http://www.huyghe.fr

Histoire de la cryptologie

"Il voit sans être vu,
Entend sans être entendu
Il connaît sans être deviné..
Il masque ses traces,
Brouille ses pistes,
Nul ne remonte à lui"

Tel est le souverain idéal, selon le philosophe Han-Fei, auteur du *Tao du Prince*, un classique de la pensée politique chinoise, il y a vingt trois siècles. Ce maître silencieux doit il pénétrer toutes les arcanes des codes et des cryptogrammes ? La chronique chinoise mentionne force histoires de messages secrets. Parmi les ruses que l'on enseignait aux apprentis stratèges, voici un moyen éprouvé : envoyez quelque agent maladroit dans le camp ennemi de façon qu'il soit pris. Sans aucun doute, on ne manquera pas de le torturer et de vérifier s'il n'a pas avalé un message caché dans une boule de cire, procédé courant à l'époque des Han. Prévoyant cela, vous lui aurez fait transporter une fausse lettre qui fera croire que le meilleur général ou le plus fidèle conseiller du souverain ennemi s'est rallié à vous. Bientôt sa tête volera. Par ce stratagème vous vous serez débarrassé d'un adversaire.

Comme en écho, Kautylia, le Machiavel indien de la fin du IVe siècle avant notre ère, ministre du grand roi Ghandragupta et auteur d'un des premiers traités du gouvernement, conseille au Prince de se doter d'un solide service de renseignement et de faire déchiffrer les "écritures secrètes". Cela prouve qu'il devait bien y avoir des espions et conspirateurs qui utilisaient la cryptographie pour dissimuler leurs messages et des spécialistes de la cryptanalyse qui savaient en briser le chiffre. D'autres textes laissent soupçonner que la science du code secret était alors fort développée. le Kama Sutra mentionne l'art l'écriture secrète au nombre des soixante-quatre disciplines que doit maîtriser la parfaite concubine.

Les Indiens, les Chinois ? Qui a inventé le premier code secret ? Les scribes égyptiens qui, il y a quatre mille ans, parsemèrent les inscriptions à la gloire de leurs maîtres défunts de nouveaux hiéroglyphes, compréhensibles des seuls initiés ? Était-ce pour dissimuler l'emplacement de quelque trésor funéraire, ou simplement graphique, pour intriguer le lecteur ? Des tablettes chiffrées en écriture cunéiformes trouvées en Mésopotamie, indiqueraient-elles une science du code sophistiquée ? Les archéologues hésitent.

Cacher les choses, cacher les mots

Par contre, nul ne doute que les Grecs n'aient rivalisé d'ingéniosité pour dissimuler leurs correspondances stratégiques. Dès le V° siècle avant notre ère, les Spartiates employaient le scytale. C'est un simple bâton autour duquel on enroule en spirale un ruban de cuir ou de papyrus. Puis on écrit dans le sens de la longueur. Une fois le ruban défait, il est donc impossible de reconstituer l'ordre des lettres, sans posséder de scytale ou du moins, sans en connaître le diamètre. Il existait d'autres procédés. Ainsi des trous minuscules dans un manuscrit permettaient au correspondant averti de noter les lettres ainsi marquées et de reconstituer le message. Ou encore, on tatoue le

message sur le crâne rasé d'un messager, puis on attend que ses cheveux repoussent. Le destinataire averti du procédé fait raser le crâne du messager et lit le texte. Surprenant, mais long, ce procédé est rapporté par Hérodote. Ou encore grâce auquel un exilé grec prévint ses compatriotes des projets d'invasion de Xerxès : il grava son message sur le bois d'une tablette qu'il recouvrit de cire et qu'il expédia, ainsi apparemment vierge à ses amis de Sparte.

Polybe aurait inventé au cours du second siècle avant notre ère un système de codage lettre par lettre. Les 25 lettres de l'alphabet grec sont rangées en carrés de cinq sur cinq et chacune est désignée par deux chiffres : celui de sa rangée et celui de sa colonne. Ce procédé permet à la fois de coder le message et de le transmettre à distance par un système de signaux lumineux : deux jeux de cinq torches agitées de façon convenue suffisent à désigner toutes les cases, donc toutes les lettres existantes.

Quant aux Romains, s'ils ne possèdent que des systèmes cryptographiques simples, ils en sont grands utilisateurs. Outre les messages stratégiques qui parcourent tout l'Empire, la correspondance privée, généralement confiée à des esclaves particuliers, représente un trafic important ; il importe donc d'en assurer la confidentialité. Les patriciens se méfient de leurs serviteurs indiscrets ou des rivaux politiques qui pourraient s'emparer de leur correspondance ; les généraux craignent que leurs estafettes soient arrêtées en route. Il faut donc coder. César écrit en employant un système de substitution relativement rustique. À chaque lettre est substituée celle qui se trouve trois lettres plus loin dans l'alphabet : le A devient D, le B se change en E, etc... De la même façon, on trouve dans la Bible un système dit "Atbash" qui consiste à remplacer la première lettre de l'alphabet par la dernière, la seconde par l'avant-dernière, et ainsi de suite.

Ce sont les premiers principes de la cryptographie. De la cryptographie et de la stéganographie, pour être exact, puisque, si le premier mot désigne la science qui vise à rendre un message incompréhensible, le second est l'art de cacher physiquement ce message. Généralement, cela consiste à en camoufler le support matériel ou à le cacher en le plaçant à un endroit insoupçonnable. Les encres sympathiques qui ne se révèlent qu'à la chaleur, les parchemins dissimulés dans un bâton creux, les boulettes avalées ou les crânes tatoués ressortent à la stéganographie comme les alphabets secrets sont des procédés de cryptologie.

Il n'y a pas mille façons de réserver les messages à leurs seuls destinataires. Il faut, ou bien, employer un procédé physique et rendre la chose imperceptible, ou bien on doit recourir à un processus sémantique et obscurcir le sens. Et si l'on choisit la seconde voie, il se dessine deux grandes options : ou bien remplacer un élément du message clair (une lettre, un mot) par un substitut convenu entre l'émetteur et le récepteur (une autre lettre, un autre mot, mais aussi, un dessin, un symbole, une note de musique, un geste...) ou bien changer l'ordre des éléments composant le message (là encore, qu'il s'agisse de phrases, de mots, de lettres ou de bits informatiques). Tous les écoliers qui, pour préserver leurs secrets ont caché des boules de papiers dans des crayons à bille, employé des chiffres au lieu de lettres ou parlé un quelconque verlan n'ont jamais fait que redécouvrir ces trois principes : dissimuler, substituer, transposer. Ajoutons que l'on peut combiner les procédés (tel est le cas d'un microfilm portant un texte codé). Et qu'il existe des systèmes difficiles à classer. Ainsi, le mathématicien, médecin et encyclopédiste du XVIe siècle, Jérôme Cardan invente, entre autres procédés, une grille trouée. Le message est écrit dans les emplacements libres, la grille retirée et tous les autres espaces de la feuille remplis de lettres n'ayant aucune signification. Contrairement au procédé habituel qui consiste à dissimuler l'existence même du message, Cardan imagine donc de laisser le significatif visible mais indiscernable du

"fond". C'est déjà le principe de la lettre volée d'Edgar Poe : laisser visible ce que l'on veut cacher.

Il faudra donc attendre la technologie moderne de la miniaturisation pour faire des progrès en ce domaine. Le principe du microfilm cher aux romans d'espionnage de la Guerre Froide, toujours plus petit, va-t-il retrouver une nouvelle jeunesse avec Internet ? En permettant d'expédier des images d'excellente qualité via le courrier électronique. La Toile devient, dit-on, le support préféré des correspondances secrète de la mafia russe : il suffit d'insérer son message dans un micropoint de la photographie que l'on numérise et que l'on expédie. Malgré leur ingéniosité, de tels procédés restent lourds (ne serait-ce que par le matériel qu'il requièrent) et peu sûrs : ils ne valent plus rien une fois que l'adversaire a compris le principe de la cachette. Aussi le génie humain s'est il bien davantage exercé dans l'art de cacher le sens. Le duel séculaire des cryptographes, inventeurs de chiffres et clefs, contre les cryptanalystes, briseurs de sceaux et décrypteurs de mystères, fait paraître terriblement primaires ces histoires d'écritures invisibles ou de James Bond attardés. La cryptologie est donc la voie royale : en elle, le principe du secret, alternance de défenses et de viols, trouve sa plus haute expression.

Quelles sont les armes de chacun ? Le cryptologue, est l'homme qui complique. Prévisibilité, similitude, régularité sont ses ennemies. Il lui faut d'abord trouver un principe surprenant : si son adversaire pouvait trop facilement reconstituer sa démarche mentale, l'affaire s'arrêterait vite. Remplacer une lettre par la suivante dans l'alphabet ou retransposer en colonnes verticales les lettres qui ont été écrites à l'horizontale est à peu près aussi original que de choisir sa date de naissance comme combinaison de son coffre fort. Il faut ensuite que le chiffré ressemble le moins possible au clair, et à la langue naturelle, y compris dans sa structure : si dans un texte codé en français on rencontre souvent deux ou trois lettres séparées par un espace d'une série de lettre plus longues, on peut parier sans trop de risque que l'on est en présence de la version codée de l'article (*le*, ou *la*, ou *un* pour deux lettres, *les*, *une* ou *des* pour trois...) ou de pronoms. Enfin, le cryptographe doit éviter qu'il existe le moindre rapport statistique entre clair et codé : la fréquence d'un signe dans le second laisse facilement soupçonner celle d'une lettre dans la langue naturelle. On sait ainsi que le E, puis le S, puis le A, puis le R et ainsi de suite ...sont les lettres les plus fréquentes de notre langue. Bref, le cryptographe, faiseurs d'énigme, est un curieux artiste dont l'œuvre doit imiter le hasard : elle est d'autant plus ordonnée qu'elle semble aléatoire, d'autant plus pensée qu'elle paraît n'obéir à aucune règle. Mais il souffre d'un handicap toute langue est redondante : elle emploie bien plus de signes qu'il ne serait nécessaire d'un point de vue strictement mathématique pour exprimer une information. Ce qui la rend extrêmement prédictible : quelques lettres d'un mot ("bonj.. Mons..") nous suffisent à compléter le sens. Ces notions auxquelles la théorie de l'information et la cybernétique ont donné des noms plus précis (entropie, redondance, etc...) et des formulations mathématiques ont été découvertes intuitivement par le cryptologue depuis quelques siècles.

Face à lui, le cryptanalyste semble d'abord bien dépourvu : chercher la fréquence des lettres, imaginer les mots dont l'apparition est probable, tenter de détecter des régularités et surtout procéder inlassablement par essais et erreurs, telles sont ses pauvres recettes. Ce sont à peu près celles que l'on trouvera dans un ouvrage arabe de 855 le "*Livre de la connaissance longuement désirée des alphabets occultes enfin dévoilés*", premier traité de cryptanalyse connu. Ce sont aussi les procédés, romanesques par excellence, dont s'inspire la littérature.

Edgar Poe, lui-même bon cryptanalyste s'amusait à défier les lecteurs d'un journal où il tenait une chronique de lui envoyer des messages codés qu'il ne sache déchiffrer. Dans

sa nouvelle *Le scarabée d'or*, il décrit la façon de déchiffrer le message indiquant l'emplacement du trésor d'un pirate. Sherlock Holmes, Arsène Lupin, des héros de romans de Jules Verne et probablement quelques dizaines de détectives de romans policiers que nous n'avons pas lus procèdent de la même manière : face à un message chiffré, ils cherchent une lettre ou un mot probable, vérifient, en déduisent un second puis un troisième, remplissent les blancs et finalement comprennent le sens global. Dans les romans de telles techniques appliquées à des messages brefs sont rapidement démontrées en quelques lignes.

Les casseurs de codes

Dans la réalité, les choses se déroulent à une autre échelle : les casseurs de code travaillant pendant des journées, souvent par équipes entières et sur des textes très longs, ce qui facilite le décryptage. Mais dans la réalité comme dans la fiction, il n'y a jusqu'à une époque récente que deux façons de déchiffrer : empiriquement par essais et erreur, logiquement en tentant de comprendre l'algorithme de chiffrement, c'est-à-dire l'ordre logique des opérations de substitution ou de transposition qui composent le chiffrement.

En bonne logique, il semblerait que le chiffreur doive toujours l'emporter. Imaginons un cas extrême : le chiffreur idéal changerait de système de codage à chaque lettre, puisant chaque fois dans un répertoire différent de telle sorte que le cryptanalyste ne puisse détecter aucune régularité ni déduire aucune règle. Et quand bien même, il disposerait d'un temps infini et essayerait tous les sens possibles d'un message codé de x lettres ou éléments, il aurait le choix entre tous les messages possibles composés de x lettres ou éléments, comme dans la nouvelle de Borgés "la bibliothèque de Babel" où les livres sont composés de toutes les combinaisons possibles des lettres de l'alphabet. Pour emprunter une autre image célèbre à l'écrivain argentin, la carte (le système de représentation) serait alors aussi grande que le territoire (le représentable). Mais dans le monde réel, la carte ne recouvre jamais le territoire. Nous sommes incapables de mémoriser un nombre de codes aussi long. Il faut donc soit que le codeur limite la complication des opérations auxquels il aura recours à des procédés transmissibles de vive voix (donc relativement simples) soit qu'il recoure à un support de mémoire comme un livre de code. Il vient alors de tomber de Charybde en Sylla, puisque le point faible de son système est qu'il doit le transmettre au destinataire et qu'un tel texte en clair peut être dérobé, falsifié, copié, perdu... Le cryptogramme parfait existe donc : il suppose un texte de référence commun à l'émetteur et au récepteur auquel chaque texte codé renvoie lettre par lettre (par exemple ayant besoin d'écrire la lettre *a,* j'indique que le livre convenu la contient à telle page, telle ligne, tel rang, puis je procède de même pour chaque lettre ainsi repérée par son emplacement). Cela équivaut à changer de code à chaque lettre puisque la relation entre la lettre claire et son équivalent codé, totalement arbitraire: elle repose sur un emplacement, non sur une signification.

Mais un tel système n'est pas adaptable aux besoins d'une correspondance diplomatique ou militaire, ni à un usage fréquent. Les complications que doit susciter le cryptographe sont limitées par des considérations pratiques, celles d'une bureaucratie du secret. Voici donc le cryptanalyste qui retrouve toutes ses chances, comme le confirme l'histoire.

"Qui ne sait pas dissimuler ne sait pas régner" enseignait Louis XI à son fils, annonçant les conseil de Machiavel au Prince. La Renaissance a le goût des complots,

de l'occultisme et des inventions, trois raisons pour que l'art des écritures secrètes s'y développe et attire de fortes personnalités. Ainsi, le grand architecte et mathématicien Leon Batista Alberti mort en 1472 invente le principe de la machine à coder, déléguant en quelque sorte la tâche de tout compliquer à un système de deux disques rotatifs portant les lettres de l'alphabet en faisant varier leur position on obtient donc divers alphabets de correspondance. Du coup, il suffit de convenir d'une lettre indice ("je mettrai x en face de a") ou d'une suite d'opérations ("je mettrai x en face de a, puis, toutes les fois que j'introduirai tel signe dans mon message, je tournerai le disque interne d'un cran à droite..."). Cette intuition géniale ne sera guère dépassée avant l'informatique, au moins en son principe. Du coup, Alberti a aussi inventé le principe de coder le codage, c'est-à-dire de convenir de l'ordre d'utilisation d'une pluralité de codes. L'idée de clef, un message généralement facile à retenir et qui dit comment disposer sa batterie de répertoires est là en puissance.

En comparaison, on est presque déçu par l'écriture inversée "alla mancina" de Léonard de Vinci, qui se lit dans un miroir, ou le code du chancelier et philosophe Francis Bacon, grâce auquel il aurait avoué, ont prétendu des historiens imaginatifs, qu'il était en réalité l'auteur des pièces de Shakespeare.

D'autres cryptologues moins illustres accomplissent des exploits remarquables. François Viète, qui brise les codes de Philippe II d'Espagne pour le compte d'Henri IV dont il est conseiller privé se voit accusé de sorcellerie par les Espagnols. Mais Viète invente aussi l'algèbre moderne. Le Milanais Jérôme Cardan mort en 1576 féru d'astrologie et parfois en délicatesse avec l'Inquisition, imagine un procédé où le message contient sa propre clé ; c'est aussi un remarquable mathématicien, il est le premier à résoudre des équations du troisième degré et il a l'intuition du calcul des probabilités. Les exemples abondent au XVIe siècle de ces cryptologues partagés entre leur goût des mathématiques et leur attirance pour l'occulte. Trithème, abbé de Wurzbourg auteur du premier livre de cryptologie imprimé est un fou de Kabbale et de magie. Blaise de Vignère qui résume toutes les connaissances de l'époque dans son "*Traité des chiffres ou secrètes manières d'écrire*" de 1596 est kabbaliste et alchimiste.... Parmi les systèmes de codage qu'il imagine, il en est un, dit "carré de Vignère" réputé inviolable presque jusqu'à la première guerre mondiale. Réputée seulement car, au début du XIXe siècle, car Charles Babbage a déjà réalisé cet exploit mais sans en rien publier. Plus étonnant encore : pour casser le chiffre de Vignère, Babbage a posé le principe d'une machine analytique à résoudre les problèmes en les subdivisant en opérations simples, principe d'où sort toute l'informatique.

Au XVI et XVIIe siècles, les spécialistes du chiffre sont de plus en plus recherchés et deviennent des sortes de consultants internationaux engagés par telle ou telle cour voire par le Saint Siège. Un expert étranger au service d'Élisabeth d'Angleterre Henry Phelipes déchiffre les messages secrets qu'échangent Marie Stuart de sa geôle et Babington qui conspire de l'extérieur pour la délivrer. Les deux malheureux ont confié leur correspondance à un agent provocateur infiltré dans la conspiration. Phelipes casse très vite leur code ; aucun de leurs mouvements n'échappe à leurs ennemis. Pire : Phillipes fabrique même de faux messages de Mary Stuart demandant les noms des six gentilshommes complices de Babbington. La conspiration une fois démantelée, les lettres codées où la prisonnière donne son assentiment au complot contre Élisabeth b servent de preuves devant le tribunal. Et c'est finalement la faiblesse de son chiffre qui coûtera sa tête à la malheureuse écossaise. Ironie de l'histoire : un autre cryptologue, John Wallis considéré comme le plus illustre précurseur d'Isaac Newton, contribuera à l'exécution de Charles I° en 1649. En effet Wallis qui s'est mis au service de Cromwell déchiffre plusieurs dépêches du roi à ses partisans et participe ainsi à leur défaite. Peu vindicatif, Charles II engagera plus tard ce brillant mathématicien.

Longtemps la cryptologie est affaire d'hommes d'exception ou de lignées. La charge se transmet souvent héréditairement et il y a ainsi des dynasties d'Argenti à Rome, de Wallis en Angleterre ou de Rossignol en France qui ont accès aux affaires les plus secrètes ; ils sont fort bien payés et comblés d'honneurs. Le déchiffrement est aussi affaire d'organisation et de moyens. Après Louis XIV qui avait compris l'importance de la cryptologie, suivant l'exemple du fameux Cabinet Noir français, l'Europe se couvre de bureaux du chiffre chargés de décrypter toutes les correspondances secrètes, travaillant en équipes polyglottes, accumulant des connaissances, perfectionnant des méthodes, examinant des centaines de lettres de particuliers ou de diplomates recopiées ou détournées par des dizaines d'agents. Avec l'absolutisme, avec la naissance de l'État moderne, le secret se révèle au cœur du politique. Foin des histoires d'amants ou d'alchimistes, le code est administré, géré, défendu par des corps de spécialistes : il est devenu la technique essentielle de lutte par l'information.

Survient une révolution : le télégraphe. Pour la première fois de l'histoire de l'humanité, une parole va plus vite qu'un homme à cheval, un ordre est reçu instantanément, un territoire se contrôle d'un point unique. La transmission se libère du transport et promet une nouvelle maîtrise du temps et de l'espace. Arme de guerre d'abord, outil de l'État ensuite et finalement instrument au service de l'économie, le télégraphe entretient un rapport singulier avec le la cryptologie. Il n'est d'abord que code puisque le télégraphe de Chiappe fonctionne d'abord sur le principe de signaux optiques conventionnels (d'où l'importance de réserver à des agents sûrs la connaissance du code). On se souvient comment dans le roman d'Alexandre Dumas, le comte de Monte Cristo se venge d'un banquier : il soudoie un agent du télégraphe et fait parvenir à Paris une fausse nouvelle qui provoque la ruine de son ennemi. Même avec l'invention du télégraphe par fil et du Morse, le télégraphe paie son économie de moyens, son indépendance du facteur humain et son instantanéité d'une incertitude : sans code efficace, comment savoir si le message n'a pas été écouté par l'ennemi ou, notion dont on ne saisit pas encore l'importance, s'il est bien authentique et émane de l'ami ?

Les machines à secrets

Avec la guerre de Sécession américaine, les militaires comprennent combien, autant que le train le télégraphe décide du sort de la guerre. À l'évidence l'armée du futur emploiera quotidiennement le code et devra en confier l'usage à des corps d'armées éloignés, bientôt à des éléments isolés, bref à de nombreux utilisateurs quotidiens. Un curieux personnage, grand partisan du volapük comme langage universel, le hollandais Auguste Kerkhoffs tire bien les conséquences de cette mutation dans un livre de 1883 Cryptographie militaire. Le système idéal de chiffrement, démontre-t-il, devra être non seulement sûr, portatif, d'usage aisé, rapide, adaptable au télégraphe, pouvoir tomber sans inconvénient entre les mains de l'ennemi etc.. et surtout sa clef devra être modifiable et transmissible sans recours à un support écrit. Bref il ne suffit pas d'une serrure inviolable, il faut aussi une clef transportable. À l'âge de la machine, la réponse s'impose avec évidence : une machine, une vraie matrice à secrets, inviolable, mais accessible à qui possède le sésame: un mot, quelques lettres. Les idées d'Alberti retrouvent une actualité et on voit apparaître des machines à crypter dès l'Exposition Universelle de 1867. Mais la machine est longue à triompher : les États se dotent longtemps de répertoires de codes, mots clefs, mots d'ordres, procédures qu'ils dispersent dans leurs corps d'armée et leurs ambassades. Répandu à une telle échelle, avec les simplifications inhérentes à son utilisation quotidienne le code est fragile tandis que les instruments de la cryptanalyse, notamment l'analyse statistique du

langage progressent. Espionnage et contre-espionnage pratiquent le déchiffrement, l'écoute, l'infiltration, l'intoxication à une échelle nouvelle.

Tout se complique : car percer un secret est une chose, l'avouer en est une autre. La connaissance acquise par déchiffrement d'une correspondance dérobée n'est pas utilisable sans précaution : a-t-on été intoxiqué ? comment utiliser les informations acquises sans perdre ou sa source ou sa crédibilité ? Ainsi, dans l'affaire Dreyfus, un télégramme chiffré joue un rôle de premier plan. Nos services s'emparent en 1894 d'un télégramme de l'ambassadeur d'Italie Panizzardi qui tend à établir l'innocence de Dreyfus. Mais comment être certains de n'avoir pas été abusé par un leurre? Les cryptologues du quai d'Orsay demandent une vérification. Pour cela, on fournit délibérément des informations militaires à Panizzardi, sachant qu'il ne manquera pas de les retransmettre à son gouvernement sous forme de télégramme chiffré. Ce qu'il fait : du coup, les services français peuvent confirmer le premier message. Mais c'est finalement une version truquée du télégramme, accablant Dreyfus, qui circulera dans la presse, au moins jusqu'à la révision de son procès. Preuve que le jeu de la désinformation, peut annuler l'efficacité de l'information acquise par déchiffrement. Il ne suffit pas de savoir, il faut savoir comment faire savoir.

Cette loi se voit confirmée lors d'un épisode décisif de la première guerre mondiale : l'affaire du télégramme Zimmermann, du nom du ministre allemand des Affaires Étrangères. Après que des sous-marins allemands aient coulé le Lusitania en 1915, tuant ainsi un millier de passagers dont plus de cent américains, l'intervention aux côtés des Alliés gagne des partisans aux U.S.A. Par ailleurs l'État Major du Kaiser veut intensifier la guerre sous-marine pour mettre au plus vite l'Angleterre à genoux, donc sans doute couler d'autres navires américains. Une confrontation semble plus que vraisemblable. Dans cette hypothèse, Zimmermann prévoit un plan de secours destiné à gêner Washington dans son effort de guerre. Ce sera un second front : une alliance avec le Mexique à qui il promet le Texas et le Nouveau-Mexique en cas de conflit. Tel est le contenu du fameux télégramme chiffré envoyé à l'ambassadeur d'Allemagne à Washington pour qu'il transmette la proposition à Mexico. Le bureau du chiffre de la marine américaine parvient à le déchiffrer à grand peine. Mais se référer publiquement à ce document ce serait faire savoir à l'ennemi éventuel, l'Allemagne, que son meilleur code doit être changé et se priver d'une arme pour le conflit à venir. Il faudra donc trouver une version avouable de ce document. Les services secrets attendent donc de disposer de la version mexicaine du télégramme, saisie grâce à un agent américain au télégraphe de Mexico, pour livrer à la presse le texte qui entraîne le président Wilson à déclarer la guerre.

Ce succès marque le début d'une époque où les cryptanalystes anglo-saxons et alliés jouiront d'une supériorité indiscutable sur les allemands et les japonais. Pendant la seconde guerre mondiale, cette capacité de savoir sans être écouté joue un rôle décisif. Mais, là encore, il ne suffit pas qu'une information soit disponible, encore faut-il qu'elle soit crue et utilisée. On a échafaudé toutes sortes d'hypothèse sur l'étrange manque de réaction américain aux signaux d'une prochaine attaqua nippone contre Pearl Harbour : pourquoi par exemple, l'exemplaire de la très performante machine à décrypter les codes japonais qui était à la base de Pearl Harbour en est il retiré en Novembre 1941 ? Alors que les Américains ont déchiffré plus vite que les japonais eux-mêmes télégramme enjoignant à l'ambassade du Japon à Washington de transmettre une déclaration de guerre, le lendemain, jour de l'attaque, pourquoi la base est elle prévenue trop tard ? De nombreux indices avaient été rassemblés grâce au déchiffrement du chiffre japonais. Apathie bureaucratique face à un danger pourtant évident ou provocation délibérée ?

Les historiens n'ont pas encore tranché, mais aucun ne doute de la supériorité du renseignement américain sur les Japonais. Pendant la guerre du Pacifique, cette supériorité est renforcée par un procédé surprenant. Pour ses communications radios, l'U.S. Army fait souvent appel à des indiens navajos. La langue navajo n'a pas d'écriture, les ethnologues étrangers ne l'ont pas étudiée et on ne chasse guère le bison du côté de Tokyo, trois raisons de croire que cette langue serait aussi impénétrable aux services nippons que l'étaient les hiéroglyphes avant la découverte de la pierre de Rosette. Après avoir la résolution quelques difficultés sémantiques (comment dire "bombardier" ou "sous-marin" en navajo ? Il suffit de trouver une jolie métaphore comme "buse" ou "poisson de fer".), le système se révéla parfaitement fiable.

Le vrai défi pour les cryptanalystes venait d'Allemagne où dès 1918 les ingénieurs se sont lancés dans la quête de la machine à crypter parfaite, qui sera, époque oblige, naturellement électrique. Bientôt ce sera la fameuse machine Enigma dont le principe peut être résumé ainsi : un jeu de rotors mobiles dont les différentes positions convenues par message codé entre les correspondants. Incroyablement compliquée par le nombre de combinaisons (donc les manières de chiffrer le même texte) qu'elle permet, la machine est pourtant d'un usage enfantin : une fois qu'elle est réglée on tape son texte clair sur un clavier et les lettres chiffrées correspondantes apparaissent à l'instant. Est-ce la machine parfaite ? Ayant appris à quel point leur code était connu des Anglais (et ceci, ironiquement, par des confidences de Churchill dans un livre de souvenirs publié en 1923), les Allemands s'équipent à grande échelle avec Enigma. Ils décident de procédures sécurisées pour les changements de réglage. L'idée est que le temps qu'un unique message soit décrypté, les réglages des Enigma auraient changé et tout serait à refaire. Certains d'être toujours en avance, les Allemands croyaient gagner la guerre du code comme la guerre des tanks, par la blitzkrieg. L'introduction du facteur temps semble condamner le cryptanalyste le plus doué à un travail de Sysiphe. Pour résoudre cette question les alliés vont devoir rassembler une énorme puissance intellectuelle, des dizaines de surdoués des mathématiques, de la linguistique, de la philosophie, de l'espionnage mais aussi du bridge ou des mots croisés (ces derniers ayant été recrutés par un concours pour cruciverbistes dans les journaux).

Machines qui pensent et machines qui travaillent

Outre la matière grise pour vaincre Enigma, il faudra mécaniser l'abstraction et inventer les machines qui pensent pour vaincre les machines qui brouillent. Si bien que l'informatique moderne est sinon fille de la cryptologie, du moins lui est redevable de quelques uns de ses concepts principaux. À preuve deux de ses "pères" officiels ont élaboré leurs principales idées en travaillant directement sur le problème du code : le logicien Türing inventeur de la :machine "à computer" et Shannon, fondateur de la théorie de la communication. Et si le troisième père, le mathématicien Wiener n'a pas contribué à la lutte contre Enigma, il s'est tenu au courant de ces travaux.

Rien n'aurait été possible sans les travaux de quelques pionniers des services secrets polonais. Dès avant-guerre ils s'étaient attaqués à Emigma et avaient imaginé des pools de machines travaillant de façon coordonnée faire dans un temps raisonnable une série d'essais et erreurs qu'aucune équipe de chercheurs n'aurait réalisée dans le même temps. Ce n'étaient pas encore des ordinateurs programmables, mais c'était déjà un pas gigantesque dans cette direction. Ces machines baptisées "bombes" en raison de leur tic-tac bruyant parviennent aux alliés après l'invasion de la Pologne.

Très tôt, les Anglais installent à Bletchey Park un service du chiffre d'une centaine de personnes qui travaille à l'opération dite "Ultra" : casser le code d'Enigma. Dès 1940 des "bombes" britanniques tournent inlassablement, mais cette fois ce sont des modèles perfectionnés par le génial Turing qui a réussi à éliminer un nombre considérable d'opérations inutiles, par pur raisonnement sur les hypothèses impossibles. Mais les bombes ne sont pas les fameuses machines de Turing (qui d'ailleurs n'existèrent que sur le papier), à savoir des dispositifs mécaniques programmables qui résolvent des problèmes divisés en une multitude d'alternatives 1 ou 0. Enigma est vaincue et aucun historien ne doute que le sort de la guerre ne se soit joué en grande partie à Bletchey Park.

Entre-temps le premier "vrai" ordinateur apparaît : une machine électronique universelle programmable, Colossus Mark II, couronnement de l'intuition de Türing fonctionne en mai 44. Cet énorme amas de tubes et de fils toujours en panne avait des performances très inférieures à celles d'une calculette d'enfant d'aujourd'hui, mais l'informatique était née, en grande partie de la cryptographie.

Technologies du secret

Désormais, avec l'informatique le code va devenir un enjeu majeur de la vie quotidienne. Il se trouve au cœur de deux changements technologiques : le numérique et les réseaux. Le numérique, d'abord : la transformation de toute information (lettre, son, image, programme, etc...) en suites de 0 et de 1, en bits, octets et kilo octets informatiques modifie la règle du codage. Il s'agira désormais d'inventer des algorithmes que l'on pourrait décrire métaphoriquement comme des recettes pour brouiller les suites de 0 et de 1 (et non plus changer des lettres ou groupes de lettres d'une manière convenue). Il s'agit donc de haute technologie, donnant lieu à des brevets : un algorithme, ou un système de chiffrement vaudra se que vaudra sa résistance aux tentatives de casseurs de codes, dotés eux-mêmes de la puissance de calcul d'ordinateurs et procédant par essais et erreurs.

On décrit souvent cette force de résistance en disant que tel clé de chiffrement est capable de résister à tant de tentatives de tant d'ordinateurs de telle puissance tournant pendant tant d'années (ou de siècles)... Et cette puissance est globalement proportionnelle à la longueur de sa clé mesurée en bits. À titre d'exemple Deep Crack le briseur de code le plus rapide du moment rassemble 1800 circuits qui examinent chacun cinquante millions de clefs par seconde (90 milliards de clefs/seconde au total) Il "craque" une clef de 56 bits en vingt heures. Pour le moment la clef à 128 bits autorisée très récemment autorisée en France assurerait encore la sécurité. Quant aux réseaux interconnectant les ordinateurs, disons Internet pour simplifier, ils ont suscité un colossal flux d'informations confidentielles qu'il s'agisse de données politiques, militaires, scientifiques, économiques voire de transactions marchandes ou de simples correspondances de particuliers via le courrier électronique. Le message secret se banalise : il cesse d'être le privilège du soldat, de l'espion ou du conspirateur pour devenir une valeur marchande (le développement du commerce électronique repose entièrement sur la capacité de faire transiter en toute sécurité des informations sensibles - le cas le plus évident étant celui d'un numéro et d'un code de carte de crédit), mais c'est aussi une pratique quotidienne pour des millions de gens dont beaucoup vivent dans la crainte d'un Big Brother numérique. La banalisation du code, le transfert d'innombrables données cryptées sur les lignes téléphoniques, impliquent deux données stratégiques majeures. D'une part les technologies de surveillance, par exemple celles auxquelles recourt la National Security Agency, premier employeur de mathématiciens du monde et capable d'intercepter des millions de communications,

permettent de tout savoir sur chacun. L'individu qui se connecte sur Internet, utilise sa carte de crédit, figure sur de multiples fichier et se soumet quotidiennement à de multiples contrôles devient transparent et impuissant face aux grandes machines de surveillance. Mais, second facteur, David prend sa revanche sur Goliath : l'escroc féru de Nouvelles Technologies, le "hacker" animé par le simple goût ludique de l'exploit, le "cracker", plus agressif, et qui prend son plaisir à répandre le désordre dans les systèmes informatiques, les cyberterroristes qui mènent leur guerre par bits interposés en détruisant les systèmes de communication adverse acquièrent un pouvoir inédit. Une ligne téléphonique et un ordinateur suffisent pour lancer contre un gouvernement ou une entreprise des attaques, qui ne requièrent ni bombes, ni commandos suicides, mais n'en sont pas moins redoutable.

La guerre du chiffre a prend d'autres dimensions. La confidentialité des communications, c'est-à-dire la capacité qu'a un intrus de s'emparer d'une information vraie pour remporter la victoire, n'en est plus qu'une partie. Ce n'est après tout qu'une forme sophistiquée d'espionnage qui consiste à s'emparer des secrets de l'autre en l'épiant afin d'agir plus efficacement. Le renseignement n'y est que le support de l'action. Désormais le code permet non seulement de cacher ce que l'on dit, mais aussi de prouver qui l'on est. "Craquer" un code devient un moyen d'emprunter une identité, d'obtenir un mot de passe, d'effectuer des opérations à la place de quelqu'un. Dans un monde dématérialisé, où tout se fait à distance et par signaux, le code doit donc désormais garantir que l'on est bien en présence, ou plutôt en contact, avec celui que l'on croit.

L'enjeu porte sur la protection ou la lutte contre des activité nocives (espionnage, criminalité). Il concerne aussi la sécurité et partant le développement de transactions impliquant des unités monétaires dématérialisées (commerce électronique, cyberbanques), des biens intangibles (propriété intellectuelle), des données confidentielles (médicales p.e.), etc..

Mot de passe contre passage. C'est une lutte sophistiquée, dématérialisée et purement sémantique entre l'intrus et le défenseur, l'imposteur et le vérificateur. Car il ne suffit plus de garder le secret, il faut aussi garder l'accès : toute base de données, tout ordinateur connecté au réseau est susceptible de subir une attaque purement informationnelle, souvent à l'insu de son propriétaire légal. S'ajoute le fait que l'effraction est invisible et indolore et la pénétration immatérielle : parfois on ne réalisera jamais que le secret a été violé. Ou, dans le cas de marquage, de "*chips*" etc.. on ne saura jamais qu'il existe un moyen de reconstituer vos activités : on laissera alors toujours une trace de tout ce que l'on a reçu et émis, un indice de tous ses mouvements physiques ou virtuels, connexions. Ceci fonctionne dans les deux sens : "prélèvement" d'information, mais aussi pénétration. *Cookies*, chevaux de Troie, virus, bombes à retardement, etc.. introduisent frauduleusement soit des machines de guerre (qui opèrent destruction, ravage, désorganisation, falsification, etc..) soit des machines de contrôle (qui permettront de prélever de l'information ou de faire exécuter des instructions).

Des barrières numériques donnent ou non accès. Des machines procèdent à ce que les stratèges du Pentagone appellent IFF (Identifying Friends and Foes). Distinguer l'ami de l'ennemi devient un problème technique voire informatique.

D'où le caractère crucial de l'identification. L'impératif du "prouve qui tu es" des systèmes est l'exact pendant de la revendication d'anonymat du citoyen. Il conditionne la reconnaissance de la valeur probante du document numérique et de la signature électronique donc toutes sortes de questions liées aussi bien aux libertés publiques qu'au développement du commerce électronique.

Le code inviolable existe-t-il ? Longtemps on a cru que la système mis au point par IBM en 1977, celui du D.E.S. (*data encryption system*) l'était et qu'il demanderait plus de deux mille ans de travail aux ordinateurs les plus puissants des années 60. Si bien que les administrations américaines se sont dotées de ce système, qui vient d'être récemment "craqué". De plus le système D.E.S requiert que les correspondants se communiquent leur clef de chiffrement, et que toute clé peut être volée. De surcroît dans des conditions tout à fait exceptionnelles, en l'occurrence la mobilisation de dizaines de milliers d'internautes qui ont fourni leurs machines pour une immense attaque collective, D.E.S. a pu être "craqué".

Le grand concurrent de D.E.S. est le système dit à clef publique ou asymétrique (RSA des initiales de ses inventeurs) et dont l'idée peut être résumée ainsi : rendre le chiffrement irréversible. Pour employer une image, cela équivaut à donner l'adresse de sa boîte postale mais à en garder la clef. A communique à toute personne qui désire lui envoyer un message un algorithme de chiffrement qui lui est personnel. Chacun peut ainsi chiffrer un message destiné à A. Mais le processus n'est pas symétrique : savoir comment chiffrer ne permet pas de savoir déchiffrer, si bien que seul A qui possède la clef de déchiffrement et ne la communique à personne peut lire les messages qui lui sont adressés. S'il veut répondre à son interlocuteur B, il emploie la clef de chiffrement de B qui applique le même procédé. Le cryptanalyste qui disposerait du message clair de B, de la clef publique de chiffrement de A et du message crypté de B à A ne pourrait rien découvrir sur la clef de déchiffrement de B, à moins, théoriquement d'y consacrer son plus puissant ordinateur pendant quelques millénaires. C'est du moins ce que l'on croyait jusqu'à ce qu'en Août 1999 un ordinateur au service de la cryptanalyse n'ait cassé un code RSA dit à 512 bits, ce qui relance une course à la puissance.

Ce système est complété par une procédure de vérification des identités : toujours sans livrer à quiconque sa clef personnelle, chacun s'identifie par une sorte de jeu de questions et réponses codées : il réalise des performances qui prouvent qu'il possède bien la clef de X ou Y et est donc bien X ou Y.

Pourrait-on aller encore plus loin et imaginer un système dont les propriétés physiques et non sémantiques serait telle qu'il serait indéchiffrable et mieux encore "inécoutable" ; on ne pourrait intercepter ou copier un message à l'insu des interlocuteurs ? Ce serait une façon sophistiquée de réinventer le principe du coffre-fort scellé. C'est ce que tente un système de codage dit quantique qui repose sur l'envoi d'électrons dont la réception ne peut s'opérer qu'une fois et la lecture n'être opérée que par un filtre précis. Cette méthode est encore expérimentale ; encore faudrait-il qu'elle soit applicable à grande échelle. En ce cas les méthodes physiques basée la nature tangible du support l'emporteraient sur les méthodes purement symboliques reposant sur l'emploi de signes et correspondances.

Le pouvoir de crypter se banalise voire se démocratise sous l'action de quelques "techno-libertaires" qui mettent délibérément à la disposition de qui le demande un système de cryptage de haute technologie capable d'embarrasser toute autorité qui tenterait de violer l'intimité des citoyens. Mais ce pouvoir banal est un pouvoir dangereux : utiliser, diffuser ou exporter un code équivaut souvent à employer une arme. Telle est du moins la doctrine qui a inspiré de multiples tentatives de restreindre

l'usage du code. Aux États Unis ce fut la N.S.A. réclamant l'interdiction des publications scientifiques sur le sujet, les restrictions légales à la vente ou à l'exportation, générale ou dans les pays non agréés par les U.S.A., des systèmes performants, la C.I.A. tentant d'interdire le cryptage des conversations téléphoniques ou encore le président Clinton cherchant à imposer au nom de la lutte contre la grande criminalité la présence de "mouchards" dans les ordinateurs connectés à Internet. Et la France qui a longtemps restreint l'accès aux systèmes de chiffrement ou leur usage à l'aide de sa législation sur les armes et le matériel stratégique a connu les mêmes débats. Comme si le privilège régalien n'était plus la maîtrise de la violence légitime, mais celle du secret autorisé. Autrefois l'État nous disait ce que nous pouvions faire, il nous dit maintenant ce que nous pouvons savoir.

F.B. Huyghe