Cryptologie et sécurité des systèmes d'information

Général Jean-Louis Desvignes

La cryptologie, ou science du secret, est vieille comme le monde. Des que deux êtres ont semblé s'échanger entre eux quelque confidence à l'abri des oreilles indiscrètes, il s'est toujours trouvé un ou plusieurs individus que ce comportement gênait et qui ont tenté de rompre cette connivence ❶[1].
Dès lors, la course entre cachotteries et indiscrétions fut engagée. Dès que l'écriture elle-même cessa d'être un code réservé à quelques initiés, la course aux armements cryptographiques prit son essor et celle-ci ne semble pas près de s'arrêter.
La cryptologie en effet, après être restée longtemps l'apanage des diplomates et des militaires auxquels elle a rendu les plus éminents services ou apporté les plus graves déboires, est aujourd'hui intégrée dans les outils que nous utilisons quotidiennement qu'il s'agisse de nos cartes à puce (bancaires, de santé, d'accès aux locaux de nos entreprises ou nos organismes divers, de nos téléphones portables, etc.), dans nos décodeurs de télévision à péage, les antivols de nos voitures ou encore dans les logiciels de nos ordinateurs.
Elle a joué un rôle considérable dans l'histoire et particulièrement durant le dernier siècle.
Elle est demeurée une composante essentielle d'une discipline plus large que l'on nomme « sécurité des systèmes d'information » ❷ elle-même partie prenante de ce qu'il est convenu d'appeler la maîtrise de l'information.
Elle continue de constituer un enjeu stratégique majeur dans cette lutte d'un genre nouveau : la guerre dans le cyberespace.

Quelques définitions et notions de cryptologie

Avant toute chose, il me faut en effet préciser quelques termes.
Au départ on a parlé de « **cryptographie** » car on cherchait d'abord à dissimuler le sens d'un message **écrit**. Avant la deuxième moitié du XX^{e} siècle a été ressenti le besoin de protéger toutes les formes de communication : la téléphonie dès la deuxième guerre mondiale, la télécopie dans les années soixante, puis toutes les formes de données incluant la vidéo ou visio conférence. Et on a adopté le terme de cryptologie plus général.

Dans le passé comme souvent les procédés utilisés aboutissaient à remplacer les lettres de l'alphabet par des chiffres ou des nombres, on se mit à parler d'opération de « **chiffrement** » lorsqu'il s'agissait de rendre le texte incompréhensible et de « **déchiffrement** » lorsque l'opération inverse était pratiquée par le destinataire légitime. Ainsi parlait-on du « Grand Chiffre de Louis XIV ». Et il y a encore quelques années existait la spécialité de

1 Ce symbole fait référence au numéro du transparent concerné.

« **chiffreurs** » au sein des armées comme au sein des Affaires étrangères.
En revanche, de celui qui réussit à percer le Chiffre de son adversaire on dit qu'il le « **décrypte** », il est aujourd'hui qualifié de « **cryptanalyste** ». Ainsi peut-on dire que Champolion a décrypté ou cryptanalysé les hiéroglyphes des Égyptiens.

L'âge artisanal de la cryptographie : de l'antiquité au XIX^{e} siècle

Le procédé le plus ancien que l'on cite généralement est celui de la **Scytale** ❸ inventé quelques siècles avant JC par les Lacédémoniens. Cela ressemblait à un bâton de maréchal, sur lequel était enroulée de manière hélicoïdale une lanière de cuir ou de papyrus et sur lequel on écrivait dans le sens de la matrice du cylindre. Une fois la lanière déroulée, les lettres ne formaient plus qu'une suite incompréhensible, sauf pour celui qui possédait le bâton du même diamètre.

Le second procédé le plus connu est celui utilisé par César qui pour écrire ses dépêches durant la guerre des Gaules, avait imaginé de décaler de trois lettres l'alphabet normal.

Le premier procédé dans lequel les lettres gardent leur signification, mais voient changer leur place, est une **transposition**.
Le second dans lequel chaque lettre est remplacée par celle qui est située 3 rangs plus loin est une « **substitution** ».

Ces deux procédés sont encore à la base de la majorité des systèmes cryptographiques d'aujourd'hui. Évidemment ceux-ci se sont singulièrement compliqués car il n'aura échappé à personne que le décryptement de ces procédés est relativement simple. Ils permettent de montrer comment se compose « **une convention secrète** » (*j'utilise là l'expression législative qui définit la cryptologie*) : celle-ci repose en effet sur 2 éléments : l'astuce : ex le décalage de l'alphabet d'une part, et la valeur de ce décalage d'autre part : 3 dans le cas présent qui constitue ce que l'on nomme **la clef**.
Il est clair qu'un enfant sachant lire et écrire, même s'il ne connaît que le procédé, est capable après plusieurs essais de retrouver la clef d'un Jules César[2].
Dans les procédés modernes l'opération de transformation, une suite complexe d'opérations logiques, est appelée « **algorithme** ». Celui-ci peut être gardé secret (c'est souvent le cas pour des systèmes de la Défense) ou rendu public : c'est le cas des algorithmes commerciaux. Dans ce cas on voit bien **que tout le secret est concentré dans la clef** qui doit donc faire l'objet des soins les plus attentifs[3].

Les deux grandes familles de système de chiffrement

Durant plus de deux millénaires, la cryptographie a reposé sur **le partage d'une même convention secrète** : la même clef étant utilisée pour chiffrer et déchiffrer le message ; on parle alors de système ou **d'algorithme symétrique**.
Naturellement ce système exige que préalablement cette clef ait été distribuée de manière sûre aux différents correspondants.

2 Il lui suffit de poursuivre de manière verticale l'alphabet sous une dizaine des premières lettres du cryptogramme, puis d'examiner toutes les lignes ainsi formées jusqu'à en trouver une qui ait du sens.

3 Remarque : un soin encore plus grand est apporté dans les systèmes de la Défense, on considère en effet qu'un jour ou l'autre un équipement de chiffrement sera perdu ou capturé et son algorithme susceptible d'être compromis.

En 1976, a été proposé par deux chercheurs géniaux Messieurs Diffie et Hellmann un principe tout à fait révolutionnaire reposant cette fois sur **deux clefs** : chacun des correspondants va posséder son propre jeu de clefs : une clef pouvant être connue de tous dite **publique** et une **clef secrète ou privée** que lui seul possède.
Pour chiffrer un message je vais utiliser la clef publique de mon correspondant et celui-ci va utiliser sa clef privée ou secrète pour le déchiffrer ❹.
Pour ce faire il faut que les deux clefs soient liées par une fonction mathématique dite difficilement réversible : connaissant l'une je ne dois pas pouvoir ou très difficilement en déduire l'autre. On parle alors de **systèmes asymétriques**.
Un ou deux ans plus tard, Rivest, Shamir et Adleman, tout aussi géniaux, réussissent à mettre en application ce principe en trouvant une telle fonction fondée sur les nombres premiers : il est en effet relativement facile de trouver deux nombres premiers, il est tout aussi facile de les multiplier entre eux. Mais s'ils sont grands et si je ne dispose que de ce produit il m'est quasiment impossible de retrouver les deux nombres initiaux. La « factorisation » que nous avons pratiquée à l'école sur de petits nombres est un véritable challenge dès que les nombres dépassent une certaine taille.
Le **RSA** (nommé par les initiales du trio), a aujourd'hui 33 ans et tient encore. Il est implanté dans tous les systèmes commerciaux par exemple les cartes bancaires. Simplement, les instances de régulation recommandent d'utiliser des clefs d'une certaine longueur ex : 2048 bits.

Ce procédé a permis en premier lieu de résoudre le problème des vastes réseaux de chiffrement pour lesquels il aurait fallu distribuer physiquement les clefs.

Mais si ces systèmes asymétriques ont constitué une véritable révolution c'est qu'on leur a trouvé d'autres vertus et d'autres propriétés.

D'abord, il n'a pas échappé aux cryptologues « traditionnels[4] » et sceptiques qu'avec de tels systèmes on ne pouvait chiffrer que de courts messages car les opérations à effectuer sur les grands nombres généraient des temps de calcul prohibitifs, ensuite l'une des clefs étant publique, n'importe qui pouvait envoyer un message chiffré à qui il voulait. Autrement dit c'était la chienlit !

Pour commencer, on eut l'idée de combiner deux systèmes : un système asymétrique permettait de s'échanger une clef pour un système symétrique plus performant en terme de débit.

Ensuite, on remarqua qu'en inversant le processus des systèmes asymétriques, on pouvait tout aussi bien chiffrer un court message avec la clef secrète et son correspondant pouvait, avec la clef publique, déchiffrer ce message et ainsi authentifier l'origine du message.

De plus, une autre forme d'algorithme asymétrique fut utilisée pour calculer une empreinte du message à transmettre : les algorithmes de **hachage**. Ceux-ci garantissent qu'à une empreinte donnée ne peut correspondre qu'un seul message. Ils garantissent donc l'intégrité de celui-ci après sa transmission.

4 Certains cryptologues gouvernementaux résisteront longtemps avant de recourir aux systèmes à clef publique sur lesquels ils émettaient les plus grands soupçons quant à leur solidité.

Dès lors moyennant une combinaison judicieuse de ces trois types d'algorithme à travers un protocole, on va pouvoir enrichir considérablement les fonctionnalités de sécurité :

- l'**authentification** des correspondants va être assurée celle-ci pouvant d'ailleurs être complétée d'un certain nombre de renseignements sur ceux-ci : nom, fonction, coordonnées, certificat, etc. de l'émetteur et du destinataire ;
- un message émis **ne pourra être répudié** ;
- l'**intégrité** du contenu du message transmis sera garantie ;
- et naturellement la **confidentialité** de l'échange sera assurée.

Les trois premières fonctionnalités sont généralement regroupées dans ce que l'on nomme la **signature électronique**. Celles-ci constituent en effet les mécanismes de base utilisés dans toutes les transactions électroniques effectuées sur l'Internet ou sur tout autre réseau.

Toute cette mécanique qui repose sur les biclés nécessite la mise en place d'une infrastructure de gestion de clefs (IGC ou PKI en anglais).
Pour intégrer un vaste réseau de chiffrement, il suffit de recevoir une fois pour toutes la clef publique de l'IGC, avec l'assurance de l'authenticité de cette clef. Ensuite, via le réseau, l'IGC communique en les signant toutes les informations de sécurité dont on a besoin, clefs publiques de ses correspondants notamment.

Retour à l'histoire

Ces rappels étant faits, penchons-nous un peu sur le passé afin de voir comment on en est arrivé là.

Tout au long de l'Histoire, la cryptologie apparaît ça et là utilisée tantôt par les souverains, tantôt par des gens d'église, tantôt par des courtisanes, etc. : les maîtres sont des abbés, des mathématiciens, des officiers, des gens de lettres, des banquiers…

Tantôt elle fait l'objet d'approche plus ou moins scientifique, tantôt elle fait penser à des recettes de cuisine.
Elle a connu des effets de mode et son degré d'herméticité a varié au fil du temps.
Je me contenterai de citer les principaux artisans de cet art ou de cette science :

Polybe moins connu que César a pourtant inventé avant ce dernier un procédé plus astucieux : le carré de 25 qui porte son nom ❺.

Les templiers utilisèrent la cryptographie pour envoyer des lettres de crédit confidentielles qui leur évitaient le transport de fonds ❻.

Alberti un génie multidisciplinaire inventa le cadran et de ce fait une première forme de substitution polyalphabétique ❼.

Quelques siècles après notre Jules, et sa substitution simple à représentation unique et fixe, l'**abbé Trithème** (1462-1516) ❽ auteur d'ouvrage sur la stéganographie (science différente consistant à cacher une information au milieu d'une montagne d'autres) est

surtout l'inventeur du premier procédé à substitution polyalphabétique sous forme de tableau.

Je saute directement à la Renaissance à **Philibert Babou**, ❾ secrétaire cryptologue du roi François 1er. Très habile au décryptement de toutes les dépêches étrangères il fut d'autant mieux traité par le roi que pendant qu'il passait des heures sur ses dépêches, sa femme les passait avec sa majesté…

Porta (1535-1615) ❿ (*vous noterez l'importance de la contribution italienne à la cryptologie*) introduisit la notion de clef dans les tableaux;

Vigenère (1523-1596) ⓫ effectua la synthèse des travaux de ses prédécesseurs et conçut le procédé qui en résulte: un tableau de Trithème avec un autoclave de Cardan dont la principale vertu est de ne nécessiter qu'une clef courte donc facilement mémorisable. Ce procédé est resté sûr jusqu'au XIXe siècle. Notons que c'est à cette époque que **Marie Stuart** fut trahie par la faiblesse de la cryptologie qu'elle avait utilisée dans son pseudo-complot contre Elisabeth et qu'elle fut conduite à l'échafaud…
Je passe sur **Viète**, père de l'algèbre moderne qui se distingua sous Henry IV par son habileté à décrypter les dépêches étrangères, pour arriver à **Rossignol** (1600-1682) ⓬ qui servit sous Louis XIII, les cardinaux et Louis XIV et porta le chiffre à son apogée. Parmi ses hauts faits sa contribution à la prise de La Rochelle, la création du cabinet noir et la création du Grand Chiffre de Louis XIV qui résista 200 ans au décryptement.
Après Louis XV grand adepte du secret, Louis XVI pourtant serrurier honnête si l'on en croit la légende, se désintéresse du cabinet noir. La compétence se perd. La Révolution va achever de faire décliner les connaissances. Est-ce parce que la Constituante va déclarer, douce utopie, le respect de la correspondance privée? Toujours est-il que Napoléon lui-même, qui considère que « le secret est l'âme de toute entreprise » va être victime de la faiblesse de sa cryptologie. Il utilise en effet le chiffre d'un empereur d'un autre âge: Jules César! Et c'est la Bérézina!

Dans cette régression générale, il existe pourtant quelques îlots de progrès.
C'est en effet sous la révolution que **Chappe** *(D..)* va révolutionner les techniques de télécommunications qui depuis plusieurs millénaires n'avaient pas beaucoup évolué. La majeure partie du courrier allait à la vitesse du cheval. Les dépêches urgentes pouvaient bénéficier dans certaines circonstances de la rapidité du vol des pigeons et cela depuis les Perses. Et quelques procédés optiques permettaient d'échanger des signaux sur de courtes distances.
Avec son télégraphe optique à bras articulés, **Chappe** introduit également un système de codage sophistiqué et tenu secret interdisant les interceptions puisque la plus grande partie des opérateurs ignore la signification des signaux qu'ils reproduisent.
Pourtant, ce système donnera lieu au premier acte de piraterie que l'on connaisse en matière de système d'information. En effet deux banquiers ayant pour complices deux opérateurs vont pendant des années utiliser le télégraphe à leur profit en se faisant transmettre durant la séquence des messages de service (répétition des messages erronés), des informations sur le cours des vins et autres denrées entre Tours et Bordeaux. Soit au minimum avec 24 heures d'avance sur les autres boursicoteurs servis par la presse. Pris de remords sur son lit de mort, l'un des compères crachera le morceau et son complice sera poursuivi sans pouvoir être condamné, ce type de délit n'étant pas

encore codifié. On peut considérer que c'est le premier exemple d'utilisation frauduleuse de ce que les informaticiens appellent des « canaux cachés ».

Mais c'est un Américain qui marque à cette époque un bond technologique important en matière de cryptologie en inventant un cylindre à disques porteurs d'alphabets désordonnés et interchangeables. Cet américain est plus connu pour sa rédaction de la déclaration d'indépendance des États-Unis dont il deviendra l'un des premiers Présidents. Thomas Jefferson *(D..)*. J'aime à imaginer que c'est en venant méditer sur les pentes du Mont Valérien, comme il est établi qu'il le faisait, qu'il a eu ses géniales intuitions, ce lieu sera appelé à la fin du XIX^{e} à abriter une école du chiffre…

Durant ce siècle un regain d'intérêt pour la cryptographie va émerger mais il est le fait plus de commerçants souhaitant protéger leurs courriers d'affaire au moindre coût (l'utilisation de code permet tout en protégeant le contenu de compresser les dépêches) ou d'artistes pour lesquels la cryptologie s'apparente à un jeu. En témoigne la correspondance frivole échangée entre Georges Sand et Alfred de Musset.
Mais la fin du siècle voit un nouvel essor de la cryptographie, sans doute imputable à la défaite de 1870. Bazaine ne disposait que d'un chiffre dérisoire et ses dépêches étaient facilement décryptables.
D'une part on redécouvre les vertus de procédés anciens, d'autre part on s'attache à définir les critères permettant de sélectionner les systèmes de chiffrement pour que ceux-ci soient réellement opérationnels.
En effet, le besoin de chiffrement apparaît de plus en plus incontournable avec l'utilisation d'une part des télécommunications électriques (télégraphe terrestre puis câbles sous-marins qui deviennent malgré les conventions internationales les premières cibles en cas de conflit) d'autre part de la TSF dont on se rend assez vite compte que ses ondes, ne s'arrêtent pas aux frontières.

Quelques personnalités doivent être citées pour s'être intéressées à la cryptologie : **Balsac**, **Jules Verne**, **Wheatstone** l'inventeur du fameux pont pour les électroniciens, **Kerckhoffs** qui édicta les grands principes d'un bon procédé de chiffrement :

- Mathématiquement indécryptable ;
- Perdable ;
- Clef communicable sans note écrite ;
- Applicable au télégraphe ;
- Portatif et utilisable par une seule personne ;
- D'un usage facile.

Également, **Delastelle**, **de Viaris** et surtout le commandant **Bazeries** qui va réinventer en l'améliorant le cylindre de Jefferson. Celui-ci sera rejeté par l'armée française mais adopté par l'armée américaine qui le conservera jusqu'au 2e conflit mondial. Bazeries procédera également à de nombreux décryptements dans des affaires importantes. Il eut certainement à traiter de l'affaire Dreyfus qui eut son épisode cryptologique : un message de l'attaché de défense italien correctement décrypté l'aurait disculpé tandis que les versions incorrectes qui furent produites durant le procès l'accablèrent…

Enfin l'utilisation de l'électricité pour les télécommunications, qui va permettre l'instantanéité de la transmission des dépêches, va rendre de plus en plus insupportables les délais

imposés par les méthodes de chiffrement archaïques. D'où des imprudences fréquentes. Tous les efforts vont donc porter sur une amélioration de l'efficacité des moyens cryptologique selon les critères de Kerckhoffs. Ces progrès vont progressivement passer par la réalisation de procédés mécaniques, puis électromécaniques et enfin électroniques.

Le Chiffre durant le premier conflit mondial

La Première Guerre Mondiale va encore voir s'affronter les cryptologues sur des procédés essentiellement manuels. Avec elle coïncide en effet la fin de l'âge artisanal et le début de l'âge industriel de la cryptologie.

C'est sur une imprudence fatale que débute le conflit sur le front de l'Est. En effet suite à des problèmes logistiques, les nouveaux codes russes n'ont pu être approvisionnés et l'État-major se trouve obligé de communiquer en clair ses ordres par radio. Il s'en suit la cuisante défaite de Tannenberg et ses conséquences. Les généraux allemands ne se vanteront jamais de l'avantage dont ils ont bénéficié. Les Russes avaient pourtant bonne réputation à la fois en cryptologie et dans l'art de récupérer les codes par des moyens « classiques ». Le **Cdt Olivari**, brillant cryptologue français envoyé à Moscou pour assurer la coopération franco-russe en cryptologie put en témoigner. Il se trouva en effet très dépité quand au bout d'une année d'efforts il présenta le résultat de son travail au général dont il relevait : la reconstitution d'un des principaux codes allemands. Celui-ci au lieu de s'extasier lui dit : « Il ne fallait pas vous donner tout ce mal, le voici, nous l'avons acheté ! ».

Ce fut bientôt au tour des Allemands de souffrir de leur faiblesse en cryptologie.
C'est en effet un décryptement magistral des services britanniques qui réussit à convaincre le Président des États-Unis d'entrer en guerre. Le « télégramme dit de Zimmermann » annonçait en effet une guerre sous-marine totale et proposait une alliance au Mexique et au Japon en cas d'entrée en guerre des États-Unis. C'est l'exemple le plus flagrant et le plus évident du rôle de la cryptographie dans l'histoire. Comme on le verra, un homme en resta marqué pour la suite des événements : Winston Churchill.

Les Français n'étaient pas en reste. La fin du XIX^{e} et le début du XX^{e} les avaient vus prendre une avance certaine en matière de réflexion et de publications. Celle-ci allait se confirmer tout au long du conflit. L'équipe réunie autour de Cartier va en effet accomplir des prodiges en décryptant presque en temps réel tous les messages allemands jusqu'à la victoire finale. L'épisode le plus célèbre est précisément celui du « télégramme de la Victoire » : Painvin un brillant lieutenant polytechnicien réussit à re-casser le procédé que le chiffre allemand venait de changer (il était passé de l'ADFGX à l'ADFGVX) juste au moment de la dernière offensive allemande : la deuxième bataille de la Marne. Il s'agissait d'un simple message logistique mais qui confirmait cette opération. Le commandement français put anticiper la contre-offensive qui fut victorieuse. Un des grands acteurs de cette victoire déclara qu'« à lui seul il valait tout un corps d'armée ». Mais cette citation est attribuée tantôt à Clémenceau tantôt à Foch ou un autre général et porte tantôt sur Painvin tantôt sur Cartier et son équipe.

Quoi qu'il en soit, si l'intérêt de la cryptologie a pu apparaître déterminant, les services qu'elle avait rendus, sous prétexte d'en assurer le secret, furent vite oubliés. Même si

les Américains firent appel à Painvin pour former l'American Black Chamber, l'embryon de la future NSA aux ordres du LCL Yardley, ce n'est pas pour autant qu'en France on capitalisa sur ces enseignements. Et de ce fait, la France allait aborder la seconde guerre mondiale dans un état de faiblesse doublé d'une mésentente entre services qui ne fut certainement pas étrangère au désastre de 1940.

La suprématie des cryptologues alliés durant le second conflit mondial

Les exploits des Alliés en matière de cryptologie sont connus, de nombreux ouvrages en ont parlé, il y a même eu des films, portant notamment sur la capture de la machine ENIGMA à bord d'un sous-marin. Aussi je ne m'y attarderai pas. Je rappellerai simplement que les décryptements de l'ENIGMA, la célébrissime machine allemande, ont commencé très tôt en Pologne et au Royaume-Uni, d'abord sur le modèle commercial inventé par Scherbius peu après la première guerre mondiale puis sur les modèles adoptés par la Wehrmacht.
Les Polonais qui bénéficient du génie des mathématiciens **Rejewski** et **Sygalski** vont jusqu'à reconstituer la machine.
Les Britanniques s'en inspirent pour réaliser leur propre machine de chiffrement Tipex. Celle-ci va leur servir également à étudier l'ENIGMA.
Les Français quant à eux vont fournir aux deux autres services des renseignements importants - des notices et des tableaux de clefs obtenus par une voie classique - et vont accueillir l'équipe polonaise après l'invasion de leur pays.
Pour mener à bien ces travaux d'attaque du chiffre allemand, les Britanniques installent à Bletcheley Park un centre spécialisé hautement secret où ils concentrent une grande quantité de matière grise : parmi les recrues le mathématicien **Turing**.
C'est là qu'ils réussissent à construire un automate, la BOMBE capable de décrypter en temps quasi réel les messages chiffrés par la Kriegsmarine.
S'ajoutant à d'autres progrès techniques comme celui des radars embarqués, leur connaissance du contenu des messages adressés aux meutes de U-boats va marquer un tournant décisif dans la bataille de l'Atlantique et in fine apporter la victoire.
C'est également à Bletcheley Park que pour décrypter d'autres machines (machine de Lorentz notamment) Turing va concevoir le premier véritable ordinateur : COLOSSUS.

Sur le front du Pacifique, les Américains de leur côté décryptent le chiffre japonais : la bataille de Midway, autre tournant important dans ce conflit, constitue une grande victoire du service de décryptement de la Navy.

Quand l'Allemagne rejoindra l'OTAN et que les Alliés seront amenés à révéler les informations dont ils ont bénéficié, les responsables allemands se montreront incrédules : « Si vous nous décryptiez aussi bien, vous auriez dû gagner la guerre beaucoup plus tôt… ». « C'est ce que nous avons fait ! » leur a-t-on répliqué. Il est en effet généralement admis que cette maîtrise de la cryptologie a écourté la guerre d'au moins une année.
C'est pourquoi d'ailleurs Churchill a cité comme facteurs clefs de la victoire : la Home Fleet, la Royal Air Force et… la cryptographie ! Plus qu'aucun autre il était conscient de l'importance de cette science dont il protégea le secret parfois au prix d'immenses sacrifices.

La deuxième moitié du XX^{e} siècle débuta avec l'électronisation des machines.

L'OTAN, cette organisation née après la guerre, lança en effet une compétition pour doter l'alliance d'une nouvelle machine à chiffrer les messages télégraphiques. Cette compétition coïncida avec la volonté de la France de renouveler son parc cryptologique. C'est la machine Myosotis premier équipement entièrement transistorisé qui porta les couleurs de la France. Celle-ci fut évaluée et jugée apte mais c'est une machine américaine la KW7 qui remporta le marché.
Bien vite la numérisation permit d'envisager d'une part de chiffrer simplement toutes les formes d'information : la voix, les images fixes puis animées et toutes les sortes de données, d'autre part de chiffrer globalement toute une artère véhiculant plusieurs communications simultanément. Tel fut le cas du système RITA de la société Thomson que nous réussirons à vendre à M. Reagan…

Le chiffre qui avait longtemps été considéré comme un frein aux télécommunications devenait transparent. Mieux, en induisant un trafic permanent, le chiffrement de voie ou d'artère permettait de dissimuler l'activité opérationnelle d'une liaison, celle-ci pouvant être un indicateur précieux pour l'adversaire.
Dès lors la cryptologie allait se répandre et descendre de plus en plus bas dans la hiérarchie gouvernementale et militaire en particulier. Les réseaux de données d'abord à la norme X25 puis conforme à l'Internet Protocole vont nécessiter de nouvelles techniques mais les principes restent à peu près les mêmes.
La véritable révolution viendra avec l'arrivée tardive des clefs publiques dans les armées et les fameuses infrastructures de gestion de clefs (IGC ou PKI).

Aujourd'hui la cryptologie s'est largement démocratisée et son usage est souvent ignoré des utilisateurs qui effectuent sans s'en rendre compte des opérations complexes en payant avec leur carte chez un commerçant, en téléphonant avec leur mobile, en regardant la télévision ou en montant dans leur automobile.
Elle s'est complètement miniaturisée : en témoigne la différence entre l'équipement de cryptophonie de plusieurs tonnes utilisé par Roosevelt et Churchill et le futur téléphone de Nicolas Sarkosy.

L'étape suivante qui est annoncée semble devoir être la cryptologie quantique qui en est à ses tout débuts et qui permet de constituer de manière sûre une clef parfaitement aléatoire utilisable ensuite de manière classique.

Mais revenons quelques instants aux innovations technologiques qui permirent à la cryptologie de changer d'âge.
L'électrification allait avoir une conséquence inattendue et terrifiante. Les parasites générés par les variations brusques de courant dans les téléimprimeurs notamment allaient dans certaines circonstances ruiner tous les efforts déployés pour rendre hermétique les messages. Ces parasites pouvaient en effet être corrélés aux caractères transmis ou frappés simplement sur un clavier. Un appareil de réception permettait alors de reconstituer à distance le texte pendant qu'on était en train de le chiffrer. C'est le phénomène qui dans le jargon de l'OTAN va être qualifié de menace TEMPEST et qui s'applique à tous les équipements fonctionnant à l'électricité. Notons que la compromission peut se propager à très longue distance si par malheur le signal parasite émis vient à se coupler fortuitement à un conducteur ou plus grave à un moyen de communication.
La deuxième vulnérabilité a été introduite quand certains informaticiens ont envisagé

de se passer des équipements cryptographiques en faisant effectuer directement les opérations de chiffrement sur les ordinateurs. Le chiffrement purement logiciel effectué sur des automates dont on ne maîtrise que très partiellement et approximativement le fonctionnement n'apporte aucune garantie sérieuse. Le problème s'est aggravé avec la mise en réseau de ces ordinateurs.

Pourtant, c'est ce qui se passe sur tous nos PC quand nous confions nos N° de carte bancaire sur un site apparemment sécurisé par le petit cadenas qui s'affiche. C'est ce qui fait la différence entre différents systèmes d'authentification soit disant forte : dès lors que par exemple on vous demande de frapper un mot de passe directement sur votre clavier ou sur un lecteur de cartes à trois sous relié à votre PC il faut considérer que ce code est perdu dans la mesure où vous représentez une cible intéressante, c'est-à-dire solvable, pour le hacker qui a pris le contrôle de votre ordinateur. Et comme l'actualité le montre c'est chose courante.

Il existe également des menaces un peu plus sophistiquées mais accessibles telles que la découverte d'un code de carte à puce par l'analyse de sa consommation de courant en fonction des chiffres que l'on essaie successivement. Méthode parmi d'autres que l'on qualifie de DPA : Analyse différentielle de la puissance consommée.

Par conséquent, comme je l'ai déjà dit, la cryptologie ne peut apporter à elle seule la sécurité.
Il est indispensable de disposer de plate-forme de confiance dûment évaluée et certifiée.

Le contrôle de la cryptographie par les États

Il est évident que les pays qui à la fin de la guerre ont compris ce qu'ils devaient à la cryptologie ne vont pas laisser filer un tel avantage et vont tout faire pour le conserver secret aussi longtemps qu'ils le pourront. Ils vont tout faire pour que les compétences en cryptologie ne se diffusent pas. D'où les réglementations nationales en matière de produits cryptologiques qui, grosso modo, vont être assimilés à des armes de guerre et soumis, au minimum à un contrôle aux exportations (cas des États-Unis), ou à un contrôle strict également sur le territoire national, comme ce fut le cas en France.
Il faudra attendre 30 ans pour que se lève le voile sur les exploits de Bletcheley Park et la fin des années soixante-dix pour que soit relancée ouvertement la recherche en cryptologie avec la montée des besoins du monde commercial.

La publication du DES : le diable sort de la boîte

C'est en effet pour répondre au besoin de confidentialité des applications financières que le Bureau de standardisation informatique américain (l'ancêtre du NIST) lança en 1975 un appel à proposition pour un algorithme robuste capable de sécuriser les échanges des institutions financières. Ce fut un vaste appel d'air qui enflamma le monde de la recherche mais qui jeta un froid parmi les services de renseignement, ceux-ci voyant là le début de leurs difficultés à continuer à écouter en toute quiétude les communications de la planète.

La compétition fut remportée par IBM avec le célèbre DES (Data Encryption Standard) un algorithme symétrique. Celui-ci fut supervisé par la NSA qui en réduisit la taille de la

clef de 64 bits à 56. Cet examen jeta la suspicion sur l'herméticité de cet outil mais après plus de 40 ans de bons et loyaux services aucune faille n'a réellement été découverte. Le DES est encore en service dans certaines applications. On l'a renforcé en le triplant. Le triple DES est un DES dans lequel en gros, on fait passer trois fois l'information à chiffrer, moyennant une clef également triplée. Plus récemment on est passé à l'AES qui a été sélectionné dans des conditions semblables et se trouve utilisé aujourd'hui jusque dans des applications militaires.

L'ébullition autour de l'affaire du DES a permis à de nouveaux talents de s'exprimer et c'est à cette occasion que Messieurs Diffie et Hellman ont eu l'idée lumineuse des systèmes asymétriques. L'affaire n'était pas mûre pour qu'une proposition soit faite mais c'est l'année suivante comme me l'a raconté Shamir que le système RSA est né.

Une fois le diable sorti de sa boîte difficile de l'y faire rentrer. Les « services » n'avaient plus que leurs yeux pour pleurer. Pendant quelques années ils ont essayé de freiner la diffusion du DES mais c'était peine perdue.

L'affaire se corsa quand M. Zimmermann mit à la disposition des internautes son célèbre PGP (Pretty Good Privacy). Une véritable provocation. Un combiné de systèmes symétrique et asymétrique permettant de créer de proche en proche de vastes réseaux de chiffrement.

Les services, plus entraînés à recueillir les signaux électromagnétiques que les octets sur Internet, y perdirent leur latin. Zimmermann fut poursuivi par l'administration et se défendit en prétendant être au service de tous les dissidents opprimés de la Planète notamment chinois. Une certaine suspicion entoura les versions suivantes de ce logiciel lorsque Zimmerman récupéra son passeport mais PGP reste un système très utilisé.

La période 1990-2000 est en effet celle de la montée d'Internet et du besoin bien vite ressenti d'assurer la protection des messages qui transitent sur ce réseau structurellement insécurisé. Mais c'est aussi celle qui voit les questions de sécurité intérieure prendre le pas sur les questions de sécurité extérieure après la chute du mur.

Or il se trouve que la France très tôt avait pris la mesure de cette menace croissante. Rappelons que nous fûmes frappés par les attentats de 1986. C'est pourquoi la réglementation sur la cryptologie qui prend en compte la possibilité pour les criminels et terroristes de tous genres d'utiliser la crypto pour dissimuler leurs crimes ou la préparation de ceux-ci, va apparaître comme l'une des plus restrictives au moment où tout le monde ne parle que d'ouverture et de liberté et où la vague de l'Internet va faire naître des espoirs complètement fous faisant perdre le sens commun à beaucoup.

Pour la communauté qui s'intéresse à l'intelligence économique, l'épopée de la libéralisation de la réglementation cryptologique ne manque pas d'intérêt. Car presque tous les acteurs vont être amenés à prendre parti parfois contre leurs intérêts pour aboutir à une situation aujourd'hui bien pire que celle qui était dénoncée à l'époque en matière de liberté individuelle.

En effet au début de la bulle Internet, les tenants de la sécurité (la police et la DGSE pour

simplifier) vont tout faire pour bloquer le développement de la cryptologie comme au début des années cinquante, n'acceptant que contraints et forcés quelques assouplissements. La police plus que la DGSE d'ailleurs car elles ne partent pas à égalité : casser du 40 bits en 1995 est hors de portée de la première. Or celle-ci refuse soudain de s'en remettre à ses collègues de la Défense en cas de besoin, commence à exiger ses propres moyens d'attaque et se met à refuser toutes les demandes d'autorisation qui lui sont soumises y compris, c'est un gag, celles d'organismes travaillant pour la Défense.
C'est dans ces conditions que, venant d'être nommé à la tête du SCSSI, je suis amené à proposer un assouplissement de l'application de la réglementation existante suivi d'une inflexion de celle-ci vers une libéralisation raisonnable poursuivant la voie déjà engagée précédemment :

- En 1986 des dérogations avaient été accordées au régime strict pour les applications commerciales par exemple pour les cartes à puce dont notre pays était en train de devenir le champion.
- En 1990, à la loi de réglementation des télécommunications avait été accroché un wagon sur la cryptologie instituant plusieurs régimes, dont un purement déclaratif pour les équipements n'assurant que des fonctions de signature et ne risquant pas de mettre en danger la Défense nationale.

Je proposai d'aller plus loin en introduisant un régime de liberté et en instituant surtout le régime des fameux « tiers de confiance ». Cette loi pouvait se résumer ainsi :
L'utilisateur pouvait recourir :

- à des moyens cryptologiques de force modérée décryptables par force brute (par essais systématiques) par les services de l'État
- à des moyens cryptologiques forts à condition que ses clefs soient gérées par un organisme agréé qui pouvait dans un cadre strictement défini remettre les clefs ou procéder aux opérations de déchiffrement à la demande d'un juge.

Cette solution, à l'étude au niveau européen, semblait le mieux à même d'assurer le plus juste équilibre entre les aspirations légitimes des citoyens à bénéficier de garanties pour la protection de leur vie privée ou des entreprises à se protéger et le besoin non moins légitime de conserver à la Justice et à son bras armé, la Police, les capacités d'investigation nécessaires au maintien de l'ordre public et de la sécurité du pays.

Les ministères sécuritaires renâclèrent mais l'enthousiasme de ceux chargés de l'Industrie, des PTT et de la Recherche fut tel que Matignon décida de passer directement à cette solution en profitant de la révision de la loi de réglementation des télécom. Ce fut chose faite au printemps 1996. Mais comme toujours, ce furent les décrets d'application qui furent longs à accoucher. Les sécuritaires s'acharnèrent en effet à charger la barque des tiers de confiance qui introduisaient un guichet auquel il fallait montrer patte blanche pour procéder à des interceptions dont on sait bien qu'elles peuvent être pratiquées sans de telles formalités.
Or malgré les charges qui avaient été imposées à cette profession, une vingtaine de candidats étaient déjà sur les rangs.

Si l'annonce de cette libéralisation avait permis de faire baisser la pression, (F. Fillon avait annoncé : « à la fin de l'année 1997 il y aura déjà deux tiers agréés ») le retard pris dans la publication des décrets qui devaient, de surcroît, être soumis à Bruxelles, relança la

polémique et les lobbies, hostiles à toute réglementation autre que celle, incontournable, de l'administration américaine, redoublèrent leurs actions :
« LIBÉREZ la Crypto ! » proclamait en une le Monde Informatique. « La France crée le cyber goulag du XXIe siècle » s'indignait un avocat du Barreau de Paris défenseur des intérêts de Microsoft dans le Wallstreet Journal.

Pourtant, du côté de l'étranger, tout le monde était attentif à ce que nous étions en train de mettre en place. La plupart des pays percevaient le danger d'une cryptologie débridée et nous enviaient d'avoir un texte de loi traitant ce sujet.
Russes, Japonais, Coréens, Singapouriens étaient venus nous voir. Notre législation avait été à maintes reprises exposée dans les forums de l'OCDE ou du G8. Sans parler des pays majeurs en cryptologie dont les agences se réunissaient périodiquement.
Même les États-Unis qui s'étaient vus refuser le système de Key escrow connu sous le nom du composant miracle CLIPPER CHIP qui devait résoudre le problème sous l'administration Clinton commençaient à s'intéresser à notre solution. De grandes firmes nous dépêchaient leur armada d'avocats pour examiner les conditions d'une « compliance » de leur solution avec la loi française…
Barbara Mac Namara, le N° 2 de la NSA pouvait alors me présenter à son nouveau boss en disant : « vous savez, le SCSSI est un petit service, mais il est terriblement actif ! »

Hélas les décrets tardaient et les lobbyistes passèrent à la vitesse supérieure d'autant qu'intervint un événement politique qui allait tout bouleverser : une dissolution « hasardeuse »…
Pour la première fois en France la cryptologie s'invita dans le débat politique. Cela avait été le cas précédemment dans la campagne présidentielle aux États unis. Alors qu'une conseillère de l'Élysée, côté Chirac, avait renoncé à faire aborder ce sujet, l'équipe Jospin s'en occupa. Cela n'eut aucune conséquence sur le résultat. Cependant durant l'été qui suivit la victoire de la Gauche, le journal « Les Échos » publia un feuilleton entièrement axé sur ce sujet : un conseiller de Jospin au terme d'un scénario crédible persuadait celui-ci de libéraliser la crypto jusqu'à 56 bits. Mon autorité de tutelle de l'époque m'avoua qu'il n'avait pas songé à faire enquêter sur les origines de ce qui m'apparaissait comme un élément d'une opération d'intelligence économique entamée depuis plusieurs mois.
Effectivement au cours de sa conférence à Hourtin, Lionel Jospin annonça son intention en tout point conforme au scénario du feuilleton !
Le gouvernement nomma un expert pour évaluer les conséquences de cette évolution. Celui-ci allait rendre un rapport très documenté chiffrant le coût de cette libéralisation en terme d'investissements pour le service chargé de retrouver malgré tout le clair des messages interceptés. Selon la rapidité visée, l'investissement variait déjà de quelques dizaines de millions à un milliard de francs. Il faut dire qu'une chose est de casser une clef de 56 bits à l'occasion d'un challenge pour lequel on pouvait réunir via l'Internet quelques milliers d'ordinateurs à travers le monde, une autre est de décrypter de manière opérationnelle plusieurs dizaines ou centaines de messages quotidiennement avec un enjeu de vie ou de mort par exemple si l'on pressent la commission imminente d'un attentat.
Mais à l'époque une clef de 56 bits pouvait toutefois apparaître comme le seuil raisonnable pour une protection d'intérêts non stratégiques. La loi, du reste, avait prévu un mécanisme de révision de ce seuil en fonction de l'évolution des technologies. L'expert gouvernemental rendit son rapport en recommandant cette nouvelle limite. Du reste

c'est ce que réclamaient les firmes américaines pour se simplifier la tâche puisque c'était ce qu'elles étaient autorisées à exporter.
Quelques mois passèrent sans que le sujet soit remis à l'ordre du jour. Cependant fin 1998 un accord international devait être renégocié celui de l'arrangement de Wassenar. La délégation française continua sur les errements en vigueur et défendit sa position très stricte habituelle.
Or en janvier un comité interministériel allait prendre une position à 180° de celle-ci à la surprise générale. L'équipe Jospin annonça en effet (avec l'accord de l'Élysée) la libéralisation du 128 bits! Cette annonce fut généralement saluée à travers le monde comme une décision courageuse et qui allait dans le sens de la liberté de communiquer et surtout de faire des affaires avec le commerce électronique.
Pourquoi être allé au-delà de ce qui était réclamé? D'abord parce que bien que le professeur ait expliqué de manière imagée la différence colossale pouvant exister entre des « 2 » affecté d'exposant différents, il n'est pas certain que tous les responsables impliqués aient compris ce que cela signifiait:

- Casser 40 bits disait le bon professeur, c'est vider le lavabo avec un dé à coudre,
- Casser 56 bits, c'est la baignoire toujours avec le même dé à coudre,
- Casser 128 bits, c'est l'Océan!

Pourtant le ministre des finances, grand partisan de la libéralisation, confia au Point: « s'agissant des services de sécurité, je leur donnerai les moyens de casser ce qu'on aura libéré ». Et montrant qu'il confondait allègrement les systèmes symétriques qui utilisent des clefs courtes avec les systèmes asymétriques qui utilisent des clefs longues, il ajoutait: « Il y a des truands qui utilisent des clefs de plus de 1 000 bits alors que nous n'autorisons que des clefs de 40 bits! »
Un polytechnicien facétieux calcula que les moyens informatiques de l'époque nécessaires pour casser du 1 000 bits feraient monter la température de la planète de 3 °C…

L'argument qui l'avait emporté était stupéfiant de naïveté: l'industrie française de la cryptologie allait booster ses ventes grâce à cette manœuvre hardie. Le résultat dépassa mes prévisions les plus pessimistes. L'industrie américaine en profita pour déverser toute sa production de solutions soit disant ultra-sécurisées en fait aussi efficaces qu'un placebo vis-à-vis de ceux qui continuaient à en superviser la conception et la commercialisation.
L'industrie française de son côté, éberluée par ce changement de politique totalement inattendu, ne se précipita pas et laissa la place aux grands éditeurs habituels. Il fallut attendre des années pour que certains se refassent une petite niche.

Malgré les mises en garde, les conseillers avaient oublié une chose: en cryptologie, la longueur des clefs n'est qu'un des éléments donnant une indication sur la force du procédé. Bien plus importante est la manière dont un procédé mathématiquement hermétique est implanté et utilisé dans un système. De multiples failles peuvent en effet ruiner la belle théorie. Parfois celles-ci sont accidentelles, d'autres sont mises en place volontairement à la demande des « services » pour leur permettre de contourner le recours aux essais systématiques aujourd'hui impraticables. Un document recueilli suite à une erreur monumentale de transmission d'une célèbre firme montre à quel point nous pouvons faire confiance à cette production venue d'outre Atlantique.

De fait, peu après cette libéralisation lors d'une réunion des SR à Washington, le patron

de la NSA en entamant la réunion s'exclama : « Et maintenant que la France a renoncé que faisons-nous ? » Un grand silence s'en suivit. Je tins tout de même à répondre que je les avais tous prévenus et que si les autres pays ne s'étaient pas contentés d'attendre pour voir mais qu'ils avaient soutenu notre initiative, nous n'en serions pas là !
Quant à ce qu'il fallait faire, c'était simple : il suffisait de remettre au goût du jour les vieilles coutumes de connivence avec les industriels de l'informatique et les grands éditeurs de logiciels pour conserver cette fameuse maîtrise de l'information sans plus se soucier de légalité comme avaient tenté de le faire les initiatives Clinton et la nôtre.
À la différence près qu'une politique fondée sur le droit et la transparence mettait à égalité tous les pays tandis qu'une solution basée sur les relations occultes avec les industriels ne favorisait que les pays sur le sol desquels se trouvaient ces industriels.

À ce petit jeu facile à comprendre mais que n'avaient pas voulu voire nos politiques ou au contraire qu'avaient parfaitement saisi certains politiques, la Justice française n'était pas gagnante. Même la Ligue des droits de l'homme s'en était émue, qui avait demandé dans un tract que le SCSSI soit chargé de labelliser les produits de sécurité qui inondaient le marché sans aucune garantie de qualité…

Et survint le 11 septembre…

En France on en était encore à afficher le plus ostensiblement possible le mot liberté dans la nouvelle loi en préparation quand s'effondrèrent les tours du World Trade Center. Dès lors l'exercice devint plus difficile car tout en continuant à afficher ce principe, ceux qui avaient poussé à la libéralisation se mirent à ramer en sens inverse.
Mais comment retrouver le clair des communications des terroristes quand on a permis à tout un chacun de dissimuler ses échanges ?

Il faut dire que les services américains qui n'avaient rien vu venir suspectèrent immédiatement l'existence d'un système cryptographique perfectionné d'Al-Quaïda qui avait masqué les préparatifs de cet effroyable attentat. Même ce bon Philippe Zimmermann eut un moment de frayeur en envisageant que son si sympathique Pretty Good Privacy avait pu servir une si ignoble cause. Avant de se ressaisir toutefois quand il fut émis l'idée que l'organisation avait probablement utilisé un système de stéganographie. Il put alors reproclamer son attachement à la liberté de crypter sans être jeté en prison.

Après l'euphorie de la fin des années quatre-vingt-dix qui avaient vu l'explosion du Net et l'annonce de son cortège de bienfaits, le 11 septembre puis l'éclatement de la fameuse bulle gonflée à l'argent virtuel, firent regarder d'un autre œil le réseau des réseaux. Celui-ci commença à soulever toutes les inquiétudes que l'on avait volontairement occultées : l'Internet, comme toute nouvelle technologie, pouvait (comme c'est étrange !) être détourné à des fins délictueuses et criminelles… Il n'était plus politiquement incorrect de le dire. Les enfants étaient en danger, nos comptes en banque étaient menacés, la désinformation régnait, Al-Quaïda pouvait refrapper, bref, il fallait nous protéger. Là on ne lésina plus sur les moyens.

De l'autre côté de l'Atlantique les mouvements traditionnellement réputés pour défendre les libertés se crurent obligées de se résoudre au silence, tout le monde vota le Patriot act.

Les firmes ressortirent avec délectation leurs concepts anti piratage permettant de contrôler de fait tous les ordinateurs avec par exemple les fameuses puces dites Fritz du nom du sénateur qui en fit la promotion.
En France ce fut la loi pour la sécurité quotidienne suivie d'une kyrielle d'autres dispositions toutes plus liberticides les unes que les autres, jusqu'aux deux dernières HADOPI et LOPPSI. Cette dernière autorisant les services spécialisés à utiliser des spywares, ces logiciels espions qui permettent de prendre la main sur votre ordinateur et récupérer vos données.
Rétrospectivement les quelques journalistes braillards qui s'étaient opposés jadis aux tiers de confiance doivent se dire que finalement, c'était le bon temps!

Mais d'un point de vue sécuritaire où en sommes nous? L'utilisation de la cryptologie est affichée comme étant libre mais les moyens cryptologiques sont désormais des standards parfaitement connus et nous avons vu que leur efficacité n'est réelle que dans un environnement de confiance difficile à trouver aujourd'hui. Même les services gouvernementaux sont vulnérables.

Les substituts à la politique des tiers de confiance sont peu crédibles et dangereux.
D'abord dans la nouvelle loi (LCEN 2004) on demande au suspect de fournir le clair ou les clefs de ce que l'on a saisi sur son ordinateur ou des communications interceptées sous peine d'aggravation de la sanction. Or:

1 la jurisprudence de la cour européenne des droits de l'homme fait qu'on ne peut obliger un prévenu à fournir la corde qui doit le pendre.
2 Je me souviens d'une certaine affaire qui a défrayé la chronique dans laquelle une fameuse cassette a été vainement recherchée chez un protagoniste d'une haute pointure. « Une cassette? Quelle cassette? ».
3 Il est la plupart du temps impossible techniquement au particulier de fournir ces éléments.

Ensuite il est précisé que le juge peut faire appel à des moyens de l'État couverts par le secret de Défense pour retrouver le clair d'un cryptogramme. Ainsi serait-il possible, dans un contexte où la démocratie aurait quelque peu reculé, que l'on puisse fabriquer de fausses pièces à conviction comme dans le cas de l'affaire Dreyfus, sans avoir à faire la preuve de la relation biunivoque entre le clair et le cryptogramme.
Il est donc difficile de mon point de vue de voir dans cette évolution de la réglementation sur la cryptologie un progrès de la démocratie.

Mais comme j'espère vous l'avoir montré la bataille autour de la libéralisation de la cryptologie n'a été qu'un écran de fumée. La véritable maîtrise de l'information passe par le maintien d'outils informatiques séduisants mais imparfaits comportant les portes dérobées nécessaires à l'action des services de sécurité qui ne vont pas s'embêter avec des tâches de décryptement. Comme le monde des internautes regorge de talents qui en découvrent chaque semaine, il est sans doute nécessaire d'en prévoir une bonne provision. C'est sans doute pour cela qu'un grand éditeur s'attache à nous fournir des produits qui en sont truffés.

La cryptologie, bien qu'on l'ait occulté le plus souvent, a joué un rôle immense au cours de l'Histoire et plus particulièrement au XX^{e} siècle.
Intégrée désormais dans ce qu'il est convenu d'appeler la sécurité des systèmes d'information, elle continue à revêtir une importance capitale car elle est à la base de tous les mécanismes garantissant des droits d'accès physiques ou logiques et la sécurité des transactions électroniques de tous types.
Elle constitue un discriminant entre les pays et peut, comme elle l'a toujours fait, procurer un avantage déterminant à celui qui la domine en particulier sur ce nouveau champ de bataille que constitue le cyber espace.
Si à certains moments on a pu croire que la cuirasse l'avait définitivement emporté sur l'épée parce que la force des algorithmes mathématiques apparaissait infinie, il n'en est rien, de nouvelles vulnérabilités souvent liées aux technologies employées pour les mettre en œuvre apparaissent périodiquement, perpétuant le combat. Même la cryptologie quantique qui était qualifiée il y a peu de Graal fait déjà l'objet de publication prétendant la contourner.
Cela ne doit pas être fait pour déplaire aux chercheurs pour lesquels rien ne serait plus ennuyeux qu'un monde de certitudes.

Je vous remercie de votre attention.