LIENS) at *Ecole Normale Supérieure* in Paris, and father of a school of cryptology in France which is at the forefront of the discipline in Europe. He has published about 150 scientific articles between 1975 and 2006.

LIENS is a combined ENS-CNRS unit. Its aim is to develop a systemic approach of the design, production and application of systems that are more secure, that communicate better, offer enhanced performances and that are more environmentally friendly.

Since September 2007, Professor Stern is also chairman of the French National Agency for Research (ANR).

Aims and presentation of cryptology or the "Science of secrecy":

For many years, cryptology was used for military and diplomatic issues. It's a young science which developed with the arrival of digital computing and telecommunication after World War II. In 1976 the concept of "public key" was born and in 1986 cryptology became an academic field of study. Now cryptology is part of our daily life: Internet (login), bank (secret code numbers), mobile telephone (SIM card), satellite TV decoders, medical ID cards, transport documents, cable, etc.

The aims of cryptology are to ensure the integrity of information, its authenticity and the confidentiality of data and transactions.

Cryptology is divided into cryptography and cryptanalysis.

- **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.

Crypto Team's Projects:

Coordinator of CESAM's project: program for improving security and decreasing energy consumption of mobile equipment.

Coordinator of AZTEC laboratory and ECRYPT network: to intensify the collaboration of European researchers in information security and more particularly in cryptology and digital watermarking (<http://www.ecrypt.eu.org/partners.html>)
