Communication
de Monsieur Jean-Louis Greffe

ꕥ

Séance du 15 octobre 2004

ꕥ

Histoire des codes secrets

Introduction

Les codes secrets ont une histoire qui suit celle de l'évolution des techniques et qui fut aiguillonnée par de grands événements historiques au cours desquels ces codes eurent parfois des rôles déterminants à jouer. Leurs auteurs comme leurs déchiffreurs sont rarement connus : secret oblige. Aujourd'hui encore les spécialistes du chiffre, celui-ci devenant techniquement de plus en plus sûr, ont peur que des pirates, des contaminateurs et surtout des terroristes s'infiltrent dans les réseaux officiels ou privés, malgré leurs propres protections. Un code secret permet une liaison discrète entre un expéditeur et un destinataire. Aujourd'hui, ce n'est plus le secret de la liaison qui pose problème, c'est l'identification sûre de l'expéditeur et du destinataire. Les nations réservent des budgets importants pour les codes secrets.

D'un point de vue scientifique, les codes secrets appellent pour leur réalisation et leur déchiffrage des disciplines nombreuses :linguistique, informatique, physique, et plus récemment astrophysique et mathématiques et ne peuvent être étrangers à une réflexion philosophique sur l'information. On distingue les codes volontairement secrets des codes de commodité comme les codes barre, l'alphabet Braille, même le Code Civil.

Un peu de vocabulaire

Un code secret est une méthode pour dissimuler le sens d'une information en remplaçant chaque signe de cette information par un signe différent : lettre,

chiffre, ou signe conventionnel. Par exemple, dans le code bancaire, votre identité a été changée en nombre qui reste secret. La notion de chiffre est synonyme de celle de code : on réserve code pour une méthode en général et chiffre pour une technique particulière connue de spécialistes : les opérateurs du chiffre, des informaticiens pour la banque, des marins autrefois avec leurs pavillons ou leurs phares, les militaires plus généralement avec l'alphabet Morse.

La clef est ce qui permet d'activer le chiffre. C'est, par exemple la carte bancaire. Quiconque peut savoir comment fonctionne une carte bancaire, mais en aucun cas connaître la clef d'autrui.

Les codes secrets servent aux armées qui les considèrent comme des armes, aux diplomates qui emploient souvent des chiffreurs militaires, aux industriels, aux banquiers, aux commerçants, aux publicistes, qui veulent protéger leurs propriétés intellectuelles.

Les codes secrets sont aujourd'hui à la mode car, considérés comme des jeux, ils excitent la sagacité des chercheurs d'énigmes. Le récent ouvrage Da Vinci Code et son succès le montre, bien qu'il véhicule des erreurs. Le vrai code de Léonard de Vinci est celui qui protégeait ses inventions : il recopiait des explications en clair à l'aide d'un miroir. Celles-ci devenaient incompréhensibles sans un miroir.

Nous allons maintenant parcourir les étapes essentielles de l'histoire des codes secrets en alternant exemples et codes.

Un premier exemple

Les plus anciens exemples de transmission discrète de messages sont rapportés par Hérodote dans ses «Histoires» qui retracent les conflits entre la Grèce et la Perse au 5ème siècle avant J.C. La vieille inimitié entre la Grèce et la Perse connut une crise aiguë quand Xèrxès, roi de Perse fit construire la nouvelle capitale de son royaume : Persépolis. Des présents vinrent de toute part, sauf d'Athènes et de Sparte. Xèrxès en prit ombrage et décida de corriger les Grecs. Il fit rassembler dans le secret une flotte très abondante.

Mais les Grecs avaient un espion : Demaratus qui était exilé à Suse en Perse. Celui-ci réussit à faire parvenir à Léonidas, roi de Grèce deux tablettes de bois ciré, pliantes. Elles paraissaient vierges, ce qui n'attira pas l'attention. Cléomène, épouse de Léonidas, interpellée par cet envoi vide, conseilla à son mari de gratter la cire : les tablettes révélèrent le plan de guerre perse. Les Grecs se préparèrent à la guerre et le 23 septembre 480 avant J.C., Xèrxès ne bénéficiait plus de l'effet de surprise. Les Grecs avaient tendu un guet-apens : ils laissèrent entrer les bateaux perses dans la baie de Salamine, fermèrent la baie, puis ils

pilonnèrent la flotte et celle-ci fut défaite, alors qu'elle était bien supérieure en nombre à la flotte grecque.

De tels exemples sont nombreux. Hérodote rapporte encore que Histaiareus rasa la tête de son messager, écrivit un message sur son crâne et attendit que les cheveux soient repoussés pour l'envoyer. Ce message avait pour objet de convaincre Aristagoras de Milet de se soulever contre le Roi de Perse.

Encore : Sparte inventa la scytale. En 404 avant J.C., Lysandre de Sparte vit un messager venant de Perse. Celui-ci lui tendit sa ceinture qui était entièrement écrite, mais incompréhensible. Il prit alors sa scytale, rond de bois calibré autour duquel il entoura la ceinture. Le message se recomposait, en clair, suivant une génératrice du cylindre. Il apprit ainsi que Pharnabase de Perse s'apprêtait à l'attaquer et il déjoua le plan d'attaque perse.

Ces exemples montrent que la dissimulation d'un message peut en assurer le secret. Mais il n'y a pas modification du message suivant un code.

Le premier code qui apparut fut celui de Jules César. Il a été décrit dans la «Vie des douze Césars» de Suétone. Ce code a, dans des versions perfectionnées, persisté pendant près de 1000 ans.

Chiffre ou code de césar

On écrit l'alphabet latin, qui sert de référence : A, B, C, D, …, X, Y, Z, soit 26 lettres, puis on écrit exactement en-dessous le même alphabet, mais décalé de 3 rangs vers la gauche. Il devient : D, E, F, ..., X, Y, Z et l'on complète à droite par les 3 lettres abandonnées à gauche : X, Y, Z, A, B, C, ce qui nous fait toujours 26 lettres. On met alors en correspondance chaque lettre de ce second alphabet (qui sert pour le code secret), avec chaque lettre placée au-dessus (avec lequel est écrit le message en clair). Ainsi, un A clair devient un D codé, un B clair un E codé, etc…

On substitue ainsi chaque lettre du message en clair par une lettre de l'alphabet du code. Ce système a été employé par Jules César pour ses messages aux armées (notamment pour la Guerre des Gaules), ainsi qu'à son ami Cicéron et à d'autres confidents connaissant le décalage de 3. Suétone lui-même fait remarquer que le décalage de 3 est arbitraire et qu'il y a 25 possibilités, ce qui est peu pour un descripteur, qui essaie toutes les combinaisons.

Plusieurs complications ont alors été apportées. D'abord associer à l'alphabet en clair, 2 alphabets décalés différemment et l'on crypte en dents-de-scie entre les 2. On prend la première lettre dans le premier alphabet crypté, la seconde dans le deuxième alphabet crypté, etc …

La complication ultime est de mélanger les lettres de l'alphabet servant à crypter. Il y aura alors 4 suivi de 26 zéros possibilités différentes. Le décryptage devient alors théoriquement impossible. Il n'est possible que si le décrypteur connaît la clef du mélange des lettres.

Ce code a résisté environ 1 000 ans, bien qu'il ait toujours excité la sagacité des chercheurs d'énigmes. La solution est venu d'Orient.

La découverte de Abu Yusuf Al Kindi

Les théologiens de Basra, de Kufa et de Bagdad essayaient de reconstituer la chronologie des révélations de Mahomet telles qu'elles apparaissent dans le Coran par la fréquence des mots employés : certains apparaissaient, d'autres disparaissaient. Pour le Hadith, journal attribué à Mahomet, ils recherchaient ce qui était à attribuer à Mahomet et ce qui n'était pas de lui : ils étudiaient la forme linguistique, le style, le choix des mots employés et enfin la fréquence d'apparition des lettres.

Ce fût une découverte essentielle, due à Abû Yusuf Al Kindi, pour la cryptonymie qui sera employée jusque vers 1920. Le code de Jules César ne résiste pas à l'analyse en fréquence des lettres.

En français, on a établi le pourcentage d'apparition des lettres sur environ 10 000 écrits : A : 9 %, D : 3 %, E : 15 %, I : 8 %, Q : 1 %, S : 8 %, etc… On ajoute certains usages des lettres, bien connus des cruciverbistes : le q est suivi d'un u, le c est souvent suivi d'un h, s est souvent à la fin d'un mot, 2 lettres sont un article, un possessif, une préposition ou une conjonction, les lettres doubles ne peuvent être que s, l, m, r, t, n, p, e, c, ou f. L'analyse en fréquence fut un outil de base des décrypteurs

La renaissance en Occident et le drame britannique

Entre 800 et 1 300, ce sont les monastères qui étaient en Occident les lieux de cryptage et de décryptage, car les moines étaient statistiquement les plus lettrés de l'époque. Ils connaissaient le code de César et ses raffinements, mais utilisaient aussi bien le grec, l'hébreu, l'arabe, et des symboles construits par eux, comme des notes de musique. Une mélodie devenait ainsi un code secret... Le Pape, comme tous les ambassadeurs ou les monarques, avait son secrétaire du chiffre. En 1500, c'était Soro, moine franciscain.

Le principe d'employer un autre alphabet fut gardé : en 1942, les américains se servirent d'une langue indienne : celle des navaros. Cette langue ne ressemblait à aucune autre. Seuls, 25 américains la connaissaient, ainsi que moins de 1 000 indigènes. De plus aucun archéologue allemand n'avait étudié cette

langue, ce qui était important en période nazie. 26 indiens furent sélectionnés par les marines américains, perfectionnés en anglais et envoyés sur le front japonais pour servir de transmetteur. Aucun étranger ne réussit à découvrir le contenu de leur message.

Aujourd'hui encore, certains messages sont indéchiffrables (comme le disque de Phaistos, en Crète), car écrits dans une langue dont on n'a pas de longueur de texte suffisante, pour reconstituer un alphabet.

Le drame britannique est l'issue fatale du complot de Babington au profit de Marie Stuart, qui dépendait directement de la résistance d'un chiffre. Nous sommes en Angleterre en 1600. La reine Elizabeth 1ère d'Angleterre avait déjoué un certain nombre de complots à son encontre dans le cadre général de la lutte des catholiques et des protestants, et plus particulièrement dans le cadre des ambitions d'Élizabeth sur l'Écosse, catholique, et dont la Reine était Marie Stuart, par ailleurs cousine d'Élizabeth. Babington, écossais, prit l'initiative de fomenter un complot pour Marie et contre Élisabeth. Il échoua et Marie fut emprisonnée en Angleterre. Elle correspondait avec l'extérieur par message chiffré, fait de signes cabalistiques qu'elle avait inventés elle-même ; Marie avait un messager en Angleterre, qui était au courant du complot mais qui, entre temps, était devenu agent double. Il prit connaissance du message que lui avait confié Marie, l'apporta au chiffreur-déchiffreur d'Elizabeth. Avec la première partie du message, il déchiffra rapidement le chiffre de Marie et rédige - en imitant son écriture - une seconde partie en forme de post-scriptum dans lequel elle demandait des précisions sur les noms et qualités des différents collaborateurs de Babington. Le message fut transmis à Babington, qui répondit par retour à Marie, réponse qui à son tour fut interceptée : Marie signait son arrêt de mort ; trois des conspirateurs furent soumis à l'estrapade et Marie Stuart fût décapitée le 8 février 1587. Ses derniers mots furent : «en ma fin est mon commencement».

Code de Vigenère : cassure du code de César

Blaise de Vigenère, diplomate français, né en 1523, décida de s'attaquer au code de César en s'attaquant à la répartition en fréquence des lettres puisque ses accidents étaient la clef du décryptage, et comment rendre cette répartition «plate», celle où toutes les lettres auraient la même fréquence d'apparition. Pour cela, Vigenère écrit l'alphabet ordinaire en lequel est écrit le message en clair. Il écrit en dessous 25 autres alphabets décalés chacun d'un rang à gauche et complétés à droite. Par exemple le 4ème alphabet correspondait à un décalage de 3 et était celui employé dans le code de César. Dans ce système, chaque lettre du message en clair avait en-dessous d'elle 25 lettres différentes.

Laquelle choisir pour crypter ? C'est là qu'intervient alors un mot-clef, connu seulement de l'expéditeur et du destinataire. Ce sont ces lettres du mot-clef répétées autant de fois que nécessaire qui va sélectionner par la première lettre de chaque ligne, la ligne qu'il faut employer, par la lettre à l'intersection de la colonne définie par la lettre du message et la ligne qui vient d'être définie. Ce système donne une répartition plate.

Le code de Vigenère fut publié en 1586, ignoré pendant 200 ans jusqu'en 1786, mais ensuite, ayant acquis rapidement la réputation d'un code indéchiffrable, il fut systématiquement employé jusqu'en 1920, à une époque où l'importance du chiffre prenait une importance grandissante.

Pendant ce temps-là, en 1854, le britannique Babbage s'intéressait à la périodicité du mot-clef du code de Vigenère. Il établit de telles corrélations que le code fut cassé : il lisait facilement les messages secrets élaborés suivant cette méthode.

Dans la seconde partie du XIX^{ème} siècle, rien ne se passe, ou à peu près pour le cryptage. On jouait avec l'encre sympathique. En physique, un progrès considérable a lieu avec l'invention du télégraphe et du Morse, puis de la TSF de Branly et de Marconi. Cela posait un nouveau challenge aux crypteurs parce que les messages se promenaient dans le ciel et servaient en particulier aux navires en mer. D'où un durcissement des codages devenait nécessaire.

Code ADFGVX

Les Allemands, en vue de la première guerre mondiale qui se préparait, élaborèrent le code ADFGVX (de lettres très différentes dans l'alphabet Morse). Il fût mis au point et diffusé le 5 mars 1918 avant la grande offensive du 21 mars. Le principe du cryptage était celui de Vigenère, mais il comportait en plus les dix chiffres décimaux, ce qui aux yeux des spécialistes confortait l'indechiffrabilité.

Le renseignement français découvrit immédiatement l'existence de la modification qu'apportait le code ADFGVX. Mais laquelle ? Pendant 3 mois, nuits et jours, le major de Polytechnique consigné, Georges Painvin, lieutenant, réussit à casser le chiffre allemand. Il réussit, en particulier, à décrypter le message allemand du 2 juin 1918 : «Acheminez munitions. Urgence. Même de jour, si camouflés...» Le message provenait d'une origine entre Montdidier et Compiègne, à environ quatre-vingts kilomètres de Paris. L'aviation alliée confirmait la concentration des troupes. Mais la surprise fut totale du côté allemand. Les troupes allemandes durent rebrousser chemin après cinq jours d'une bataille acharnée. Georges Painvin continua à faire

des décryptages difficiles, mais les expériences de la guerre remirent en cause les méthodes de déchiffrage.

La machine Enigma

En 1918, Arthur Scherbius et Richard Ritter inventèrent une machine à chiffrer électrique et automatique… «Pour s'amuser» (genre Concours Lépine). L'invention, jugée d'abord curieuse, fut ensuite reconnue comme ayant une efficacité redoutable. Malgré son prix très élevé, plusieurs pays ou grandes compagnies s'en équipèrent. L'Allemagne y vint tardivement, mais en commanda trente mille pour son armée. Elles devinrent le fer de lance du renseignement allemand. Hitler pensait qu'elles joueraient un rôle déterminant dans une victoire sur les Alliés.

Dans sa version élémentaire, le principe de la machine s'appuie sur le code de César. Elle comporte 3 disques, sur chacun desquels un alphabet était gravé. Chaque disque convertissait un alphabet en un autre, dans un ordre différent, qui dépend de la position initiale des disques. Il s'agit d'un surdécryptage : on crypte un message déjà crypté. On peut même mettre en bout un réflecteur qui faisait repasser le message dans l'autre sens, cela fait 6 cryptages. Et un nombre considérable de clefs. Enfin pour décrypter, il faut posséder une machine et la faire marcher en sens inverse. Mais à condition de savoir les positions initiales des disques. C'est pourquoi, les Allemands avaient diffusé dans leurs services des carnets de code permettant de réactualiser chaque jour à minuit les machines. Ces carnets étaient valables 1 mois (à cause des sous-marins).

La cassure d'Enigma : la trahison de Schmidt

Jusqu'en 1926, les cryptanalistes anglais continuaient à contrôler les communications allemandes. Mais, après apparurent les messages Enigma et les Alliés s'avouèrent vaincus par le chiffre allemand qui devenait ainsi le plus sûr du monde. Mais les Alliés restaient militairement et diplomatiquement les maîtres : L'absence de leur zèle cryptologique était concevable.

La Pologne était prise entre l'Allemagne et la Russie et se devait d'intercepter les messages secrets. Le chef du renseignement polonais Ciezki réussit à faire acheter une machine Enigma commerciale et comprit le principe de l'invention de Scherbius, mais il ne put s'en servir car l'agencement des disques entre eux n'était pas le même que celui des armées allemandes et reconstituer le bon agencement était hors de portée.

Alors arriva la trahison suivante.

Hans-Thilo Schmidt, né à Berlin en 1888, fit la guerre de 1914-1918 puis fut écarté de l'armée (Traité de Versailles). Son frère aîné Rudolph, fut gardé dans l'armée et promu à la tête du Corps des Signaux. C'est lui qui imposa la machine Enigma. Il réussit à placer son frère, chômeur, dans les services du Corps. Sa famille, elle, resta en Bavière où la vie était moins chère. Il accumula vite rancœur et ressentiment vis-à-vis de son frère et de sa patrie. Il trouva un dérivatif en vendant le secret d'Enigma à des puissances étrangères.

Le 8 novembre 1931, Schmidt rencontre au Grand Hôtel de Verviers en Belgique un agent secret français du nom de Rex auquel il vend pour 10 000 marks les plans d'Enigma. Si ces plans n'étaient pas tout à fait complets, ils permettaient de faire une réplique exacte d'une machine Enigma militaire. Cela ne suffisait pas, il fallait connaître la clef, c'est-à-dire la position initiale des disques : celle diffusée chaque mois par les carnets allemands. Ils contenaient, jour par jour les 12 paramètres d'initialisation des disques.

Les Français avaient tout pour réussir : ils ne construisent pas une Enigma. Les Polonais, menacés par une invasion allemande, demandèrent à la France les documents de Schmidt, qui les leur donna en vertu d'accords de coopération militaire. Les Polonais pensaient qu'il y avait un raccourci pour trouver la clef d'Enigma.

Pour casser un chiffre, on employait surtout des linguistes. Les Polonais changèrent cette habitude et employèrent des mathématiciens bilingues, formés à l'Université de Poznan, à la frontière allemande pour le cryptage. Trois mathématiciens se révélèrent particulièrement efficaces dans l'exercice du chiffre, notamment Marian Rejewski, 23 ans, qui se destinait aux assurances. La méthode de M. R. était de comparer différents messages du même jour et de voir ce qu'ils avaient de commun dans l'organisation des lettres. Il réussit à établir les relations qui existaient entre les lettres en face les unes des autres et donc le positionnement relatif des disques entre eux, mais pas le positionnement initial : il y avait 105 456 positions initiales possibles. Un bureau travailla un an pour faire le tableau de toutes ces positions et dès lors Rejewski était capable devant un message chiffré par la machine Enigma de le décrypter instantanément. C'est intellectuellement la plus forte avancée de la cryptanalyse. Toutes les communications allemandes étaient devenues transparentes en particulier celles de H. Goering, qui employait systématiquement le chiffre ; de plus, la recherche des corrélations dans les messages surcryptés fut mécanisée par Rejewski en une machine qui fût appelée «Bombe». Elle était au déchiffrement ce qu'était Enigma au chiffrement.

Rejewski et l'Ecole polonaise étaient parvenus à la quintessence du décryptage : cela dura 10 ans de 1928 à 1938. Mais en décembre 1938, les Allemands

renforcèrent la sécurité de leur Enigma en ajoutant deux disques aux trois précédents ce qui compliquait notablement la combinatoire du déchiffrement : Rejewski capitula vis-à-vis de ce nouveau problème et l'invulnérabilité d'Enigma portait un coup terrible à la Pologne, car la Pologne était au centre de la stratégie du Blitzkrieg - ou guerre éclair - d'Hitler. Sa force tenait à la rapidité de l'attaque grâce à la rapidité des transmissions.

Puisque la Pologne, pour laquelle le renseignement était vital, ne pouvait pas améliorer le décryptage, le chef du bureau du chiffre polonais invita ses homologues français et britanniques à venir à Varsovie. Il leur montra une machine Enigma, version militaro-diplomatique, leur montra une «Bombe» et leur donna un plan de celle-ci, en attendant le 19 août où une Enigma parvint à Londres dans les bagages de Sacha Guitry et d'Yvonne Printemps. Ce fût une astuce conçue par l'ambassadeur de France en Pologne.

Le 1er septembre 1939, Hitler envahissait la Pologne.

Bletchley Park

Les Anglais prirent le taureau par les cornes, pensant trouver dans les travaux et le matériel polonais de quoi percer les nouveaux fonctionnements d'Enigma. Au cours des années précédant la deuxième guerre mondiale, les Allemands transmettaient 2 millions de mots par mois, maintenant ils en transmettaient 2 millions par jour. Il fallait donc rechercher la performance, la rapidité sans relâcher la sécurité, il fallait donc trouver un compromis.

Les Anglais structurèrent massivement leur bureau du chiffre. Ils rassemblèrent dans un château au milieu d'un grand parc - Bletchley Park - d'abord deux cents puis jusqu'à sept mille spécialistes du chiffre pour s'attaquer à Enigma. Ils étaient recrutés parmi les meilleurs étudiants en mathématiques d'Oxford et de Cambridge, les champions d'Angleterre d'échecs et de mots croisés, les spécialistes des puzzles, les réparateurs de porcelaine ancienne, des traducteurs et des linguistes de toutes langues. Les suivants furent recrutés sur des concours de mots croisés publiés dans les journaux. Tout ce personnel était distribué dans le parc dans des «huttes», spécialisées chacune dans une partie du travail. Ceci procédait d'une méthode rationnelle et protégeait le secret : seul, l'état-major, dans le château, avait connaissance de l'ensemble.

À partir des travaux polonais, le décryptage de la nouvelle Enigma avançait, mais pas assez vite pour contrer les dégâts dûs aux sous-marins allemands dans l'Atlantique. C'est pourquoi le gouvernement britannique décida l'action directe, notamment sur les transmissions navales : il fallait récupérer des carnets de code allemands, ce qui permettait d'initialiser les disques d'Enigma. Les Anglais attaquèrent les navires météo allemands, ils coulèrent quelques

destroyers et sous-marins allemands en ayant bien soin de récupérer les carnets de code sur les marins. Ils parachutèrent des mines vers lesquelles se dirigèrent les sous-marins allemands pour signaler leurs présences. Les messages qu'ils communiquaient entre eux étaient tous interceptés.

C'est alors qu'apparut à Bletchley Park, Alan Turing, mathématicien de Cambridge et premier inventeur des algorithmes informatiques à la base de la conception des ordinateurs.

Celui-ci analysa les messages cryptés allemands et remarqua des analogies, notamment dans les bulletins météo. Il inventa la notion de «mot probable», «crib», en anglais. Il soumettait ce mot probable à la machine Enigma marchant à l'envers, en recherchant si sa version en clair apparaissait, ce qui voulait dire que son choix de mot probable était le bon. Il automatisa son procédé de recherche avec une machine électronique qui était une «bombe», et qui fut baptisée «Victoire».

L'apparition de l'informatique

Pendant la seconde guerre mondiale, les décrypteurs anglais eurent la suprématie sur leurs collègues allemands. Mais ces derniers avaient pressenti que la machine Enigma avait pu être contournée. Ils ont alors imaginé des perfectionnements de la machine qui n'étaient rien d'autre que des complications de son fonctionnement. Le nouveau modèle fut baptisé Lorenz : peu d'exemplaires furent réalisés et étaient réservés aux messages d'Hitler à ses généraux.

Les Anglais ont répondu à cette nouvelle avancée en construisant une machine à crypter d'un genre tout à fait nouveau : la Colossus, mise au point fin 1943. Son principe était basé sur le concept d'ordinateur programmable, ce qui faisait faire un grand pas dans la rapidité des traitements. Cette machine avait pour objet d'automatiser le décryptage du code Lorenz et ce fut une réussite. Les Allemands progressent de leur côté, une véritable lutte entre crypteurs et décrypteurs par ordinateur programmable était lancée. Mais seuls les propriétaires d'ordinateurs pouvaient en user c'est-à-dire les gouvernements et les armées.

Comment transmettre la clef avec le message

Un problème devient majeur avec la multiplication des ordinateurs, leur accès par tous, et la standardisation de leur fonctionnement : transmettre la clef de lecture, ce qui de tout temps a fragilisé le chiffrement. Il s'agit apparemment d'un cercle vicieux car avant que deux personnes échangent un

secret (le message crypté), elles doivent déjà partager un autre secret : la clef de décryptage. La solution se fait par informatique. Nous allons la décrire par une analogie. Soient deux partenaires Alice et Bernard. Alice veut envoyer un message secret à Bernard, partenaire éloigné. Alice met un message en clair dans une valise qu'elle verrouille avec un cadenas. Le message devient secret, sauf pour Alice. Elle envoie le tout à Bernard. Bernard ne peut prendre connaissance du message. Il verrouille à son tour la valise avec son propre cadenas et envoie le tout à Alice. Alice enlève son cadenas et retourne la valise à Bernard qui l'ouvre avec sa clef et prend connaissance du message d'Alice. Si la valise n'est pas fracturée le secret est bien gardé. Dans la réalité la transmission de la valise se fait de façon informatique.

Cette façon de procéder est très sûre, mais elle suppose plusieurs trajets de la valise. Par ailleurs, il ne faut pas que la valise soit perdue ou détruite. C'est pourquoi des recherches furent tentées pour améliorer le processus.

Le système RSA (Rivest, Shamir, Adleman, 1977)

Une amélioration est faite par le système RSA, dont nous allons donner à nouveau une analogie. Maintenant Alice est en possession de cadenas identiques qui se ferment en cliquant dessus et s'ouvrent avec une clef qu'elle possède. Alors, Alice envoie des cadenas ouverts à l'ensemble de ses correspondants : elle en a un annuaire. Si Bernard veut envoyer un message à Alice, il le met dans une valise qu'il ferme avec le cadenas qu'il a reçu. Alice l'ouvre avec sa clef.

Cette clef d'Alice s'appelle «clef privée», qui sert au décryptage. Le cliquètement du cadenas s'appelle «clef publique», qui sert au chiffrement. Ce système est très sûr, mais nécessite une grande préparation.

Il reste encore un trajet de valise. On peut le supprimer par un moyen physique. Si Bernard veut envoyer à Alice un message secret : Alice brouille la liaison par un moyen connu d'elle. Bernard envoie son message à Alice. Il est brouillé, mais Alice en prend connaissance en le «débrouillant», selon son procédé.

L'avenir

Un organe de transmission particulièrement moderne et efficace est la fibre optique. Un rayon lumineux transporte avec lui un champ électromagnétique qui vibre perpendiculairement et ceci aléatoirement. Mais on peut le faire vibrer dans un seul plan : on dit alors que la lumière est polarisée dans ce plan. On peut aussi changer le plan autant de fois que l'on veut. On

peut donc le faire suivant les signes d'un code. Si le récepteur a un système dépolarisant et programmé suivant les instructions de l'expéditeur, il peut lire le message codé.

La cryptographie a encore un bel avenir devant elle, et n'hésitera pas à employer les technologies les plus avancées. Mais aujourd'hui, on est à peu près sûr de pouvoir transmettre un message sans qu'il soit intercepté.

Discussion

Le Président Michel Burgard remercie l'orateur pour son exposé passionnant.

Interviennent : Michel Vicq, Dominique Flon, Henri Claude, Philippe Martin, Alain Larcan, Marion Créhange et François Le Tacon.

Michel Vicq remercie Jean-Louis Greffe d'avoir confirmé les propos qu'il avait tenus lors de sa conférence sur Échelon. Michel Vicq indique qu'il a lui-même été confronté au déchiffrage en son début de carrière.

Dominique Flon fait part à l'assemblée d'une anecdote relative au codage d'un message.

Henri Claude fait part, comme Michel Vicq, de sa propre expérience d'officier du chiffre après la dernière guerre.

Philippe Martin évoque également une expérience personnelle. Il y a une dizaine d'années, l'Université de Nancy 2 a été contactée par la police régionale de Metz qui n'arrivait pas à avoir la clef de messages incompréhensibles échangés entre un quartier de Forbach et l'Europe de l'Est. En fait, il s'agissait tout simplement d'un dialecte «Rom» compris par très peu de personnes.

Alain Larcan se réfère à l'ouvrage de l'histoire des codes de Simon Singh. Simon Singh est aussi l'auteur d'un remarquable ouvrage sur le théorème de Fermat paru en 1997. Il y pose le problème du calcul impossible. Alain Larcan se demande si, de nos jours, avec les progrès de l'informatique, il y a encore des calculs qui ne peuvent être effectués. Le problème de l'extraordinaire carré de Vigenère a été résolu avec deux siècles de décalage. Alain Larcan évoque les problèmes ésotériques posés par le grand homme du décryptage du Moyen Age, Johannes Trithémius ou Tritheim. Il pose la question des grands textes religieux comme la Bible et le Coran. Il évoque aussi les crypteurs des rois de France dont François Viète. Le talent de ce dernier était tel que Philippe II

fit une demande de procès en sorcellerie auprès du Saint-Siège. Il évoque les Rossignol, père et fils, crypteurs de Louis XIV ainsi que l'énigme du masque de fer avec les deux hypothèses classiquement avancées. Une autre hypothèse est liée au décryptage d'un texte de Louvois crypté par les Rossignol et décrypté par Etienne Bazeries à la fin du XIX^{ème} siècle. Selon ce texte, le masque de fer serait Vivien de Bulonde, un général qui avait fui, abandonnant blessés et munitions au profit de l'Autriche, ce qui aurait compromis toute la campagne du Piémont. Le texte de Louvois est parfois considéré comme une fausse piste destinée à égarer les historiens. Alain Larcan rappelle aussi qu'il existe, dans les *Mémoires* de l'Académie, une communication sur la machine ENIGMA.

Jean-Louis Greffe indique qu'il n'avait pas le temps d'aborder la question des crypteurs de Louis XIV. Il précise que la notoriété des Rossignol était telle, que leur patronyme est devenu un nom commun donné à un passe-partout.

Marion Créhange pose également la question de «l'indéchiffrabilité» liée à la puissance actuelle de l'outil informatique. Il est en effet maintenant possible de faire travailler en parallèle différents ordinateurs. Marion Créhange se demande par ailleurs s'il existe des méthodes de chiffrage autres que lettre par lettre.

Jean-Louis Greffe indique qu'il existe des méthodes de chiffrage par groupe de lettres.

Michel Vicq reprend la parole pour aborder la question des messages codés par le son. Il revient sur la machine Enigma et se demande si les moyens informatiques actuels auraient permis de «casser» le code de cette machine plus rapidement.

Jean-Louis Greffe répond par l'affirmative.

Alain Larcan revient sur la question de la rapidité des moyens actuels de décryptage pour les tâches d'urgence.

Jean-Louis Greffe indique que cette question plus générale pose le problème de la décomposition d'un nombre entier en facteurs premiers. Cette opération simple dans le cas des petits nombres devient très complexe avec les grands nombres, ce qui peut induire un long temps de décryptage.

François Le Tacon demande si les ordinateurs quantiques, beaucoup plus rapides que les ordinateurs actuels, vont rapidement être mis sur le marché.

Jean-Louis Greffe n'est pas optimiste dans un avenir proche, mais pense que ces nouvelles machines constitueront un jour le futur de l'informatique.