Conférence prononcée le 6 février 2015 aux Archives nationales à l'Hôtel de Soubise dans le cadre de l'exposition « Le secret de l'Etat, Surveiller, protéger, informer »

Cryptologie : la grande illusion

Bonjour à toutes et à tous …

Tout d'abord je dois vous dire que cette conférence répond à une demande de Sébastien-Yves Laurent le co-commissaire de cette exposition avec Pierre Fournié. Dans le cadre du soutien que l'ARCSI (que j'ai l'honneur de présider) a apporté aux Archives nationales pour le montage de cette exposition, le professeur Laurent avait souhaité que je lui fasse des propositions de conférences d'accompagnement et quand je lui ai fait mes premières propositions il m'a gentiment mais fermement invité à me compter dans la liste. J'ai donc obtempéré en cherchant ce qui pourrait bien intéresser un public par ailleurs déjà bien instruit par les autres conférenciers. L'actualité aidant j'ai fini par proposer ce thème de l'illusion portée par la cryptologie pour l'avoir vécue à différents moments de ma carrière mais surtout lorsque j'ai été en charge de ce domaine au plus haut niveau de l'Etat en tant que chef du service central de la sécurité des systèmes d'information.

Tout d'abord face à un auditoire vraisemblablement hétérogène je me permettrai de faire quelques rappels sur le vocabulaire et sur quelques grands principes de la cryptologie. Ensuite j'évoquerai quelques désillusions cruelles qu'ont connues certains acteurs de la petite comme de la grande Histoire, dont le cours s'en est parfois trouvé modifié.

J'en arriverai à l'histoire plus récente en particulier celle que j'ai vécue comme acteur de ce domaine hautement sensible et je vous parlerai alors de ma grande illusion à moi, celle d'avoir cru qu'il était possible d'instaurer un contrôle démocratique de la cryptologie. Enfin je terminerai par la situation actuelle, celle qui a été révélée au grand public en particulier par les lanceurs d'alerte Assange et Snowden mais qui n'était pas tout à fait un scoop pour certains initiés.

Quelques rappels de Vocabulaire

Comme dans chaque discipline il existe un langage qu'il vaut mieux utiliser convenablement car je vois dans cette salle des spécialistes capables de vous crucifier si vous n'employez pas le bon mot.

La **cryptologie** est la « science du secret ». Ce terme est assez nouveau, pendant longtemps on a parlé de **cryptographie** car on ne traitait que des écritures secrètes. Très tôt en effet, en fait dès que l'écriture qui était en elle-même une forme de codage se démocratisa les plus suspicieux inventèrent un moyen de protéger leurs écrits selon différents procédés. On n'a pas toujours considéré que c'était une science, certains considéraient que c'était un art, d'autres de la sorcellerie et d'autres enfin ont été jusqu'à parler de recettes de cuisine, une autre forme d'art en somme. La sorcellerie c'était surtout pour ceux qui arrivaient à percer **la convention secrète** utilisée par l'adversaire.

La **convention secrète** se compose d'un procédé, une astuce, aujourd'hui on parle d'**algorithme** et d'un élément variable que l'on appelle la **clef**.

L'opération consistant à transformer un texte clair en quelque chose d'incompréhensible s'appelle le **chiffrement**, l'opération inverse pratiquée par le destinataire légitime du message s'appelle le **déchiffrement**.

L'opération consistant à retrouver le sens d'un message chiffré sans connaître tous les éléments de la convention secrète (le procédé et/ou la clef) est un **décryptement**.

Notons tout de suite que le message chiffré est un **cryptogramme** mais qu'il ne faut en aucun cas dire que l'on « crypte » un message car ce verbe n'aurait pas de sens puisqu'il signifierait que l'on chiffre sans connaître la convention secrète ! Bon ! Je vous l'accorde c'est une question de convention… Et la confusion est souvent entretenue par une mauvaise traduction des termes anglais mais aussi par la pratique d'une célèbre chaîne de télévision à péage dont le procédé de chiffrement était si faible que les autorités de l'époque n'avaient pas voulu qu'elle galvaude le terme réglementaire…

Vous trouverez pour désigner les « attaquants » d'un chiffre adverse différents mots et expressions: les décrypteurs, les cryptanalystes, les briseurs de codes…

Ah ! Surtout n'allez pas qualifier un cryptologue de cryptographe ! Celui-ci vous rétorquera qu'il n'est pas une machine…

Les grands principes de base

A l'école des apprentis chiffreurs on apprend que les deux plus anciens procédés de chiffrement sont la **Scytale** des Lacédémoniens et le **chiffre de César** pour les Romains. Même si **le carré de Polybe** moins connu est plus ancien et plus astucieux.

Le premier qui consiste à entourer une lanière ou bandelette de papyrus autour d'un bâton cylindrique de manière hélicoïdale puis à écrire son message dans le sens de la matrice du cylindre réalise ce qu'on appelle une **transposition** : les caractères composant le message s'en trouvent déplacés et mélangés une fois la bandelette déroulée.

Le chiffre de César consiste en un simple décalage d'alphabet de trois caractères. C'est une substitution (on peut préciser : « substitution simple à représentation unique »).

On peut noter qu'à cette époque le procédé doit être tenu aussi secret que la clef (le diamètre du cylindre pour la Scytale et la valeur du décalage de l'alphabet pour César).

Aujourd'hui, excepté pour des procédés gouvernementaux qu'on s'efforce de garder confidentiels, le secret ne repose que sur la clef c'est même un des principes qui sera énoncé au XIX è siècle par Kerchoffs : en effet pour la plupart des applications de la vie courante on utilise pour des raisons d'interopérabilité des algorithmes standards qui ont été sélectionnés et validés par la communauté internationale.

La faiblesse des premiers procédés.

Là je vais vous faire une confidence. A 15 ans j'avais fait la connaissance d'une jeune Italienne en voyage d'étude dans la cité romaine d'Autun où j'étais pensionnaire… Nous nous promîmes de nous écrire mais quand nos lettres devinrent un peu tendres Giusi me proposa d'utiliser un alphabet secret composé de signes mystérieux.

Je ne fus pas long à trouver la faille de ces substitutions simples malgré le caractère tarabiscoté des signes qu'avait imaginé ma belle Sicilienne pour échapper à la surveillance de ses frères. Les mots probables, la fréquence des lettres, les répétitions, le maintien de la ponctuation, tout cela constituait autant de possibilités de se trahir. Je me pliai pour lui plaire à cette discipline mais je m'aperçus que nos correspondances devenaient d'un ennui mortel et notre relation n'y survécut pas. La cryptographie, mot dont je ne connaissais pas alors le sens n'était pas faite pour moi. Et ce fut ma première désillusion !

Cela pour dire que la plupart des perfectionnements que crurent réaliser les premiers cryptologues étaient souvent des leurres : ils se compliquaient bien souvent la vie sans accroître la force de leurs coffres forts épistolaires.

Heureusement, d'autres se révélèrent mieux inspirés et ayant découvert la faiblesse de la représentation unique cherchèrent les moyens de briser cet homomorphisme d'ailleurs dénoncé dans un ouvrage remarquable de Al Kindi 801-873….

Dans cet exercice, différents noms se sont succédé : Cardan, Trithème, Alberti (substitution polyalphabétique), chacun apportant sa pierre à l'édifice. C'est Blaise de Vigenère qui réalisa finalement la synthèse de différentes améliorations compliquant sérieusement la tâche des cryptanalystes. Les carrés de Vigenère résistèrent en effet près de deux-cents ans jusqu'à Babbage! Mais ne furent pas toujours appliqués avec la même rigueur. Certains et certaines s'en mordront les doigts. Il faudra attendre la réalisation d'outils spécifiques tels des réglettes, des disques et des cylindres pour réaliser sans erreur les opérations fastidieuses de chiffrement et de déchiffrement.

Les grandes désillusions du passé : certains ici en connaissent davantage, je citerai les plus connues.

Marie Stuart est souvent citée comme une victime d'une cryptologie mal appliquée. En effet pendant sa détention par Elizabeth 1ère elle fut accusée de comploter contre sa cousine, le chef du GCHQ ou du MI6 de l'époque ayant réussi à décrypter les messages qu'elle échangeait avec ses soutiens extérieurs. L'objectif étant de la compromettre tout fut monté y compris la filière des messages pour la faire tomber dans le piège. Elle fut raccourcie comme bien d'autres …

De fait le procédé utilisé emprunté à la cour d'Henri II était encore une substitution simple avec quelques raffinements mais néanmoins facilement accessible.

Les Huguenots de Réalmont assiégés par Condé se trouvèrent fort dépourvus quand affamés ils furent. Manquant de vivres et de munitions ils exfiltrèrent un messager chargé d'aller quérir du renfort. Las ! Celui-ci fut intercepté et son message pourtant chiffré, tombé entre les mains de

Rossignol fut décrypté. Condé retourna à l'expéditeur le message dans sa version « en clair » et de dépit les assiégés se rendirent…

Remarqué pour cet exploit le Sieur Rossignol s'en fut bientôt au service de Richelieu qui assiégeait **La rochelle**. Cette fois c'est un message annonçant l'arrivée de navires anglais qui fut intercepté et de la même manière les assiégés furent avisés que leur plan était déjoué. Aux mêmes maux les mêmes effets et la Rochelle se rendit…

La dynastie Rossignol fit faire de grands progrès au chiffre français et celui-ci culmina sous Louis XIV et Louis XV mais bien qu'honnête serrurier selon la légende, Louis XVI semble avoir ignoré cette technique et répugné à ces méthodes anticipant sur un mouvement qui va voir l'expertise cryptologique française se perdre à la fin du XVIIIème siècle, inspiré tantôt par l'utopie: « cachez ce décryptement malhonnête que je ne saurais voir », tantôt par le cynisme : « inutile de se casser la tête à retrouver un code quand on peut l'acheter ».

Marie-Antoinette s'adonnera aux joies de la cryptologie pas vraiment pour comploter à la barbe de ses geôliers mais surtout pour se faire conter fleurette. Quelle horreur! Les experts n'en finissent pas de se quereller pour savoir la nature de ses relations avec le Comte de Fersen. On en est à radiographier les textes biffés pour faire jaillir la vérité. De toute manière l'imprudence qui lui fit ne chiffrer qu'une lettre sur deux ne fut pas à l'origine de sa décapitation même si certains la cite parfois au rang des victimes de la cryptologie mal maîtrisée.

Malgré quelques exceptions notables comme le **télégraphe de Chappe** qui va apporter un progrès considérable dans la rapidité et la confidentialité des messages(Notons toutefois que ce moyen moderne de communication fut détourné à des fins frauduleuses par deux hommes d'affaire qui ayant soudoyé deux employés du télégraphe s'échangèrent des informations boursières gagnant 24heures sur leurs concurrents servi par la presse) on aborde le XIX ème siècle dans une pauvreté cryptologique assez inquiétante.

Napoléon bien que préoccupé par les questions cryptologiques va voir ses messages interceptés et décryptés facilement durant la campagne puis la retraite de Russie offrant un avantage certain à son adversaire Koutouzoff. Il faut dire qu'entouré de cavaliers toujours pressés ceux-ci ne peuvent perdre du temps avec Vigenère et se contentent dans le meilleur des cas de Jules César. Cette négligence de certains grands chefs militaires se poursuivra encore longtemps. « L'urgence prime la sécurité » devient facilement un slogan déculpabilisant.

Napoléon III ne fera pas mieux et c'est encore en compagnie de Jules César qu'il se fera prendre à Sedan. Les Militaires français n'avaient pas de codes adaptés aux opérations militaires mais seulement des codes adaptés au langage diplomatique…

La fin du siècle et le début du suivant sont marqués en France par **l'affaire Dreyfus**.

Bien que peu évoquée la cryptographie y joua cependant un bien mauvais rôle : parmi les pièces figuraient le télégramme chiffré adressé par l'attaché militaire italien à son état-major. Intercepté ou récupéré dans une poubelle, il fut d'abord incorrectement décrypté et sa traduction inclinait pour la culpabilité du capitaine. Or un second décryptement correct l'innocentait au contraire. Ce fut

pourtant la première version qui fut produite au procès. Nous reparlerons plus tard de ce risque grave que fait courir une législation susceptible de produire de fausses preuves.

Arrive la 1ère guerre mondiale.

Ce sont les Russes qui sont les premières victimes d'une grave négligence : leurs armées n'ont pas reçu à temps les codes à utiliser pour correspondre en toute discrétion avec ce nouveau moyen de communication que constitue la TSF. Qu'importe, leurs généraux pensant sans doute que les ondes radio, s'arrêteront à la frontière, transmettent leurs ordres de bataille en clair. Les généraux allemands Hindenburg et Ludendorff savent tout : qui, où et quand. Résultat : **la bataille de Tannenberg** se transforme en déroute. Un revers tel que le grand historien de la cryptologie David Kahn s'interroge sur le rôle de cette bévue cryptologique monumentale dans le déclenchement de la révolution russe.

Mais finalement dans ce conflit **ce sont les Français qui vont se montrer les meilleurs**. Il faut dire que la défaite de 1870 a fait réfléchir. Une commission spéciale de cryptographie a été créée. Plusieurs noms vont apparaître et c'est la France qui publie à l'époque le plus d'ouvrages consacrés à la cryptologie. On est passé des divertissements coquins de George Sand et Alfred de Musset à Kerchoffs et ses principes pleins de bon sens et toujours d'actualité, de Lastelle, Bazeries, son cylindre et ses décryptements.

On aborde ce conflit avec quelques officiers de talent Cartier, Givierge, Olivari et qui vont savoir intégrer dans leur équipe des réservistes de premier plan. Résumons leurs exploits en disant que tout au long du conflit ils garderont une intimité constante avec leur adversaire en décryptant quasiment tout leur trafic. Le grand exploit viendra en 1918 quand leur adversaire en cryptologie le capitaine allemand **Fritz Nebel** tente de compliquer le code ADFGX en introduisant une sixième lettre ADFG**V**X au moment crucial où se profile une grande offensive dont on n'arrive pas à connaître l'axe sur lequel celle-ci va être lancée. Le capitaine Painvin travaillant jour et nuit va réussir à casser ce code et permettre le décryptement d'un message capital. Joint à un relevé goniométrique et quelques autres renseignements, il permet au commandement français de déclencher une contre-offensive qui va clouer sur place l'offensive allemande et dès lors l'initiative restera du côté des Alliés jusqu'à la victoire finale.

La confrontation organisée 50 ans plus tard entre Painvin et Fritz Nebel montre selon les témoins de la scène l'allemand réalisant comment il a peut-être fait perdre la guerre à son pays. Cruelle désillusion là encore.

Mais avant cet épisode un autre exploit cette fois au crédit des Britanniques doit être conté. C'est l'affaire **du télégramme de Zimmermann** le ministre allemand des affaires étrangères. Alors que la guerre sous-marine fait déjà rage celui-ci annonce au gouvernement mexicain qu'il va intensifier la lutte et s'attaquer aux navires américains. Si les Etats-Unis entrent en guerre, il propose une alliance au Mexique et leur promet après la victoire la restitution des Etats du Sud dont le Nouveau Mexique et l'Arizona. En outre il propose d'associer le Japon à cette aventure.

Les Britanniques violant quelque peu les bonnes pratiques diplomatiques envers un pays neutre interceptent le message adressé à l'ambassade d'Allemagne aux Etats Unis, celle-ci étant chargée de

le réacheminer sur Mexico. Ce message chiffré dans un nouveau code nouveau n'est que partiellement décrypté, et les Britanniques compte tenu de leur façon de procéder (l'interception de communications de pays neutres) ne peuvent en faire état. Ils attendent que le message soit retransmis à MEXICO cette fois chiffré dans un procédé ancien qu'ils maîtrisent parfaitement. Le décryptement est complet et peut être présenté à Wilson et à la presse internationale. Couplé au torpillage du Lusitania cet exploit cryptographique provoque l'entrée en guerre des Etats-Unis.

Le Miracle de la Vistule, prémisse d'une nouvelle grande bataille cryptologique

La guerre russo-polonaise de 1919-1920 n'est pas très connue mais elle mérite notre attention car c'est une très belle victoire de la cryptanalyse polonaise qui va jeter les bases de l'équipe qui s'attaquera bientôt à la célèbre ENIGMA. Peu de gens surent que la victoire surprenante des Polonais sur les Bolchéviques lors de la bataille de la Vistule était due au décryptement en une nuit par le lieutenant Jan Kowalewski du code russe. Cette victoire allait permettre la constitution d'un bureau chiffre efficace ayant l'appui du commandement du moins de ceux qui étaient dans le secret de ce succès. Le bureau allait surtout sous l'impulsion de son chef Ciezki, malgré une erreur de jugement lui faisant faire appel à un médium farfelu, innover en matière de méthode et de profils. Des mathématiciens avaient fait leur apparition et rendu de grands services durant la guerre russo-polonaise, il allait en recruter et les meilleurs pour la nouvelle bataille.

La bataille contre ENIGMA

Cette bataille pour le décryptement d'ENIGMA par les Polonais ayant fait l'objet d'une conférence ici même de Philippe Guillot le 19 décembre dernier, je ne m'appesantirai donc pas sur cette épopée. Mais si vous avez des questions à lui poser je suis certain qu'il se fera un plaisir d'y répondre. De même je ne voudrais pas déflorer le sujet de la prochaine conférence de Marie-José Durand-Richard et je ne ferai que survoler la grande victoire remportée par les Alliés sur le chiffre allemand et plus particulièrement, une fois les épisodes franco-polonais terminés, par le grand mathématicien Alan Turing.

Je me contenterai de dire, puisque j'en suis à relater les grandes illusions cryptologiques que l'inviolabilité d'ENIGMA qui semblait acquise a volé en éclat grâce à ce génie bien mal récompensé. Certes les Britanniques ont bénéficié des travaux des services polonais et ont commencé par exploiter les premières bomba et les fameuses grilles mais aussi de l'immense succès du renseignement français. Celui-ci, comme c'est relaté dans l'exposition, avait réussi à acheter le fameux traitre à son pays Hans Thillot Schmitt qui fit parvenir le mode d'emploi de la machine et les tableaux de clef. Mais les Allemands ont sans cesse modifié leur machine et c'est bien Turing qui a su trouver une autre méthode et automatiser au mieux ses propres bombes. Il a en outre certainement participé à la mise au point de Colossus ce premier véritable ordinateur qui viendra à bout de l'autre machine allemande, celle de Lorentz réservée aux plus hauts niveaux de l'appareil nazi.

Au bilan on s'accorde aujourd'hui pour dire que les exploits des cryptologues alliés ont permis de réduire la durée de la guerre de deux années économisant des milliers de vie.

D'autres grands succès de la cryptologie

On prendra soin de ne pas oublier que sur le front du Pacific les services de cryptanalyse américains notamment ceux de la Navy ont eux aussi permis de grandes victoires comme celle de Midway et de bien d'autres succès peu connus car souvent occultés. Mais contrairement au service du chiffre français de 1918 qui remporta de grands succès que l'on s'empressa de cacher surtout pour ne pas faire de l'ombre aux grands stratèges puis d'oublier, nos alliés eux, surent tirer parti de cet avantage inestimable qu'ils avaient pu exploiter. Le secret oui, mais l'oubli certainement pas.

Les conséquences des succès cryptologiques des Alliés principalement UK USA

UKUSA est d'ailleurs le nom d'un pacte d'entraide des services secrets américains et britanniques qui coure encore**.** Vous savez sans doute qu'il existe une base US d'interception sur le sol Britannique. Celle-ci était d'ailleurs traditionnellement commandée par le N° 2 de la NSA arrivé en fin de mandat.

Quand on possède un tel avantage que celui dont ont disposé nos deux pays complices on ne le brade pas facilement. D'où la chape de plomb qui va être coulée sur tous le domaine cryptologique pendant des années avec le consentement tacite des autres pays occidentaux. La RFA va bientôt en faire partie. On lui révélera en partie l'opération ULTRA et quand les officiers allemands entré dans l'OTAN s'étonneront : « si vous nous écoutiez si bien vous auriez dû gagner la guerre beaucoup plus tôt ». « C'est ce que nous avons fait leur répliquera-t-on ».

Pour maintenir cet avantage nos grands Alliés déploieront une grande énergie. Un blackout sera instauré sur les travaux des chercheurs et réservé aux applications gouvernementales. Un contrôle étroit sera exercé sur les produits proposés pour sécuriser les communications de l'Alliance et je soupçonne les américains de s'être servis de la normalisation Tempest très rigoureuse pour éviter la prolifération cryptologique c'est-à-dire éviter que trop de pays se bâtissent une compétence dans ce domaine. Tempest qu'est-ce que c'est ? Il s'agit du phénomène des signaux parasites compromettants. Tout appareil électrique donnant lieu à des coupures brutales de courant génère des parasites. Un moulin à café comme une imprimante. Une machine électromécanique traitant des informations confidentielles peut donc révéler son activité et rayonner parfois à grande distance. La France et plusieurs pays occidentaux dont les Etats-Unis et la Grande-Bretagne ont été victimes de ce phénomène dans leurs ambassades situées dans les pays de l'Est. Le phénomène y était aggravé par la pose d'émetteur clandestin placé dans les téléimprimeurs ou les machines à écrire. Un technicien du quai d'Orsay a en effet découvert qu'un condensateur comportait des fils qui n'avaient rien à y faire et un contrôle systématique a permis de découvrir l'ampleur de la supercherie. On peut considérer que pendant au moins six années les Soviétiques ont pu intercepter tout le trafic secret français sous l'ère Giscard !

Il s'en est suivi des recommandations visant à éliminer ces parasites soit en plaçant tous les équipements sensibles dans des cages de Faraday soit en les transformant eux-mêmes en cage de Faraday selon des normes très sévères et secrètes. Autant il est relativement facile de concevoir un

bon système de chiffrement au plan théorique autant il est difficile de le réaliser physiquement en tenant compte de ces contraintes. Quelques pays seulement maîtrisaient ces techniques.

Par ailleurs pendant un certain temps les Britanniques qui avaient récupéré un stock d'ENIGMA les ont aimablement fourgués à leurs amis du Commonwealth en particulier en leur vantant les mérites de cette machine que désormais ils contrôlaient parfaitement. D'autres comme la France ont su brader leurs matériels d'avant-guerre telles les C36 à leurs anciennes colonies. Unecélèbre firme suisse se spécialisa dans la commercialisation de cryptographes d'apparence sérieuse mais parfaitement perméables à la NSA.

Tout allait pour le mieux d'autant que la législation sur la cryptologie était généralement particulièrement restrictive et que les préoccupations des populations étaient à cent lieues des questions cryptologiques.

Mais advint le temps où le besoin de protéger autre chose que les communications diplomatiques ou militaires se fit plus pressant.

1975 Le diable sort de la boîte.

C'est en 1974 que le Bureau de standardisation américain lance un appel à candidature pour un algorithme standard de cryptologie destiné à protéger les transactions commerciales. A la stupéfaction des services de renseignement et de la NSA en particulier. Le monde de la recherche entre en ébullition et pense que l'on a désormais le droit de s'emparer de ce domaine considéré comme une sorte de fruit défendu. J'ai plagié un jour pour décrire cet attrait exercé par la cryptographie le titre de Buñuel « cet obscur objet du désir ».

C'est IBM qui remporte la compétition avec le DES. On discutera longtemps du rôle qu'a joué la NSA dans ce choix et surtout dans les modifications qu'elle y a introduit. Honnêtement je ne crois pas qu'on ait trouvé quelque chose à lui reprocher sauf d'avoir raccourci la longueur initiale de la clef. Mais là n'est pas l'important. En fait c'est à l'occasion de cette compétition qu'un nouveau concept cryptologique va naître. En effet Diffie et Hellman en profitent pour avancer une idée réellement révolutionnaire celle d'un système à « clef publique ».

Depuis plus de 2000 ans en effet tous les systèmes reposaient sur le partage d'un même secret : une convention secrète permet en effet de chiffrer un message et le destinataire utilise la même convention secrète pour prendre connaissance de ce message. Or voilà un duo qui propose d'utiliser une clef différente pour chiffrer et déchiffrer. Je chiffre mon message avec la clef connue de tous donc publique de mon correspondant et celui-ci le déchiffre avec une clef secrète que lui seul possède. Génial ! Sauf qu'il faut trouver une fonction mathématique liant ces deux clefs de manière asymétrique. Facile dans un sens difficile voire impossible dans l'autre. Finalement c'est un trio qui va trouver la solution technique en se basant sur la difficulté de factoriser les grands nombres : il est facile de fabriquer deux grands nombres premiers. Il est tout à fait facile de les multiplier entre eux. Mais si on ne possède que leur produit il est extrêmement difficile voire impossible de retrouver les deux nombres originels. C'est le principe du RSA les initiales des trois inventeurs Revest Shamir et Aldemann. Cette invention prodigieuse va résoudre plusieurs problèmes de sécurité :

1) La distribution des éléments secrets.

Dès lors que je peux trouver la clef publique de mon correspondant dans un annuaire il n'y a plus de limite à la taille des réseaux de chiffrement.

2) Je peux retrouver les performances d'un bon système symétrique en échangeant simplement les clefs de celui-ci
3) En inversant le procédé je peux chiffrer un court message avec ma clef secrète et mon correspondant peut vérifier que c'est bien moi qui le lui ai adressé.
4) Je peux avec une fonction de même type créer une empreinte de mon message et mon correspondant pourra vérifier en refaisant la même opération que le message reçu est intègre.
5) Je pourrai lui adresser au cours de cet échange différentes informations pouvant lui être utiles telles que mes identifiants.

   Bref les systèmes asymétriques ou à clef publiques combinés avec des systèmes classiques symétriques offrent toutes les fonctionnalités nécessaires aujourd'hui aux transactions électroniques pratiquées à grande échelle sur Internet.

   Je passe sous silence toutefois d'autres problématiques qui ont fini par aboutir à la mise en place de ce qu'on nomme des infrastructures de gestion de clefs IGC ou PKI en anglais.

Inutile de dire que cette révolution venait contrarier le confort dans lequel baignaient les services de sécurité. Tout un chacun allait pouvoir écrire en mode protégé à commencer par ceux qui étaient surveillés. Que faire ? Légiférer? Nationalement ? À l'échelle internationale ? Tout cela fut tenté.

Concentrons-nous sur la France qui jouissait d'une réglementation qui la mettait à l'abri. En effet les moyens cryptologiques avaient été classés sans le moindre émoi dans la catégorie des matériels de guerre régi par un décret/loi de 1939. En gros un régime de prohibition tant pour l'utilisation que pour la mise sur le marché. Ce régime se heurta bientôt aux besoins du commerce d'autant que notre pays grâce à l'ingéniosité de quelques chercheurs allait nous propulser comme champions des paiements électroniques grâce à l'invention par Michel Ugon de la carte à microprocesseur.

« Pardonnez-moi Monsieur le Secrétaire général du gouvernement j'ai pénétré dans cette enceinte de Matignon porteur d'une arme de 2ème catégorie » déclara le représentant du ministère de l'Industrie en exhibant sa nouvelle carte bancaire qui contenait des outils cryptographiques. Il fallait donc que les choses évoluent. Un assouplissement fut donc introduit en 1986 pour exclure certains équipements et logiciels commerciaux puis en 1990 une loi de réglementation des Telecom se vit accrocher un wagon législatif traitant de la cryptologie. L'objectif principal affichait encore clairement les impératifs de défense nationale. Deux régimes étaient admis un déclaratif pour les systèmes ne permettant que la signature (et non la confidentialité) et un régime d'autorisation strict pour tout le reste. Les décrets étaient à peine parus que les doléances des industriels et des premiers internautes commencèrent à se faire entendre. Il faut dire que le ministère de l'Intérieur qui n'avait jamais bronché face aux autorisations délivrées par le délégué interministériel (qui lui-même s'en remettait à l'avis de la DGSE) se rebiffa et se mit à refuser systématiquement les autorisations à tout système qu'il ne savait pas décrypter c'est-à-dire pratiquement tout.

C'est dans cet état de véritable crise que je débarquai à la tête du SCSSI en 1995.

Après avoir écouté les doléances des uns et des autres (Editeurs, industriels français et étrangers, les ministères concernés ainsi que nos partenaires étrangers) j'en arrivai à la conclusion qu'il fallait agir rapidement d'autant qu'on sentait poindre l'arrivée d'Internet même si une certaine élite des

TELECOM freinait non sans raison de toute ses forces cet avènement. Après bien des discussions je rédigeai un rapport réclamant clairement un assouplissement de la législation existante et une expérimentation d'un dispositif novateur celui des Tierces parties de confiance. Présenté en Directoire de la SSI ces propositions reçurent un accueil enthousiaste des ministères de la justice, de l'industrie et de la recherche mais un accueil plus que réservé de la Défense et surtout de l'Intérieur. Le SGG quant à lui, ravi de voir une porte de sortie à ses problèmes d'arbitrage permanent entre DISSI et Intérieur décida de passer sans attendre au régime des tiers de confiance. La loi de réglementation des télécom étant de nouveau en chantier il fallait faire vite et trois mois plus tard c'était chose faite.

Le principe de la nouvelle loi :

- Introduction d'un régime de liberté d'utilisation des moyens cryptologiques même très puissants gérés par un organisme agréé (TPC) c'est-à-dire ayant la confiance de l'utilisateur et celle de la justice.
- Liberté également d'utilisation des systèmes de signature
- Régime déclaratif pour les utilisateurs de produits de force modérée sans TPC mais à la portée d'un centre de décryptement étatique.
- Régime déclaratif également pour les fournisseurs de produits de signature
- Régime d'autorisation pour les fournisseurs de produits non gérables par TPC et tout autre produit exotique.

En outre le seuil de la cryptologie modérée (exprimé par la longueur de la clef utilisée) était fixé par décret simple en fonction de l'évolution de la technologie. Au départ il était fixé à 56 bits.

Il est important de noter que dans ce dispositif le recouvrement du clair d'un fichier se faisait soit par déchiffrement par le TPC soit par attaque par force brute méthodes toutes deux présentables en justice et n'ayant pas besoin d'être couverte par le secret de défense. Un système somme toute transparent empreint de légalité et parfaitement digne d'une démocratie.

Hélas ! D'abord les services rancuniers menèrent un combat d'arrière-garde pour retarder la sortie des décrets d'application. Ils chargèrent à outrance les contraintes des TPC tentant de rendre leur activité peu attractive. Ensuite les décrets dans la nouvelle procédure durent être soumis à Bruxelles où certains pays s'ingénièrent à les retarder. Enfin une dissolution hasardeuse de l'Assemblée Nationale vint chambouler le paysage politique. Et le ministre en charge des télécom (François Fillon) qui avait promis « deux TPC agréés avant la fin de l'année » s'en était allé.

Tous ces aléas avaient exacerbé les revendications et l'impatience du monde de l'Internet. C'est alors que le Messie arriva promettant de libérer la cryptologie de ses contraintes. Jospin en effet s'était laissé convaincre d'inscrire cet objectif et l'avait annoncé à Hourtin cette grand-messe du nouveau parti au pouvoir. J'imagine le militant de base recevant cette promesse…

En fait au départ ainsi qu'un feuilleton des Echos l'avait annoncé durant l'été il n'était question que de libérer les produits de moins de 56 bits.

Pour tenir cette promesse Claude Allègre lui conseilla de faire appel au pape de la cryptologie du moment Jacques Stern professeur à la rue d'Ulm afin de chiffrer financièrement le coût d'une telle mesure. DSK de son côté avait promis dans le Point qu'il donnerait aux services les moyens de casser

ce qui allait être libéré. Sic. Ajoutant même qu'il connaissait des brigands utilisant du 1000 bits alors qu'en France on n'avait tout juste droit au 40 bits. Montrant par là qu'il confondait allègrement les systèmes symétriques (les plus concernés) et les systèmes asymétriques non concernés mais utilisant des clefs bien plus longues…

Notre cher professeur rendit sa copie. A l'époque le coût pour casser du 56 bits dans des conditions opérationnelles était de mémoire évalué à environ un milliard de francs. Ce qui semblait acceptable. Un X malicieux avait calculé qu'avec les moyens de l'époque casser du 1000 bits aurait entraîné un réchauffement de la planète de 3 degrés…

On en resta donc à cet objectif mais un élément vint perturber le projet : Venait d'apparaître le spectre d'ECHELON ce réseau d'espionnage, sévissant jusque dans les couloirs de l'UE, secret de Polichinelle s'il en était mais auquel les conseillers du premier ministre accordèrent une importance démesurée. Est-ce la raison profonde ou était-ce parce que j'avais dit par boutade que si DSK voulait prendre des parts de marché dans l'industrie cryptologique il faudrait libérer le 128 bits ? Toujours est-il que ce fut cette solution, la mauvaise que l'on place dans un devoir de l'école de guerre pour permettre à l'instructeur de la rejeter sans se tromper, qui fut adoptée en janvier 1999.

Soyons honnêtes, à part moi, tout le monde a applaudit cette mesure, qui nous ramenait dans le rang des pays laxistes. Car il faut bien voir que la France qui souvent était comparée aux pays très crypto rigides voire peu démocratiques comme la Chine, la Russie ou Israël était en fait celle qui avait compris avant tout le monde que la menace principale n'allait plus être extérieure mais intérieure et que la cryptologie non contrôlée allait poser des problèmes à la lutte contre le crime organisé, les mafias, le terrorisme ou les pédophiles. Arguments balayés par les apôtres de la nouvelle économie qui faisaient miroiter les milliards à venir du commerce électronique. Sans compter que notre diplomatie qui défendait encore un mois plus tôt la position très dure de la France dans la négociation des arrangements de Wassenar fut ravie de ne plus se préoccuper de cette exception française venant s'ajouter à celle de la culture et de l'agriculture.

Quelque temps plus tard une réunion des directeurs techniques des agences de 5 pays les plus avancés se tenait à Washington DC. Le directeur de la NSA nous accueillit par ses mots : « maintenant que la France a lâché qu'est-ce qu'on fait ? ». Suivit un grand blanc et voyant que le DT de la DGSE ne bronchait pas j'ai pris la parole pour dire 1) que si nous nous étions sentis soutenus dans notre initiative de mettre en place des TPC les choses auraient pu tourner autrement. 2) qu'il ne fallait pas en faire un fromage car nous savions bien que d'autres méthodes avaient commencé à être utilisées consistant à aller chercher l'information en clair directement dans les serveurs grâce à des back Doors.

Nous en avions acquis la preuve écrite en 1997.

Le directeur décida alors une interruption de séance et je sentis une effervescence dans les couloirs. Puis le N 2 de la NSA Barbara Mac N'amarra vint vers moi et me dit : « Jean-Louis vous avez jeté un sacré pavé dans la marre ! »

Evidemment je ne pense en aucune façon que j'aie pu en quoi que ce soit influencer la politique américaine mais il me semble indéniable que la décision française de renoncer à un contrôle démocratique que certaines firmes américaines étaient prêtes à suivre a fourni à la NSA le prétexte

qu'elle attendait pour industrialiser la pratique jusque-là artisanale des back-doors non seulement pour les cœurs crypto mais pour tous les systèmes informatiques.

En France dans ma solitude je reçus toutefois le soutien inattendu de… la Ligue des droits de l'homme qui avait compris que les produits de sécurité qui allaient déferler sur notre territoire ne seraient que des placebos. Dans un tract elle exigeait que les produits proposés au marché français soient labellisés par le service que je dirigeais… Belle reconnaissance de la confiance que nous avions (re)trouvée en peu de temps.

Evidemment l'industrie française de la cryptologie ne fut nullement boostée par cette décision. Pendant que DSK veillait à ce qu'un internaute lambda puisse protéger ses mails d'amoureux transi ce que lui-même ne fit pas quand il fut au FMI(il se fit pincer par un mail adressé à sa dulciné qu'il avait omis de chiffrer), il laissa les banques continuer pendant plusieurs années à fournir des cartes bancaires protégées par une clef bien trop courte malgré plusieurs avertissements de mon service risquant de compromettre la crédibilité de notre fleuron industriel. Cela faillit arriver avec l'affaire Humpich au cours de laquelle je fus conduit à relancer mon avertissement un mois avant mon départ du service, départ que certains interprétèrent comme une victoire des Banques…

Un an plus tard ce fut le 11 septembre 2001 et tous ceux qui avaient œuvré à la libération de la crypto se firent étrangement discrets ou se mirent à ramer en sens inverse mais dans des conditions bien plus difficiles et en recourant à des dispositifs occultes. Il leur fallut attendre 2004 pour faire voter la nouvelle loi sur la confiance dans l'économie numérique soit plus de cinq ans après avoir tout casser… On y a gardé le terme de liberté mais assorti de contraintes tantôt inefficaces tantôt contraires à la jurisprudence de la CEDH. Dans une confession pathétique le Premier ministre avoua avoir fait preuve de naïveté en matière de sécurité il ne savait pas à quel point car il ne pensait certainement pas à ces questions de cryptologie.

Aujourd'hui où en sommes-nous ?

Les révélations de Snowden ont surpris même ceux qui auraient dû subodorer les pratiques de leurs grands amis. La confiance dans les technologies de l'information est à reconstruire entièrement. Or au moment où de l'autre côté de l'Atlantique les mouvements luttant pour la défense des libertés individuelles reprennent un peu de poil de la bête, au moment où le Patriot Act cède la place au Freedom Act nous sommes en train de compléter notre arsenal liberticide par des lois qui nous font reculer de plusieurs dizaines d'années en termes de démocratie avec toujours la même préoccupation de certaines corporations sécuritaires de s'affranchir des contraintes et garde fous judiciaires.

J'ai cru sincèrement au système des tiers de confiance pour assurer le plus juste équilibre entre le droit des citoyens de protéger leur vie privée et le devoir de la Justice de poursuivre les criminels système qui avait aussi pour avantage de placer tous les pays sur un pied d'égalité. Ma grande désillusion fut que ce soit un gouvernement traditionnellement épris de justice et de liberté qui mette à mort ce dispositif pour s'engager dans un dispositif occulte qui privilégie le pays qui possède l'essentiel de l'industrie de l'information.