12es Rencontres de l'ARCSI

Jeudi 8 novembre 2018
BNF - Avenue de France - 75013 Paris

1928 - 2018
90e anniversaire

La cryptologie, de la Grande Guerre au post-quantique

Les conférences et tables rondes s'attacheront à retracer les grandes évolutions de la cryptologie, science du secret, au cours du siècle passé, en soulignant les capacités de la France par rapport aux autres nations et en révélant les événements marquants de l'Histoire, dont le lien avec la cryptologie est souvent méconnu. Elles s'achèveront en évoquant les problématiques d'aujourd'hui et de demain.

Les hommes on le sait, sont particulièrement inventifs lorsqu'il s'agit de s'entre-tuer. Les guerres sont en effet à l'origine de multiples progrès techniques dont heureusement certains trouvent une utilité une fois la paix retrouvée. La Grande Guerre, dont nous célébrons le centenaire de la fin, n'a pas échappé à la règle : dans le domaine de compétence de l'ARCSI, la cryptographie et certains moyens de télécommunication qu'elle est venue renforcer ont fait des bonds de géant. C'est ce que notre prochain colloque se propose de montrer.

Celui-ci est en effet pour l'ARCSI l'occasion de célébrer un double anniversaire : le centenaire de la victoire de 1918 à laquelle, on le sait peu, les cryptologues ont pris une part déterminante, et les 90 ans de notre association constituée en 1928 précisément par ces héros de l'ombre, soit 10 ans après leurs succès et alors que la nécessaire discrétion qui avait entouré leurs exploits avait déjà cédé la place à l'oubli… D'autres pays et surtout d'autres responsables politiques avaient su reconnaître ce qu'ils devaient à ce qui était en train de devenir la science du secret. Ils surent, quand la terre trembla de nouveau, lui donner rapidement les moyens leur permettant de vaincre. Ainsi fit Churchill à *Bletchley Park*. D'autres sauront s'en servir pour assurer leur domination sur la planète comme Snowden a pu le révéler.

Mais c'est aussi durant cette guerre de 1914-1918, comme cela sera présenté, que les grands principes régissant les systèmes cryptographiques énoncés par Kerckhoffs ont été vérifiés tandis qu'était inventé par Vernam le procédé du « masque jetable » ou des « clefs une fois », qu'apparurent les premières machines ENIGMA ou que fut mis en application le « saut de fréquence » inventé par Nicolas Tesla.

Et c'est parce que cette période peut être considérée comme le point de départ de la cryptographie moderne que ce colloque se propose également de passer en revue les évolutions que sont l'industrialisation de la cryptanalyse qui va accélérer le développement de l'informatique, la compression des signaux vocaux utilisée dans le téléphone sécurisé de Roosevelt intégrée dans tous nos joujoux d'aujourd'hui, la véritable histoire de l'invention des systèmes à clé publique, l'engouement actuel pour les « blockchains » ou encore la crainte que suscitent aujourd'hui les performances de nouveaux algorithmes de factorisation sans parler des très attendus et redoutés ordinateurs quantiques.

Tout cela sera abordé au cours de ce colloque exceptionnel par des experts de très grand talent. Avec une envie commune pour les intervenants : sortir des sentiers battus.

Venez nombreux, l'ARCSI sera heureuse de partager avec vous cette journée mêlant histoire et technologie du futur.

Jean-Louis Desvignes

08 h 30 ***Accueil***

09 h 00 Général (2s) Jean-Louis Desvignes[A], *Président de l'ARCSI*
M^me^ Isabelle le Masne de Chermont, *Directrice du département des Manuscrits (BNF)*
• Introduction

09 h 20 P^r^ Olivier Forcade, *Professeur à la Faculté des Lettres (Sorbonne Université)*
• Le contexte des télécommunications civiles et militaires au début du XX^e^ siècle et de la Grande Guerre
Par rapport à l'acheminement des messages, accélération des communications grâce aux réseaux filaires (câbles sous-marins notamment), mobilité des moyens grâce à la radio, mais vulnérabilité physique des réseaux filaires et indiscrétion des émissions radio nécessitant des moyens cryptologiques ; problème : délais des opérations de chiffrement encore manuels.

10 h 00 M. Philippe Guillot[A], *Maître de Conférences (Université Paris 8 Vincennes Saint-Denis)*
• Les grands succès et échecs de la cryptologie à l'aube du XX^e^ siècle
La guerre franco-prussienne de 1870 a mis en évidence la faiblesse que constituait l'absence d'un système de communications fiable et discret entre Paris et les généraux de Province.
La défaite a conduit à une réaction qui, sous l'impulsion des travaux d'Auguste Kerckhkoffs, a mené la France à une position dominante en matière de cryptologie.
Les services de renseignements et les bureaux du chiffre des différentes armées ont eu une importance notable sur le déroulement de la première guerre mondiale et des conflits qui ont suivi. Trois épisodes typiques seront présentés : le télégramme Zimmermann, le radiogramme de la victoire et le miracle de la Vistule. Dans chacun de ces cas, le décryptement des dépêches chiffrées a été déterminant.

10 h 40 ***Pause***

11 h 00 P^r^ Jean-Jacques Quisquater[A], *Cryptologue, Professeur émérite (Université catholique de Louvain), Commissaire de l'exposition "Top secret !" au Mondaneum (Mons, 10 octobre 2017 - 20 mai 2018)*
• Du chiffre manuel à la mécanisation
Purement manuelle au départ (le code de César se calculait à la main), la cryptographie le restera longtemps sauf à considérer dans la scytale ou bien plus tard dans les disques de Jefferson un début de mécanisation…
Les mots-clés, tables ou dictionnaires resteront durant des siècles les seuls auxiliaires du cryptologue.
La mécanisation du calcul (Schickard, Pascal, Leibniz…) n'entraîna que peu de réalisations pour la cryptographie si ce n'est des exceptions (Leibniz, Babbage…) sans suite.
La Grande Guerre au contraire fut l'occasion de deux inventions majeures : la machine qui deviendra la célèbre ENIGMA et le chiffre de Vernam-Mauborgne. Leurs histoires fort étonnantes sont révélées dans des publications récentes. Suivit de peu la mécanique quantique (1924, Max Born) mais c'est une autre histoire…

11 h 45 Table ronde animée par M. Hervé Lehning[A], *Écrivain et journaliste scientifique*
Intervenants : Olivier Forcade, Philippe Guillot[A], Jean-Jacques Quisquater[A]
• De l'ingénieur au mathématicien
La Grande Guerre fut un temps de contrastes entre des transmissions rapides et des chiffrements manuels laborieux qui les ralentissaient. De même, l'organisation embryonnaire de l'exploitation des renseignements, qu'ils viennent du décryptement ou d'ailleurs, freina souvent l'efficacité du dispositif. Ces échecs ont-ils appelé les évolutions postérieures ?

12 h 30 ***Cocktail déjeunatoire***

L'inventeur et collectionneur américain Jon Paul[A] présentera durant les pauses, dans l'espace Partenaires, une reconstitution du quantificateur du système SIGSALY ainsi qu'un micro simulateur d'ENIGMA.

[A] *Membre de l'ARCSI*
Questions/réponses possibles après chaque intervention

14 h 00 M^me Marie-José Durand-Richard [A], *Maître de Conférences honoraire (Université Paris 8 Vincennes Saint-Denis), Chercheuse associée au laboratoire SPHERE (UMR 7219 CNRS-Université Paris Diderot)*

• La cryptanalyse dans la Seconde Guerre mondiale et son impact sur la naissance de l'informatique

L'histoire de la cryptologie pendant la Seconde Guerre mondiale se réduit souvent à la seule contribution d'Alan Turing (1912-1954) au décryptement d'ENIGMA. Pourtant, une équipe de mathématiciens et ingénieurs polonais décryptait cette machine dès 1932, cyclomètre et *Bombas* permettant de surmonter les complications croissantes du chiffrement allemand. L'installation de la *Governement Code and Cypher School* à *Bletchley Park* en août 1939 marque un changement radical d'échelle. Les moyens manuels, logiques et techniques sont coordonnés en une véritable "manufacture" mobilisant jusqu'à 12 000 personnes. Parallèlement aux décryptements manuels, l'ENIGMA navale sera décryptée grâce aux Bombes de Turing, et la machine de Lorentz grâce aux *Colossus* — premiers calculateurs électroniques — de Max Newman (1897-1984), tandis que Turing contribuera à l'élaboration de systèmes de chiffrement de la parole aux États-Unis (*Sigsaly*) et en Grande Bretagne (*Delilah*).

14 h 40 M. Jean-Luc Moliner, *Directeur de la sécurité (Groupe Orange)*

• Les deux faces de la cryptologie de masse

Malgré les brillantes inventions académiques dans la cryptologie depuis les années soixante-dix, la standardisation de solutions élégantes et la généralisation de leur utilisation, l'usage de la cryptologie demeure un défi quotidien pour les particuliers et les entreprises sous le regard toujours soupçonneux des États. Quel est le niveau réel d'utilisation de ces outils, leur solidité et leur résistance face aux attaques de tous bords ? La pérennité de la numérisation, l'intégrité de nos vies privées et la souveraineté des nations sont dépendantes des réponses que nous y apportons.

15 h 15 ***Pause***

15 h 45 M. Philippe Duluc, *Directeur technique Big Data & Sécurité (ATOS)*

P^r Jean-Jacques Quisquater [A]

• L'avenir plus ou moins proche : quantique, post-quantique et "cataCRYPT"

On fête cette année le centenaire de la naissance de Richard Feynman qui proposa en 1982 d'utiliser les propriétés quantiques pour accélérer les calculs (simulations ou informatiques). La théorie très alléchante conduit à imaginer des accélérations fabuleuses. Shor publie en 1995 un algorithme quantique efficace pour la factorisation (RSA) et le calcul du log discret (courbes elliptiques) tandis que Grover découvre en 1996 les méthodes quantiques pour accélérer les recherches exhaustives mettant alors en danger la cryptographie symétrique et les fonctions de hash.
Les performances de ces ordinateurs quantiques conduisent la NSA à reconsidérer la sécurité des standards cryptographiques (août 2015) et le NIST publie très vite un appel à propositions pour passer sans encombre à l'ère post-quantique dont les enjeux sont considérables.

Les progrès de l'algorithmique, en général, des ordinateurs classiques associés aux ordinateurs quantiques peuvent conduire à un désastre général : une véritable "cataCRYPT", concept créé lors des rencontres de l'ARCSI, en 2010.
S'ajoutent toutes les attaques physiques locales ou distantes qui ne peuvent qu'affaiblir les réalisations techniques (sans compter les bogues !). Et évidemment l'introduction de *backdoors* pourrait encore aggraver le processus.
La cryptographie quantique peut-elle alors constituer un recours ?

16 h 40 Table ronde animée par le P^r Sébastien-Yves Laurent, *Professeur à la Faculté de Droit et de Science Politique (Université de Bordeaux), Commissaire de l'exposition "Le secret de l'État" aux Archives nationales (Paris, 4 novembre 2015 - 28 février 2016)*
Intervenants : ANSSI, CNIL, Jean-Louis Desvignes [A]

• Le dilemme sécurité/liberté

La problématique éternelle pour les gouvernements est d'assurer la sécurité de nos concitoyens en développant les capacités de renseignement tout en garantissant les libertés individuelles. Comment tordre le cou à la fausse bonne idée des backdoors et autres façons d'affaiblir la robustesse des moyens de protection ? A fortiori interdire les moyens de chiffrement dont rêvent encore certains responsables politiques et policiers.

17 h 30 ***Fin des Rencontres***

L'inventeur et collectionneur américain Jon Paul [A] présentera durant les pauses, dans l'espace Partenaires, une reconstitution du quantificateur du système SIGSALY ainsi qu'un micro simulateur d'ENIGMA.

[A] *Membre de l'ARCSI*
Questions/réponses possibles après chaque intervention

Partenaires de l'ARCSI

Durant toute cette journée, pensez à visiter les stands de nos partenaires