Chaire d'excellence Pierre de Fermat

Cette manifestation est organisée dans le cadre de la Chaire d'excellence Pierre de Fermat décernée par la région Midi-Pyrénées au Professeur Jean-Jacques Quisquater pour la période 2004-2006.

Ce séminaire s'adresse à un large public et sera suivi d'un cocktail.
Le séminaire se tiendra à l'Hôtel de Région, 22 boulevard du Maréchal Juin, Toulouse.
Accès gratuit, mais inscription impérative avant le 4 septembre 2006.

Inscription obligatoire :

- par mail à : histocrypt@laas.fr
- ou par fax au : 05 61 33 64 11
- ou sur papier libre à l'adresse ci-dessous.

Attention, n'oubliez pas de mentionner : nom, prénom, organisme, présence aux conférences et présence au cocktail qui suivra.

LAAS-CNRS
Pôle SINC
7 avenue du Colonel Roche
31077 TOULOUSE Cedex 4 FRANCE

Séminaire «Chaire Pierre de Fermat»

Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS

HISTOIRES SECRÈTES DE CODES SECRETS

par

M. le Professeur Jean-Jacques Quisquater
Université Catholique de Louvain - Belgique

Dr. David Kahn
Journaliste et écrivain, historien de la Cryptologie - USA

Vendredi 8 septembre 2006 de 17h00 à 19h00
Hôtel de Région, Salle du Conseil

Organisé par le LAAS-CNRS avec le soutien de la Région et de l'Adermip

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE — LAAS — RÉGION MIDI-PYRÉNÉES — ADERMIP

Jean-Jacques Quisquater

Le Professeur Jean-Jacques Quisquater est de nationalité belge. Il est marié (Myriam), a deux enfants dont Michaël, chercheur … en cryptographie (à l'INRIA).

Il est ingénieur civil en mathématiques appliquées (1970) et a un doctorat d'Etat en science informatique obtenu en 1987 au Laboratoire de Recherche en Informatique (LRI) d'Orsay.

Il a travaillé entre 1970 et 1991 au laboratoire de recherches Philips où il dirigeait une équipe en cryptographie: il a ainsi contribué à l'étude de la mise en œuvre de la cryptographie dans les cartes à puce (2 premières mondiales : première carte à puce avec le DES, système standard de cryptographie à clé secrète, première carte à puce avec un coprocesseur RSA standard de cryptographie à clé publique).

Il est aujourd'hui professeur de cryptographie et de sécurité multimédia au département d'électricité, à la Faculté de Sciences Appliquées de l'Université Catholique de Louvain, à Louvain-la-Neuve (Belgique).

Il est le principal concepteur des coprocesseurs cryptographiques Philips actuels pour les cartes à puce. Il détient 17 brevets dans le domaine de la carte à puce. Il a publié plus de 150 papiers dans des revues de conférences internationales, dans les domaines de la théorie des graphes et surtout de la cryptographie. Il est co-inventeur d'un schéma cryptographique fort connu, le protocole GQ, utilisé par environ 100 millions d'ordinateurs – clients dans le monde, sous licence Novell (NDS, netware). Il a un nombre d'Erdös de deux.

Il est un directeur de l'IACR (International Association for Cryptology Research), membre des comités d'organisation de CARDIS et ESORICS, et de plusieurs comités IFIP. Il a reçu un doctorat honoris causa de l'Université de Limoges, le prix Montefiore, l'Award Kristian Beckman de l'IFIP et la chaire Fermat de Midi-Pyrénées (sans compter la Chaire Franqui, en Belgique) pour 2004.

L'exposé

«Les khipus donneront-ils la clé des secrets de l'histoire des Incas ?»

L'histoire des Incas reste aujourd'hui un grand mystère. En effet, il n'y a pas d'écriture connue utilisée par les Incas. Les Incas dominèrent une partie importante de la côte ouest de l'Amérique du sud, avec un empire d'une longueur maximum de 4.700 kilomètres ; et ce pour une durée d'un siècle, juste avant l'invasion par les Espagnols. Curieusement, et pas trop loin, régnaient les Mayas où il y avait bien une écriture. Des chroniques espagnoles, nous savons que les Incas étaient très organisés et utilisaient un système élaboré de comptabilité basé sur des noeuds et des cordelettes, les fameux khipus (aussi écrits quipus). Ces khipus devaient servir à bien des choses et bien des questions demeurent sans réponse. Calendriers ? Recueils de leur histoire ? Poésies ? Codes secrets accessibles uniquement aux chefs Incas ? ...

L'exposé fera le tour de la question et montrera qu'en mettant toutes les connaissances éparses stockées dans différents musées du monde et autres lieux d'archivages, on pourrait avoir une vision meilleure de l'usage des khipus par les Incas et, donc, lever un peu le secret de leur histoire ...

David Kahn

Journaliste, écrivain et scénariste, David Kahn est surtout connu comme l'historien de la cryptologie, la science des codes secrets.

Il a obtenu un doctorat de l'Université d'Oxford en 1974. En plus de nombreux livres, il a publié des articles sur les codes et la cryptographie dans divers journaux et magazines, allant du New York Times à Playboy, du Journal of Strategic Studies à l'Encyclopedia Americana.

David Kahn a donné des cours sur le renseignement politique et stratégique moderne à Yale et à Columbia et il a enseigné le journalisme à New York University.

David Kahn a passé deux ans à Paris en tant que rédacteur de l'International Herald Tribune. Au cours de ce séjour, il a écrit une bonne partie de son fameux livre «The Codebreakers», qui a été sélectionné en 1968 comme finaliste pour le prix Pulitzer.

Ce livre a passionné nombre de ses lecteurs, et il est à l'origine de la vocation de certains des meilleurs chercheurs en cryptologie actuels. Il a été traduit et publié, en totalité ou en partie, en français, italien, polonais, serbo-croate et arabe. Une nouvelle édition augmentée a paru en 1995, et une autre est en préparation.

L'exposé

«La Victoire de l'Intelligence»

Les codes secrets et la cryptographie ont été utilisés depuis longtemps surtout par les gouvernements et les militaires. Dans beaucoup de pays, cela a même été considéré comme de leur usage exclusif, ne permettant pas au citoyen de les utiliser pour communiquer.

Pourtant, il n'en a pas toujours été ainsi. Napoléon, par exemple, a considéré en 1814 que les codes secrets étaient inutiles, se trouvant ainsi sans moyen de communications sûr lors de la bataille de Waterloo. La leçon ne fut pas bien tirée et la même situation se reproduisit en 1870. Puis vint la télégraphie sans fil avec sa très grande facilité d'interception.

L'exposé montrera comment l'interception et l'analyse des messages chiffrés durant la guerre 14-18 ont convaincu les généraux que le renseignement, qu'ils ont regardé d'abord comme insignifiant et presque inutile, peut les aider à gagner des victoires.