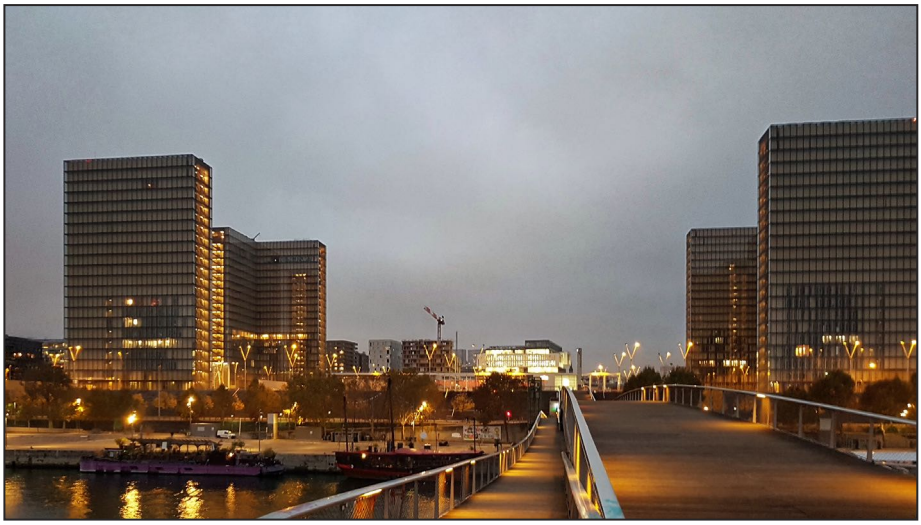
12es Rencontres de l'ARCSI
Allocution d'ouverture

Jean-Louis Desvignes



La Bibliothèque nationale de France

Bonjour à toutes et à tous. Je me réjouis de vous voir aussi nombreux pour participer à ces 12es Rencontres de l'ARCSI qui revêtent comme vous avez pu le voir un caractère doublement solennel et exceptionnel puisque nous célébrons en même temps, pardonnez-moi cette expression jupitérienne, mais qui ici n'oppose pas, au contraire, le centenaire de la victoire de 1918 et les 90 ans de notre association. Il se trouve en effet que ce sont les vainqueurs de la lutte contre le chiffre allemand, dont nous sommes les héritiers qui ont créé une amicale des officiers de réserve servant dans cette spécialité pour que ne soit pas complètement oublié ce que la victoire devait à ces hommes de l'ombre qui ont contribué à faire basculer l'histoire. C'est d'ailleurs pourquoi notre journée comportera une partie historique mais dans laquelle le côté scientifique et technique ne sera pas absent bien au contraire et une partie sans doute plus technique au fur et à mesure que l'on avancera vers notre époque mais qui elle ne sera pas dénuée d'aspects historiques et sociologiques qui font le charme de cette science du secret.

Mais avant toute chose je voudrais m'adresser aux membres de l'ARCSI pour les informer, s'ils n'ont pas regardé leur messagerie depuis hier soir, d'un évènement qui nous touche cruellement : notre secrétaire général Jean-Marc Laloy qui était la cheville ouvrière de notre association nous a quittés. Depuis des années il se dépensait sans comp-

ter pour organiser nos manifestations, il n'hésitait pas à relancer les uns et les autres pour les encourager à participer à nos évènements. Jean-Marc notre collègue notre ami, notre complice nous a quittés hier matin à l'issue d'une longue maladie. Vous aviez certainement remarqué sa disparition sur le réseau et pour certains un changement physique lors de ses dernières apparitions. Le mal était profond et malgré une résistance hors du commun Jean-Marc a fini par céder. C'est une immense perte pour tous, pour sa famille d'abord, pour ses amis et pour nous tous membres de l'ARCSI. Pour ceux qui le souhaitent il sera possible de le voir une dernière fois demain entre 10 heures et 11 h 30 à la salle funéraire de l'hôpital Charles Foix à Ivry-sur-Seine. Il sera ensuite ramené dans son cher Périgord dans son fief de la Coquille.

Son épouse me disait hier soir qu'il suivrait certainement de là où il sera notre journée pour laquelle il se faisait encore du souci il y a quelques semaines seulement. Je peux témoigner que jusqu'au bout il aura pensé à l'ARCSI qui était sa vie, et à s'intéresser au montage de notre colloque auquel il était frustré de ne pouvoir participer si ce n'est à travers les objets qu'il a bien voulu mettre à notre disposition pour une mini-exposition que vous pourrez voir dans l'espace partenaires. D'ailleurs à présent je sens qu'il s'impatiente et veut voir d'où il est, comment nous nous débrouillons sans lui.

La meilleure façon de lui rendre hommage est de réussir ce colloque.

Le magnifique amphithéâtre de la Bibliothèque nationale de France

En premier lieu puisque nous sommes dans cet amphithéâtre magnifique je voudrais adresser mes très chaleureux remerciements à la Bibliothèque nationale de France en la personne de Madame Isabelle le Masnes de Chermont Directrice du département des manuscrits et représentant Madame Sylviane Tarsot-Gillery Directrice générale de la BNF. Pour célébrer les 90 ans de notre association nous avons en effet pensé à changer de cadre et avons opté pour cet écrin prestigieux. La BNF nous a accordé des conditions avantageuses en montrant de surcroît un intérêt pour nos activités car des travaux de cryptologie ont commencé à la BNF sous la houlette d'Isabelle de Chermont. Il me sem-

ble d'ailleurs que ces travaux pourraient contribuer à exaucer les vœux de l'un de nos membres Daniel Tant ancien archiviste de Reims, qui rêve de pouvoir accéder au contenu de multiples documents dormant au fond d'armoires nationales et régionales faute de pouvoir être mis au clair les codes ayant souvent disparu. Je cède la parole à Isabelle de Chermont.

Sachez que j'ai proposé à votre directrice générale de vous offrir une tribune plus substantielle lors de l'une de nos prochaines manifestations.

Je veux également adresser mes plus vifs remerciements à nos généreux et fidèles partenaires dont vous pouvez apercevoir les Logos sur les planches projetées. THALES, ORANGE, CAP TRONIC, THEGREENBOW, G-ECHO, HS 2, CITALID, QUARKSLAB, et toujours avec le partenariat des Magazines GLOBAL SECURITY MAG et MAGSECURS.

C'est grâce à ces partenaires que nous pouvons vous recevoir dignement et être sûr que vous ne tomberez pas d'inanition. Vous pourrez en effet profiter des pauses pour reprendre quelques forces et pour aller visiter les stands de ces partenaires. Vous pourrez également voir l'exposition de l'ARCSI comprenant la collection de Jean-Marc ainsi que l'atelier de Jon Paul. À l'heure du déjeuner un buffet sera dressé. Comme chaque année nous avons fait appel à l'école de restauration Ecofih. J'espère que vous en serez satisfaits.

À présent venons-en au colloque qui a subi deux ajustements de dernière heure :

Notre premier intervenant le professeur Olivier Forcade a dû s'absenter inopinément pour un grave évènement familial. Cependant quand il m'a appelé hier pour me prévenir celui-ci a immédiatement suggéré pour le remplacer de faire appel à sa brillantissime disciple Agathe Couderc bien connue désormais des membres de l'ARCSI, que je présenterai tout à l'heure, ce que j'ai bien entendu accepté.

Deuxième changement : la table ronde finale ne permettra pas d'entendre le point de vue de l'ANSSI, celle-ci, en raison de sa charge de travail n'a pas été en mesure d'honorer notre rendez-vous traditionnel. À moins que cet organisme de 600 personnes n'ait pas trouvé de candidat pour affronter le redoutable commissaire de la CNIL… Mais nous ne perdons pas au change, loin de là, puisque c'est Jean-Luc Moliner une pointure avérée et déjà entendue dans un précédent colloque qui a accepté de revenir relever le défi alors qu'il nous aura déjà gratifiés d'un exposé très alléchant dans l'après-midi.

Je suis certain que ces deux changements gérés dans l'urgence ne perturberont en rien le bon déroulement ni l'harmonie de notre programme.

Après l'ouverture du feu par Agathe Couderc, c'est Philippe Guillot de Paris 8 qui poursuivra l'évocation historique en nous faisant le point sur l'état de l'art en cryptographie à l'aube du XX^{e} siècle, tandis que Jean-Jacques Quisquater (professeur émérite de l'université catholique de Louvain) qu'il est inutile de présenter davantage nous réservera quelques-unes de ses dernières trouvailles sur cette période charnière pour la cryptographie. La matinée se terminera par une table ronde introduite par Hervé Lehning désormais auteur à succès après son best-seller « toutes les mathématiques du monde ». Cette table ronde permettra des échanges entre les intervenants précédents et avec la salle.

Après le repas nous reprendrons le cours de l'histoire avec Marie-José Durand-Richard qui nous montrera comment la lutte contre la machine ENIGMA désormais vulgarisée

grâce au film « *Imitation game* » et celle de Lorentz a véritablement industrialisé le travail de cryptanalyse et offert à l'informatique l'occasion de démontrer son efficacité et ouvrir de fantastiques perspectives. Marie-José ne manquera certainement pas l'occasion d'évoquer le pèlerinage de l'ARCSI à Bletchley Parc en juin dernier. Comme elle évoquera aussi les systèmes de cryptophonie de la deuxième guerre mondiale, je vous signale que dans l'« espace partenaires », là où est exposée la collection de Jean-Marc, vous pouvez bénéficier d'explications supplémentaires fournies par notre ami inventeur et collectionneur Jon Paul sur le système SIGSALY dont il a reconstitué le cœur en utilisant des composants d'époque ainsi qu'à des démonstrations de son nouveau simulateur d'ENIGMA dont vous pouvez même passer commande ! Entre nous, j'ignore totalement si ce véritable équipement cryptographique qui n'est pas à la portée du premier cryptanalyste venu est considéré comme un objet pédagogique ou une redoutable arme de guerre qui devrait être soumise à autorisation avant d'être mise sur le marché… Profitez donc de l'incertitude actuelle si vous avez quelques secrets à échanger !

Suivra ensuite un morceau de bravoure avec une revue très complète du développement de la cryptologie moderne par Jean-Luc Moliner dont le parcours extrêmement riche et varié tant au service de l'État qu'au service de l'entreprise où il exerce ses talents lui permet d'aborder tous les aspects de celle-ci.

Puis c'est un duo de choc composé de Philippe Duluc au parcours également très riche au sein du ministère de la Défense puis de l'entreprise BULL désormais ATOS, et Jean-Jacques Quisquater qui reviendra sur un sujet que je lui avais demandé d'examiner lors de précédentes rencontres et qu'il a érigé en scénario catastrophe au nom déposé : CATACRYPT.

La dernière table ronde sera animée par le professeur Sébastien Yves Laurent de l'université de Bordeaux. Celui-ci s'est beaucoup intéressé aux questions de renseignement et nous avons eu l'occasion de collaborer avec lui alors qu'il était commissaire de l'exposition des Archives nationales sur le Secret de l'État en 2015-2016. Cette exposition a considérablement boosté notre notoriété grâce à notre efficacité dans l'aide au montage de l'exposition et la programmation des conférences largement assurées par des membres de l'ARCSI. Dans cette table ronde nous débattrons essentiellement de la liberté de chiffrer, de l'utilisation des back-doors et d'autres façons de contourner légalement ou non les procédés cryptologiques avec le commissaire de la CNIL François Pellegrini, Jean-Luc Moliner déjà présenté et moi-même.

Les questions peuvent être posées à la fin de chaque exposé et lors des tables rondes à l'invitation de l'intervenant ou de l'animateur. Je rappelle comme le fait souvent notre ami Gérard Peliks qu'une question se compose d'une phrase aussi concise que possible suivie d'un point d'interrogation.

J'ajoute que se présenter brièvement avant de poser sa question attire parfois une réponse mieux ciblée.

Je vous souhaite un très agréable et très enrichissant colloque.

12es Rencontres de l'ARCSI
Compte rendu de la journée

Gérard Peliks

Jean-Marc Laloy nous a quittés la veille après un long combat contre une maladie qui ne l'avait pas empêché de contribuer à cet évènement et d'avoir été d'une efficacité reconnue par tous comme secrétaire général de l'ARCSI. Cet évènement est dédié à sa mémoire et une minute de silence tenue par les ARCSIstes, et leurs amis présents dans l'auditorium, lui a rendu hommage. Comme le souligne Jean-Louis Desvignes, président de l'ARCSI : « *d'en haut Jean-Marc doit noter toutes les imperfections que connaîtra cette journée* ». Et en bas, l'exposition montrait des frises sur l'histoire de la cryptologie, le quantificateur de la machine SIGSALY, élaboré par Jon D. Paul, la C-36, des microsimulateurs de machines Enigma numériques également élaborés par Jon D. Paul et des machines à chiffrer tirées de la collection personnelle de Jean-Marc.

Un public très attentif !

Dès l'aube à la Bibliothèque nationale de France, des membres du bureau de l'ARCSI étaient présents pour aider à monter l'exposition, et les frises murales sur l'histoire de la cryptologie, et pour organiser l'accueil des participants. Soulignons la gentillesse et l'efficacité du personnel de la Bibliothèque nationale de France qui nous a aidés à faire de cet évènement un grand succès.

Le général (2S) Jean-Louis Desvignes, président de l'ARCSI, ouvre cet évènement, dans le magnifique auditorium de 250 places de la BnF, en remerciant les participants d'être venus si nombreux. Il remercie les intervenants et nos sponsors. Il rappelle le rôle déterminant des cryptanalystes dans la victoire de 1918 dont on célèbre cette année le 100e anniversaire. Ce colloque marque aussi le 90e anniversaire de l'ARCSI. Jean-Louis Desvignes accueille Isabelle le Masne de Chermont, directrice du département des Manuscrits de la BnF.

Isabelle le Masne de Chermont

Isabelle le Masne de Chermont nous fait part de sa satisfaction de voir ce colloque organisé à la Bibliothèque nationale de France. La BnF possède des manuscrits précieux, certains remontent aux XVIe et XVIIe siècles, sur les cryptologues, les cryptanalystes et sur leurs œuvres. Elle cite des tableaux et dictionnaires de chiffrement, qui sont à la disposition des chercheurs pour consultation. Les documents sur la cryptologie sont de bons témoins des tensions dans l'histoire car, quand les tensions augmentent, le nombre de documents sur la cryptologie aussi. Elle souligne qu'il existe sûrement des pistes de collaboration entre la BnF et l'ARCSI. La BnF développe un programme de recherche sur l'histoire de la cryptologie et possède de nombreux manuscrits chiffrés, qui ne demandent qu'à être décryptés. Notre ami ARCSIste Hervé Lehning, qui a déjà mené des actions de décryptement à la Bibliothèque de Strasbourg, pourrait aider la BnF à mettre en clair certains manuscrits jusque-là non exploités car non compréhensibles.

Jean-Louis remet à Isabelle le Masne de Chermont, comme il le fera pour chaque intervenant, la médaille commémorative des 90 ans de l'ARCSI et un livre. Une fructueuse coopération entre la BnF et l'ARCSI semble être en bonne voie.

Agathe Couderc

Le Professeur Olivier Forcade de l'Université de la Sorbonne n'ayant pu se rendre au colloque, une de ses doctorantes, historienne du chiffre, Agathe Couderc, le remplace au pied levé pour traiter « **du contexte des télécommunications civiles et militaires au début du XXe siècle et de la Grande Guerre** ». Durant cette période, la France a été, d'après l'historien américain David Kahn, à la pointe de la technologie sur la cryptanalyse, pour des applications militaires mais aussi civiles. Au siècle précédent, durant la guerre de Crimée qui vit un affrontement opposant Français et Britanniques alliés contre les Russes, les communications constituèrent un facteur important de la victoire. Avant cette période de l'histoire, le télégraphe de Chappe a aussi joué un rôle important pour les transmissions de messages par sémaphores.

Dans la première décennie du vingtième siècle vint la TSF qui a donné un avantage aux Japonais dans les combats

qui les ont opposés aux Russes. Entre les deux grandes guerres, les câbles sous-marins qui relient les continents furent un enjeu stratégique. Les télécommunications ont fait évoluer les mentalités civiles et militaires pendant que le Renseignement technique faisait évoluer la cryptologie mais, à ses débuts, comme un moyen de contre-espionnage plutôt que d'espionnage. En 1916, les transmissions chiffrées furent largement utilisées dans un but offensif. La bataille de Verdun a marqué un tournant dans la première guerre mondiale avec l'exploitation intensive des télécommunications et du renseignement technique.

Alors que la Grande Bretagne contrôlait en 1900, plus de 70 % des câbles sous-marins, nouveaux moyens de télécommunication de l'époque, elle n'en contrôlait plus que 56 % en 1908. Ces câbles sous-marins étaient très coûteux et leur pause était complexe. L'utilisation des ondes électro magnétiques, qui permettaient de se passer de câbles, allait révolutionner les transmissions. Les travaux de Marconi ont rendu possible les transmissions « au-delà de l'horizon » et l'utilisation du Morse allait faciliter la vitesse des échanges. Dès le début du vingtième siècle la TSF est passée, en France, sous l'autorité civile des PTT. L'armée et la marine ont jugé que la radio télégraphie était un outil stratégique. En 1909 sous l'impulsion du général Gustave Ferrié, la Tour Eiffel et son antenne ont été utilisées comme poste de Réseau et de Commandement.

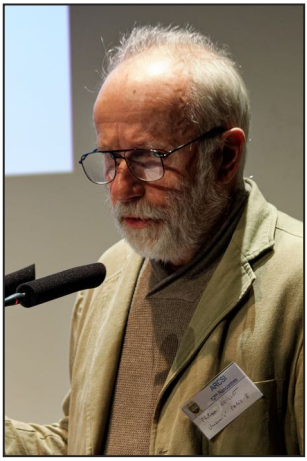
La Grande Guerre a fait croître l'importance de la TSF, qui fut interdite aux particuliers. En 1914 et 1915, le Renseignement technique et le 8e Régiment du Génie alignaient 2 000 combattants près des lignes de front pour capter les ondes électromagnétiques émises par les Allemands et décoder leurs transmissions. Ces messages restaient rares et souvent étaient émis en clair faute de temps pour les chiffrer ou les déchiffrer. La Radiotélégraphie fut abondamment utilisée par l'armée de terre et par la marine. Pour redonder l'antenne de la Tour Eiffel, deux autres antennes ont été déployées, une à Lyon et l'autre à Bordeaux. La Radiogoniométrie, par des dispositifs de triangulation a permis le repérage des postes émetteurs. En 1912 la Section du chiffre est créée et les renseignements militaires sont confiés au 2e Bureau.

À l'été 1918, le renseignement technique français a réussi à décrypter des messages indiquant, parmi cinq endroits possibles, Compiègne comme lieu à partir duquel les Allemands allaient lancer une offensive sur Paris. L'offensive allemande se brisa sur les défenses de l'armée française qui les attendait à cet endroit précis, et l'armée allemande fut refoulée vers la frontière. La cryptanalyse a ainsi grandement participé à la capitulation de l'Allemagne.

Philippe Guillot de l'Université de Paris 8 monte sur scène pour traiter « **Les grands succès et échecs de la cryptologie à l'aube du XXe siècle** ».

Le télégraphe a été l'initiateur de la cryptologie moderne. Chiffrer ralentissait les temps de transmission mais ne pas chiffrer conduisait à la défaite. Dès 1886, le Néerlandais Auguste Kerckhoffs énonçait ce qui allait devenir un des fondements de la cryptographie moderne : « le secret devait résider au niveau des clés de chiffrement et non au niveau du mécanisme ».

En 1917, Le décryptement du message de Zimmermann, ministre des Affaires étrangères de l'Empire allemand, qui incitait le Mexique a déclencher une guerre contre les États-Unis, avec l'appui de l'Allemagne qui projetait, en parallèle, une attaque à outrance par ses



Philippe Guillot

sous-marins pour couper l'approvisionnement de la Grande Bretagne, provoqua l'entrée en guerre des États-Unis aux côtés des alliés. Les câbles sous-marins autour de l'Allemagne étant sectionnés par les Britanniques, la seule voie de transmission qui restait aux Allemands passait par la Suède, pays neutre, en transitant par l'ambassade des États-Unis à Berlin qui ouvraient leurs moyens de communications pour faciliter les pourparlers de paix. Les Britanniques avaient capté et décrypté le message de Zimmermann mais ne pouvaient informer les États-Unis de son contenu pour deux raisons. La première est qu'ils ne voulaient pas avouer qu'ils avaient intercepté le message en espionnant les Américains et non les Allemands. La seconde raison est qu'ils ne voulaient pas dévoiler aux Allemands qu'ils connaissaient partiellement le code le plus moderne de leur diplomatie. Comme ce nouveau code n'avait pas eu le temps d'être délivré partout avant le début de la guerre, ils pensèrent que, peut-être, il n'avait pas été livré au Mexique. Ils demandèrent à leur espion sur place de le vérifier… et il trouva bien le message chiffré dans le vieux code dans les poubelles de la Western Union, message qu'ils produisirent. À la vue de ce message perfide, le président Wilson, jusque-là drapé dans sa neutralité, demanda au Congrès, le 2 avril 1917, d'accepter l'entrée en guerre des États-Unis contre l'Allemagne. En juin 1917, l'armée américaine débarquait à Saint Nazaire pour combattre aux côtés des Français et des Britanniques.

Le décryptement d'un télégramme en morse, de l'armée allemande, chiffré en ADFGVX en juin 1918, connu sous le nom du « radiogramme de la victoire » permit au capitaine George-Jean Painvin, du service français du chiffre, d'informer l'État-Major que les allemands allaient déclencher, de manière imminente, une offensive sur Paris, à partir de Noyon. L'offensive allemande fut un échec et l'armée allemande fut refoulée jusqu'à la frontière. Les alliés remportèrent la victoire dont nous fêtons le centenaire aujourd'hui. Philippe Guillot nous passe une petite vidéo montrant une des rares interviews de Painvin dans laquelle, bien après la première guerre mondiale, il explique, comment il a procédé pour décrypter le radiogramme de la victoire, chiffré par une substitution et une transposition.

Le traité de Versailles avait créé sur la frontière Est de la Pologne, la Biélorussie au nord et l'Ukraine au sud. Au début de l'année 1920, l'Union Soviétique déclencha une guerre contre la Pologne, précédée d'offensives sur Minsk et sur Kiev. En août 1920, Varsovie était pratiquement perdue. La prise de Varsovie par les Soviétiques était imminente. Les Polonais priaient pour que leur patrie soit sauvée, mais surtout, trois mathématiciens polonais avaient réussi à décrypter les messages qui indiquaient tous les secrets de l'offensive soviétique, et sauvèrent leur pays. Cette bataille de Varsovie est connue sous le vocable du « miracle de la Vistule ».

C'est maintenant l'heure de la pause. Les frises murales expliquant l'histoire de la cryptologie à travers les âges et les technologies du chiffrement symétrique et à clé publique, de la mécanique quantique et son utilisation dans la cryptologie, l'exposition des machines à chiffrer, en particulier celles tirées des affaires personnelles de Jean-Marc Laloy

L'espace des partenaires

Le stand de l'ARCSI

Les B-211, CX-52 et C-36 de Jean-Marc Laloy

Le quantificateur de la machine SIGSALY…

… présenté par Jon Paul

et la machine Sigsaly de chiffrement de la parole, reconstituée avec du matériel d'époque, ainsi que les microsimulateurs de diverses versions des machines Enigma de Jon D. Paul, sont très entourés. Les stands des sponsors, TheGreenbow, Captronic, H2S, G.Echo, HS2, Orange, et aussi Thales, IDECSi, Citalid et Quarkslab, attirent beaucoup de participants. Thé, café et viennoiserie sont proposés et nous revenons dans l'amphi pour la suite du colloque.

Jean-Jacques Quisquater

La parole est donnée au professeur Jean-Jacques Quisquater, de l'UCL Crypto group à Louvain-la-Neuve, en Belgique, sur le sujet « **Du chiffre manuel à la mécanisation** ».

Jean-Jacques Quisquater commence par nous révéler un scoop : On devrait fêter aussi cette année le centenaire de la machine Enigma car un brevet atteste qu'une machine similaire a vu le jour dès 1918, et même peut-être un peu avant. Après l'époque du chiffrement sur papier, la mécanisation de cette discipline expérimentale a relevé du bricolage, parfois intelligent mais du bricolage tout de même. Par contre la cryptologie mathématique repose, elle, sur des preuves. On pourrait parler déjà du début de la mécanisation avec la Scytale que les Grecs auraient utilisé durant les guerres qui les opposèrent aux Perses, mais aucun récit n'atteste que la scytale fut réellement utilisée pour faire passer des messages sensibles. Le disque de Jefferson utilisé durant la Guerre de Sécession, lui, a une existence avérée pour une utilisation en cryptographie.

Parmi les machines à chiffrer mécaniques, Jean-Jacques Quisquater cite le boulier et la Pascaline (1642). À la fin du XVII^{e} siècle (1693), Leibniz construit une machine à roues dentées avec des cylindres à encoches de différentes longueurs et un clavier, sorte de machine Enigma avant l'heure, mais sans rotors. En 1709, Johannis Poleni fabrique une multiplicatrice. Au début du XX^{e} siècle commence l'histoire de ce qui deviendra l'Enigma à rotors. Plusieurs brevets sont alors déposés : Aux USA en 1917 par Edward Hebern, en Allemagne en 1918 par Arthur Scherbius, aux Pays Bas en 1919 par Hugo Koch et encore en 1919 en Suède par Arvid Damm. Mais si des prototypes ont réellement existé, ils sont couverts par le secret militaire et seuls les brevets déposés par les personnes en droit de publier un brevet, attestent que ces inventeurs sont les pères de l'Enigma. Les Enigmas furent d'abord des machines civiles. En 1937, les Polonais ont réussi l'exploit de casser des messages chiffrés par cette machine.

La fin de la guerre voit aussi l'invention par Vernam de ce qui va devenir le masque jetable (*One-time pad*) qui est un chiffre de Vigenère où la clef est aussi longue que le message. Mauborgne remarquera qu'il fallait que la clef soit choisie aléatoirement et non réutilisée. Techniquement, message et clef étaient inscrits sur deux bandes aléatoires de 0 et de 1 qu'on additionnait sans retenue. Ce chiffrement présentait néanmoins des faiblesses et la génération de bandes aléatoires n'était pas non plus sans failles. Le célèbre téléphone rouge de la guerre froide, pour établir une liaison chiffrée entre Washington et Moscou, fut en fait d'abord un télex, puis un Fax et maintenant un vrai téléphone. Il devait chiffrer

avec une clé de même longueur que le message. Cette clé ne devait surtout pas être réutilisée pour chiffrer d'autres communications. Le chiffrement à clés publiques, puis l'utilisation de la physique quantique, avec Max Born et Richard Feynman, dont on fête aussi cette année son centième anniversaire, allaient révolutionner les méthodes de chiffrement du siècle passé et annoncer la cryptologie du XXIe siècle.

Jean-Jacques Quisquater termine son temps de parole en évoquant l'évènement Histo-Crypt qui se tiendra à Mons, en Belgique du 16 au 19 juin 2019.

Hervé Lehning

Une table ronde modérée par Hervé Lehning, écrivain et journaliste scientifique, prend place, avec tous les intervenants qui viennent de s'exprimer : Jean-Jacques Quisquater, Agathe Couderc et Philippe Guillot, pour débattre du thème « **de l'ingénieur au mathématicien** ».

Les mathématiques font partie intégrante de la cryptologie. Philippe Guillot parle des origines arabes, au XIIe siècle où la valeur numérale de chaque lettre était multipliée par une constante, pour produire le message chiffré. Vers 1920 la cryptologie devient algébrique, un peu plus tôt pour le décryptement, un peu plus tard pour le chiffrement.

Hervé Lehning conte l'histoire du jeune professeur de mathématique Antoine Rossignol et de son décryptement réussi, en 1626, par l'analyse fréquentielle et la méthode des mots probables, d'un message envoyé par les huguenots de Réalmont assiégés par les troupes du prince de Condé. Ce message était un appel au secours, vers l'extérieur, des habitants de la place forte, affamés, et à cours de munitions. Ils ne pouvaient plus combattre et allaient demander leur reddition, alors qu'ils faisaient croire que leur moral était bon et qu'ils pouvaient encore résister. Les assiégés ne purent ainsi compter sur une aide extérieure et se rendirent. La bataille fut gagnée grâce à la seule arme du Chiffre ! Hervé Lehning remarque que, même s'ils n'utilisaient pas de théorèmes particuliers comme le feront les Polonais puis Turing avec la machine Enigma, les grands décrypteurs furent souvent des mathématiciens, sans doute car ils ont l'habitude de reconnaître des structures cachées.

Pour Agathe Couderc, toutes les sciences se nourrissent les unes des autres, comme c'est le cas, par exemple, entre les mathématiques et la cryptologie. Les cryptanalystes de la Première Guerre Mondiale, comme Painvin, étaient des mathématiciens mais ils n'utilisaient pas forcément les mathématiques pour essayer de décrypter les messages chiffrés.

Jean-Jacques Quisquater constate que les mathématiques, en commençant par les statistiques, sont en effet entrées très tard dans les technologies de la cryptologie. Dans le chiffre de Vernam, un « ou exclusif » XOR entre le texte et une clé était utilisé pour convertir un texte en clair en un texte encodé. Mais si on réutilisait la même clé sur un autre texte, cela fragilisait le chiffrement. La méthode des mots probables permettait parfois de remettre en clair le message chiffré, mais là, à part le XOR qui effectuait une transformation « modulo 2 », les mathématiques n'intervenaient pas vraiment.

Hervé Lehning présente les travaux de Claude Shannon prouvant mathématiquement que le chiffre de Vernam avec bande aléatoire ne permettait pas de retrouver le message en clair, sans posséder la clé de chiffrement. Donc le chiffre de Vernam est mathématiquement sûr.

Il y a une différence entre un résultat prouvé dans une théorie, comme celui de Shannon, et une affirmation qui ne repose que sur l'expérience, comme celle du général Givierge sur les machines chiffrantes. Shannon, le mathématicien, ne s'est pas trompé, si toutefois la clef aléatoire n'est utilisée qu'une seule fois.

Face à la complexité du décryptement, induite par les nouvelles machines, la tâche des cryptanalystes semblait désormais insurmontable. Pourtant un peu avant la deuxième guerre mondiale, des cryptanalystes polonais, à qui on n'avait pas dit que c'était insurmontable… l'ont surmonté.

C'est maintenant l'heure du cocktail déjeunatoire.

L'équipe de l'École ECOFIH

Impeccable pour les hors-d'œuvre, les plats, les desserts et les boissons. Rien à reprocher au personnel qui nous servait. Tous les superlatifs peuvent de même traduire la satisfaction et l'intérêt des conférences et la compétence des intervenants du matin. Par contre il reste encore des points à améliorer, côté logistique du cocktail déjeunatoire (offert) aux participants par l'ARCSI. La disposition des plats sur les tables et la présence du personnel, par ailleurs très accueillant, ont causé la formation d'une longue file d'attente. Et il y avait aussi trop peu de tables où poser nos assiettes. Il était donc difficile, avec seulement deux mains, de manger, de boire et de discuter pour ceux qui restaient debout. Mais je ne parle pas pour moi qui ai été accueilli à la table d'un de nos sponsors TheGreenbow, par notre ami ARCSIste Jérôme Chappe, fondateur et président de cette so-

ciété. Je parle juste pour celles et ceux qui n'ont pas eu cette chance. La logistique du cocktail déjeunatoire pourra être améliorée dans un prochain colloque.

Marie-José Durand-Richard

Les présentations magistrales reprennent avec Marie-José Durand-Richard, Maître De Conférences honoraire à l'Université Paris 8 sur « **la cryptanalyse dans la 2e Guerre mondiale et son impact sur la naissance de l'informatique** ».

Entre les deux guerres mondiales, la France, qui avait été à la pointe de la cryptologie, a perdu en compétences. Lors de leur réarmement, les Allemands avaient adopté la machine Enigma pour leur marine en 1926, leur armée de terre en 1928 et leur armée de l'air en 1935. Les Britanniques, ont recruté une équipe de mathématiciens, en particulier Alan Turing, hébergés dans des « huts », chacune spécialisée dans une certaine fonction de décryptement, à *Bletchley Park*, dans le cadre du GC&CS. Ils ont élaboré les Bombes, machines électromécaniques qui simulaient, chacune, plusieurs Enigmas pour décrypter les messages chiffrés des Allemands. Ils ont construit également les Colossus, machines électroniques programmables, pour décrypter les messages chiffrés par les machines de Lorentz. Ces machines ont fait merveille et ont été un des instruments de la victoire. Vers la fin de la guerre, l'ensemble du personnel de *Bletchley Park* comptait plus de 12 000 personnes.

L'Enigma, machine de chiffrement/déchiffrement à piles, transportée dans une mallette, avait fait l'objet de dépôts de plusieurs brevets et les tentatives pour casser son code ont longtemps été infructueuses. Avec trois rotors en rotation, dont il fallait connaître lesquels étaient choisis parmi 5 rotors disponibles, leurs places respectives, leur initialisation, et le tableau de connexions dont il fallait connaître où étaient reliées les fiches, tout cela donnait un nombre immense de possibilités. Il était facile et rapide de chiffrer un message sensible par une machine Enigma quand on connaissait les combinaisons pour l'initialiser correctement, et pour le déchiffrer, mais sans ces combinaisons, même quand on possédait une machine Enigma, le décryptement des messages était en pratique impossible. De plus les circonstances des combats imposaient de décrypter les messages chiffrés par l'ennemi en quasi-temps réel. Pourtant, avec l'aide du service du chiffre de l'armée française (Gustave Bertrand et Rodolphe Lemoine), les Polonais, en particulier les mathématiciens Rejewski, Rozycki et Zygalski, avant la deuxième guerre mondiale, décryptaient déjà la machine Enigma dans les conditions de chiffrement d'avant la guerre. Ils utilisaient notamment la méthode de l'horloge, fondée sur l'indice de coïncidence de Friedmann, mais aussi des machines, le cyclomètre et la Bomba polonaise. Mais le code d'initialisation des machines Enigma ne cessait de se complexifier. Les Britanniques ont mis en place à *Bletchley Park* une véritable entreprise de décryptement, fondée sur une stricte division du travail, pour faire face à l'énorme quantité de messages chiffrés. Pour faire fonctionner les Bombes d'Alan Turing et de Gordon Welchman, et les Colossus de Max Newman, des méthodes ont été produites pour diminuer le nombre de possibilités à explorer, en exploitant certaines erreurs de chiffrement commises par les Allemands. Le décryptement de l'Enigma navale a nécessité, outre les Bombes, la saisie de livres de codes, obtenue lors

de la capture de bateaux allemands, par exemple à la bataille de Narwik en 1940, ou des Îles Lafoden en 1941, et ce jusqu'en 1942.

Marie-José Durand-Richard nous parle également du vaste projet Sigsaly des Bell Labs, aux États-Unis, pour la transmission numérique et chiffrée de la parole. Cette machine électronique, opérationnelle dès juillet 1943, utilise le système Vocoder, le chiffre de Vernam et la modulation d'impulsions codées. Une petite machine portable sécurisée de communication de la parole, la machine Delilah, a également été élaborée en Grande-Bretagne par Turing à la fin de la guerre.

L'obligation de trouver des solutions très rapides de chiffrement, de déchiffrement ou de décryptement, et en particulier les travaux d'Alan Turing et de son équipe pour le décryptement ont largement contribué, par le passage de l'analogique au numérique, à la conception des ordinateurs et à l'avènement de l'informatique.

Jean-Luc Moliner

Jean-Luc Moliner, Directeur de la sécurité du Groupe Orange traite le sujet : « **La longue marche vers un avenir radieux… Le citoyen, l'entreprise et la cryptologie de 1968 à nos jours** ».

Au Panthéon des inventeurs et des inventions, Paul Baran, peu connu, devrait pourtant trouver une place de choix. Visionnaire et créateur d'un réseau d'ordinateurs, avec commutation de paquets et chiffrement de bout en bout, inspirateur du réseau Arpanet, Paul Baran avait prévu un changement de clés à chaque session et un code correcteur d'erreurs. Horst Feistel en 1971, alors employé chez IBM, pour protéger les distributeurs de cash des banques anglaises, a initié le chiffrement par blocs. Jean-Luc Moliner évoque ensuite les travaux de Whitfield Diffie et Martin Hellman, et leur stagiaire moins connu à l'époque, Ralph Merkle. En 1978 ces trois cryptologues ont jeté les bases du chiffrement à clés publiques, en produisant une clé de chiffrement en deux endroits sans s'échanger de renseignement permettant de la reconstituer. Le chiffrement à clé publique allait être concrétisé plus tard par le RSA, du nom de ses inventeurs Rivest, Shamir et Adelman. Les courbes elliptiques plus rapides pour chiffrer ont été introduites par Niel Koblitz et Victor Miller en 1985. Phil Zimmerman introduisait le PGP en 1991 mais qui était encore très peu utilisé, à l'époque, par les entreprises. L'algorithme Kerberos de chiffrement et d'authentification, développé dans le cadre du projet ATHENA au MIT est devenu un standard IETF en 1993, et l'Open Source faisait une entrée dans la cryptologie avec aussi S/MIME en 1998, et les solutions de *Single Sign-On* (SSO).

L'année 2000 a été celle des PKI, de l'*Active Directory* et de l'adoption de Kerberos par Microsoft. L'année suivante, deux Belges Joan Daemen et Vincent Rijmen, avec leur algorithme AES, remportaient l'appel d'offres émis par le NIST pour un nouveau chiffrement symétrique qui remplacé le DES et le 3DES. Daniel Julius Bernstein introduisait le chiffrement asymétrique par courbes elliptiques en 2005. À cette époque, les entreprises étaient assez démunies pour assurer la confidentialité de leurs données stockées ou transmises. Les cryptologues étaient encore trop peu nombreux. Le recrutement de tels

profils était d'ailleurs rarement envisagé, et les fournisseurs de solutions de chiffrement n'étaient ni français, ni européens.

Aujourd'hui, la cryptologie a un grand rôle à jouer dans notre monde de brutes, où on apprend après plusieurs années d'utilisation que des portes dérobées sont incluses dans les mécanismes de chiffrement pour permettre à certains États d'espionner les utilisateurs. Et on découvre des vulnérabilités dans les outils de chiffrement, réputés sûrs.

Après ces constatations peu réjouissantes pour nos vies privées, **c'est l'heure de la pause**. On se restaure, on fait des rencontres, on retourne voir les frises murales et le matériel de cryptologie exposé et les sponsors qui nous attendent sur leurs stands. On discute avec l'Américain Jon D. Paul qui nous transmet sa passion des machines à chiffrer, et on retourne dans l'amphi pour la suite de la journée.

Philippe Duluc

Philippe Duluc, Directeur technique Big Data et Sécurité d'ATOS et le professeur Jean-Jacques Quisquater prennent le relais pour évoquer le **quantique et le post-quantique**.

Jean-Jacques Quisquater éprouve plus de soucis côté algorithmique que côté ordinateurs vraiment quantiques. Ceux-ci sont encore loin d'exister. Aujourd'hui, la physique quantique est utilisée pour générer des nombres aléatoires indispensables pour créer des clés symétriques, et pour distribuer ces clés de manière sûre. Philippe Duluc voit le quantique sous l'aspect calcul très rapide et sur l'aspect cryptologie postquantique. Il explique l'expérience des franges d'interférences, causées par les ondes lumineuses qui passent à travers deux fentes de Young. Ceci a prouvé la nature ondulatoire de la lumière. Mais ceci peut s'expliquer aussi par sa nature corpusculaire, car la lumière est constituée de photons. En 1918, Max Planck a reçu le prix Nobel pour ses recherches sur l'énergie des quantas. En 1921, Einstein recevait le prix Nobel pour ses travaux sur l'énergie photoélectrique qui établissait la dualité ondes-particules. Comprendre cette dualité est indispensable pour expliquer des phénomènes qui se produisent dans l'infiniment petit.

Philippe Duluc explique le principe de l'intrication quantique et le principe de superposition des deux états |0> et |1> qui caractérisent chaque qubit. Il explique la décorrélation qui se produit quand on fait des mesures. Les algorithmes de Shor qui réduisent la complexité de la factorisation des grands nombres d'un problème exponentiel à un problème polynomial, et les algorithmes de tri de Grover sont évoqués ainsi que les différences entre bits et qubits.

Côté simulateurs ou ordinateurs quantiques, ATOS travaille dans son centre de recherche, de la Région parisienne, ouvert en 2016, sur quatre piliers : bâtir un simulateur quantique, développer des algorithmes postquantiques, travailler sur une architecture quantique de nouvelle génération et enfin utiliser le quantique pour la cryptologie et la cybersécurité… quand les ordinateurs quantiques existeront. Il vise une machine à 100 qubits sans correcteurs d'erreurs à l'horizon de cinq ans.

Pour Jean-Jacques Quisquater, même si l'algorithme de Shor permet de factoriser de grands nombres, il ne faut pas craindre l'obsolescence du RSA avant de très nombreuses années. Les courbes elliptiques seront menacées bien avant la factorisation des grands nombres qui toutefois deviendra un jour envisageable. La cataCRYPT qui rendra obsolète, par les ordinateurs quantiques, le chiffrement à clés publiques n'est pas pour demain. Mais peut-être cette factorisation se fera même par des ordinateurs classiques bien avant l'existence de vrais ordinateurs quantiques. C'est en tout cas ce que pense Jean-Jacques Quisquater et aussi Whitfield Diffie (celui qui, avec Martin Hellman, a donné une solution pour l'échange de clés).

Pour l'échange de clés de chiffrement symétriques, les Chinois ont réalisé une expérience par satellite, qui utilise le principe de l'Intrication quantique de photons, mais cette expérience ne peut fonctionner que la nuit et sur une distance limitée. Elle exige, sur une distance longue, le passage d'un état quantique à un état classique puis à nouveau à un état quantique.

La génération de nombres purement aléatoires par la physique quantique est par contre une technologie aujourd'hui maîtrisée et même utilisée par des banques.

Philippe Duluc nous présente les réalisations d'ATOS.


Sébastien-Yves Laurent

Nous passons ensuite à la dernière table ronde, animée par le Professeur Sébastien-Yves Laurent, Professeur à la Faculté de Droit et de Science Politique de l'Université de Bordeaux, avec le Général (2S) Jean-Louis Desvignes, président de l'ARCSI, le Professeur François Pellegrini de l'Université de Bordeaux, s'exprimant pour la CNIL, et Jean-Luc Moliner, directeur de la sécurité du Groupe Orange. L'ANSSI invitée à intervenir dans cette dernière table ronde n'a pas délégué de représentant.

Le sujet : « **Le dilemme sécurité / Liberté** ». Ce thème peut être traité sous l'angle de la morale, du juridique et du politique.

Le thème de la morale est écarté, et il est précisé bien entendu que le juridique est inspiré par le politique. Jean-Luc Moliner parle de la nécessité du « Privacy by Design » qui commence à entrer dans les entreprises, aidée par le règlement européen RGPD pour la protection des données à caractère personnel. Il faut limiter les traitements aux seuls nécessaires et n'utiliser que les données personnelles qui sont indispensables. Jean-Louis Desvignes avant de parler de « *Privacy by design* » estime qu'il faut revenir au « *Security by design* » prôné depuis près de 30 ans mais qui n'est toujours pas entré dans les mœurs et qui doit devenir une règle dès la conception d'un produit. Il n'est jamais bon d'ajouter la sécurité une fois le produit industrialisé et commercialisé. Il cite à ce sujet les 50 milliards d'objets connectés qu'on nous annonce conçus pour la plupart sans aucune préoccupation sécuritaire malgré les dangers que peuvent faire courir ces milliards de futurs zombies… La *privacy* n'est qu'une des applications qui peuvent en être victimes.

Jean-Luc Moliner déplore le mauvais fonctionnement de certains produits de sécurité et

Table ronde sur « Le dilemme sécurité / Liberté »

l'incapacité des États a en garantir la qualité. Nous sommes ainsi plongés dans un brouillard total avec une impression de sécurité illusoire. François Pellegrini cite un proverbe corse « Ce que tu ne sais pas, tu ne pourras pas le dire » au sujet d'une nécessité de protection légale mais pas opérationnelle. Pourtant la démocratie a la responsabilité morale de protéger la population.

François Pellegrini

François Pellegrini, au nom de la CNIL, pense que le RGPD doit devenir une marque mondiale et aller bien au-delà de la sphère privée. La protection par l'obscurité ne peut fonctionner, et induit un risque systémique. Les normes sont importantes. Il faut développer une vraie expertise pour pouvoir dénoncer les produits déloyaux. Il faut limiter les mécanismes qui permettent la surveillance de masse, mais pas nécessairement les interdire. Il faudrait instaurer une stratégie de puissance européenne et pouvoir fondre, en Europe, nos composants électroniques pour assurer une souveraineté européenne.

Jean-Louis Desvignes rapporte sa stupéfaction devant la réaction d'un haut responsable de la Gendarmerie en charge de la voiture connectée à qui il demanda : « Ne craignez-vous pas la présence de *backdoors* dans les logiciels embarqués ? ». « J'espère bien qu'il y en aura » justifiant sa réponse par la possibilité d'arrêter des gangsters sur les autoroutes négligeant au passage le fait que le secret de ces *backdoors* ne saurait être gardé très longtemps…

Le colloque à la BNF se termine par les conclusions du général Jean-Louis Desvignes qui a une pensée pour Jean-Marc Laloy qui de là-haut, doit nous applaudir.

Le dîner sur la Seine

La journée n'est pas terminée. En route pour le Quai Branly où une vedette des Bateaux parisiens nous attend au pied de la Tour Eiffel, pour une navigation sur la plus belle artère de Paris : la Seine. Les ARCSIstes et leurs conjoints ou conjointes montent à bord pour un très sympathique dîner de gala fluvial.

Et vogue le navire, coupe de champagne, noix Saint Jacques, bœuf Rossini, fromage et vacherin coco, vin blanc, vin rouge et quel merveilleux privilège de se retrouver entre amis ARCSIstes pour papoter sur cette si intéressante journée. Les conversations vont bon train, animées par une chanteuse. Paris et les lumières de ses rives défilent lentement du pont de l'Alma jusqu'au quartier de Bercy avec virage près de la BNF et retour jusqu'à la statue de la liberté, contournement de l'Île des cygnes et accostage au pont de l'Alma.

Je termine par une appréciation du Général Jean-Louis Desvignes, président de l'ARCSI, faite quelques jours après ce colloque, durant le débriefing du Conseil d'Administration de notre association : « Ce colloque a été le meilleur que notre association a organisé. Et bien sûr je salue encore l'immense travail de tous ceux qui ont contribué à faire de cet évènement le succès qu'il a connu, et en particulier je rends une fois de plus hommage à Jean Marc Laloy, qui fut un efficace secrétaire général de l'ARCSI, et organisateur de nos évènements, mais qui nous a hélas quittés et sans qui cet évènement n'aurait pu être ce qu'il a été ».

Encore merci pour ton travail de préparation de cette journée et bravo Jean-Marc, tu sais que les ARCSIstes gardent de toi un merveilleux souvenir.