

A.R.C.S.I.

Association des Réservistes du Chiffre et de la Sécurité de l'Information



Vendredi 10 octobre 2008

(Salle des congrès du MEEDDAD – 20 Av. de Ségur – 75007 PARIS)

L'ASSOCIATION des RESERVISTES du CHIFFRE et de la SECURITE de l'INFORMATION

organise son **5^{ème} colloque** sur :

« La cryptologie d'hier et d'aujourd'hui »

Son président, le Général (2s) Jean-Louis DESVIGNES,
le Conseil d'Administration et tous les membres
célébreront à cette occasion le **80^{ème} anniversaire** de
l'ARCSI

Frais de participation : 20€ (à régler à l'accueil)
Gratuit pour les étudiants.

Inscription en ligne : <https://arcsi.fr/colloque-10-10-08/>

Pour évoquer la cryptologie au cours des siècles, l'Association des Réservistes du Chiffre et de la Sécurité de l'Information vous propose de vous réunir sur le thème de la :

« CRYPTOLOGIE D'HIER ET D'AUJOURD'HUI »

- 08h15 : Accueil
- 09h00 : **Allocution d'ouverture** du Président de l'ARCSI Général (2s) Jean-Louis DESVIGNES,
- 09h30 : **M. Pascal GRISET – Agrégé des Universités et Docteur en histoire.**

Professeur à la Sorbonne Paris-IV. Spécialiste de l'histoire économique et technique de l'information. Exposé : Codes et cryptage au cœur de l'histoire des télécommunications : une perspective de longue durée. Le cryptage est un élément essentiel de l'histoire des Transmissions. A en croire les médias, cette dimension est également devenue récemment un point clef de l'évolution des échanges

commerciaux, voire personnels d'information La sécurité des réseaux et la confidentialité des échanges apparaissent ainsi comme un enjeu majeur en ce début de siècle. Il s'agira dans cette communication d'articuler enjeux militaires et civils pour souligner que cette facette du monde de l'information et de la communication présente est primordiale depuis bien plus longtemps. En effet, depuis les tous premiers développements des réseaux d'échange d'information, le codage et le cryptage sont un enjeu clef tant pour les utilisateurs que pour les concepteurs et opérateurs de systèmes de télécommunications. Quelques jalons essentiels associés à des exemples plus spécifiques permettront donc de placer ces questions dans le temps long, de l'histoire des premiers grands réseaux du XIX^e siècle jusqu'aux problèmes plus contemporains.

- 10h15 : **M. J.P. FABREGUETTES – Membre de l'ARCSI.**

Cdt de la Cie d'instruction de régulateurs chiffreurs au 28 RGT lors de sa création ;

Chef du cours chiffre à l'école de Montargis (EAT) ;

Officier du chiffre du 2 CA -FFA. Diplôme du BECS ;

Chef du bureau chiffre (devenu sous mon impulsion le bureau SECOM-GUEREELEC) de 80 à 84 et membre de la commission interministérielle du chiffre : sous-com crypto ;

Vice-président de la Croix-Rouge de Strasbourg.

Exposé :

De la fin de la guerre jusqu'en 1956 le chiffre vivote. C'est le hors-circuit. 1956 : Suez et nos découvertes. Le concours OTAN. Le chiffre revit La SECOM et son annexion par le chiffre. Le RITA et la fin des ateliers par le chiffrement de jonctions.

- 10H55 : P ause
- 11h20 : M. Patrick HEBRARD (Des hiéroglyphes à Enigma)
- 12h00 : M. David NACCACHE – Université Paris II (Impact sociétal de la crypto)
- 12h45 : **Mme Sophie de LASTOURS - Membre de l'ARCSI.**

Docteur en histoire militaire, DESS de droit de la défense ; Ancienne auditrice du CHEAR, de l'IHEDN et de l'INHES. Elle est directrice de la collection histoire de la défense chez l'Harmattan. Elle a publié plusieurs ouvrages et écrit des scénarios sur l'histoire du renseignement pour une maison de production.

Exposé : " Le chiffre et les femmes"

"John Edgar Hoover qui fut presque cinquante ans à la tête du FBI nourrissait une méfiance certaine vis à vis des femmes, spécialement dans l'exercice du renseignement. En nous basant sur quelques exemples touchant au domaine de la cryptologie, nous pourrions étayer ou contester ce jugement et conclure que curieusement la misogynie n'est pas étrangère à la cryptologie."

- 13H00 : ***D éjeuner au restaurant administratif du Ministère de l'Ecologie***
- 14H30 : **M. David POINTCHEVAL – Directeur de recherche au CNRS.**

Responsable de l'équipe de cryptographie du laboratoire d'informatique de l'Ecole Normale Supérieure, commune avec le CNRS et l'INRIA. Ses travaux de recherche portent sur la cryptographie asymétrique et la cryptographie à base de mots de passe avec, comme objectif essentiel, la sécurité prouvée dont il fut l'un des initiateurs.

Exposé : Les preuves de sécurité en cryptographie.

Les résultats sur la sécurité prouvée des protocoles cryptographiques concrets sont très récents. En effet, la formalisation théorique des problèmes de sécurité a moins de 30 ans, avec l'avènement de la cryptographie asymétrique. Une recherche foisonnante a trouvé ses racines au sein de la théorie de la complexité, qui a modélisé la sécurité, mais avec des analyses asymptotiques. Ces dernières années ont vu se développer la notion de « sécurité prouvée », qui s'attache à étudier la sécurité de schémas concrets et efficaces, tout en permettant une interprétation effective quant à la taille des paramètres à utiliser en fonction du niveau de sécurité souhaité.

- 15H15 : **M. Benoît CHEVALIER-MAMES - Expert du laboratoire de cryptologie - DCSSI.**

Diplômé de Supélec et docteur de l'Université de Paris VII dans le domaine de la cryptographie à clé publique. Ses travaux portent principalement sur la conception de schémas cryptographiques et la sécurité prouvée.

Exposé :

A.R.C.S.I.

Association des Réservistes du Chiffre et de la Sécurité de l'Information



Présentation des avancées récentes dans le domaine de la cryptologie. Révélations sur certains domaines dans lesquels la recherche publique ou privée pourrait conduire à des changements importants.

- 16H00 : **Pause**
- 16H30 : **M. Sébastien LEONNET – Administrateur Principal au Secrétariat Général du Conseil de l'Union Européenne.**

Ancien Officier supérieur de l'Armée de l'Air française. Diplômé de l'Enseignement Militaire Supérieur Scientifique et Technique ;
Chef de l'Unité « Sécurité des Systèmes d'Information et de Communication Sensibles » au Secrétariat Général de l'UE.

Exposé : SSI et cryptologie : Les enjeux du Conseil de l'Union Européenne.

La nouvelle donne Européenne en matière SSI (domaine PESZC/PESD) ; Nos besoins, nos systèmes, nos challenges, nos difficultés ; La problématique cryptologique à 27 (+ les organisations internationales) pour les besoins de chiffrement des communications ; La problématique cryptologique pour les besoins d'authentification, de contrôle d'accès, de signature et de chiffrement local de l'information ; Nos procédures de sélection de matériels cryptologiques.

- 17H15 : **Clôture : Patrick PAILLOUX – Directeur de la Direction Centrale de la Sécurité des Systèmes d'Information.**

Le livre blanc sur la défense et la sécurité nationale retient le risque d'une attaque informatique contre les infrastructures nationales comme une des menaces majeures des 15 prochaines années. Le recours accru à des produits et des réseaux de sécurité de haut niveau fait parti des mesures à prendre afin de contrer ce risque, au même titre que la détection précoce des attaques et la mise en place de réservoir de compétence au profit des administrations. Pour mener à bien cette stratégie, le gouvernement a décidé la création d'une agence nationale qui sera chargée de la sécurité des systèmes d'information (ANSSI).

- 17H45 **FIN**