Quelle confiance dans la cryptographie ? Une approche historique

Philippe Guillot

Quelle confiance peut-on avoir dans la cryptographie ? Que nous enseigne l'histoire dans ce domaine ?
Voici deux citations contradictoires sur la confiance qu'un chiffre peut inspirer.

En 1585, dans son traité des chiffres, Blaise de Vigenère (1523-1596) dit sa confiance : « *il se trouvera à l'encontre assez de manières de chiffres du tout inexpugnables et invincibles, à qui n'en aura le secret* ».

Au contraire, dans le numéro de juillet 1841 du Graham Magazine, Edgard Poe (1809-1931) exprime des doutes : « *L'intelligence humaine ne peut concocter un chiffrement que l'intelligence humaine ne puisse résoudre* ».

Ces deux citations ne sont pas pourtant incompatibles. L'inventeur d'un chiffre est trop souvent certain de son inviolabilité, et pourtant, son chiffre finit toujours par être cassé. L'attaque est une question de temps. La solidité d'un bon chiffre est certes réelle, mais provisoire.

Par exemple, pendant la première guerre mondiale, Fritz Nebel (1891-1977) conçoit le chiffre allemand ADFGVX composé d'une substitution – le changement d'une lettre par d'autres – et d'une transposition, c'est-à-dire un mélange des lettres. Au regard de ce qui se faisait à ce moment-là, ce chiffre avait la réputation d'une grande solidité. Les Allemands l'utilisaient en toute confiance. Il sera pourtant résolu manuellement par un travail assidu et acharné de l'équipe française du chiffre où opérait en particulier Georges-Jean Painvin (1896-1980), principal acteur de cet exploit. Il sera maintenu secret jusqu'en 1968. À cette date, à l'occasion de l'inauguration d'une salle du musée des Invalides consacrée à la grande guerre pour le 50e anniversaire de l'armistice du 11 novembre 1918, les deux hommes se rencontrent. Painvin révèle alors à Nebel qu'il lisait en clair la plupart des messages chiffrés. Les témoins de cette rencontre ont témoigné de la perplexité et de l'incrédulité de Nebel face à cette révélation.

Le secret comme source de confiance

Aux origines, c'est la confidentialité du procédé, élaboré dans le secret des cabinets noirs, qui était source de confiance. Laisser l'ennemi dans l'ignorance même du procédé de chiffrement était considéré comme un gage de sécurité. Cette approche a été ensuite vigoureusement remise en cause par Kerckhoffs (1835-1901) dont l'essentiel de la thèse est de revendiquer le non-secret dans l'élaboration du chiffre. Pourtant, le secret du procédé perdurera jusqu'à une époque très récente, conduisant à de nombreux déboires.

Le terme « cabinet noir » désigne des officines secrètes créées dans la plupart des pays européens dès l'apparition du service postal. Ils étaient en charge de l'interception du courrier. La tentation du contrôle total des communications n'a rien de nouveau. Les articles 13 et 14 de l'édit de Louis XI du 19 juin 1464 énoncent : « *Les courriers et messagers seront visitez par les commis du grand maistre auxquels ils seront tenus d'exhiber leurs lettres pour connoistre s'il n'y a rien qui porte préjudice au service du Roy et qui contrevienne à ses édits et ordonnances* ».

Outre l'interception du courrier, ces cabinets étaient également chargés du décryptement des missives chiffrées. Ils concevaient aussi des chiffres, à l'instar, sous le règne de Louis XIV, de la dynastie Rossignol Antoine (1600-1682), son fils Charles-Bonaventure (1649-1705) et son petit-fils Antoine-Bonaventure. On lui doit le *Grand Chiffre du Roy* qui gardera son mystère jusqu'à ce qu'il soit résolu par Étienne Bazerie (1846-1931) dans les années 1890.

Les cabinets noirs seront particulièrement développés sous Louis XV, où un *Cabinet du secret des postes* décachetait les lettres et transmettait les copies au lieutenant général de police et au ministre des affaires étrangères.

En 1789, de nombreux cahiers de doléances réclament leur abolition. La convention proclame l'inviolabilité des correspondances, mais le cabinet noir est rétabli par le Directoire et perdurera jusqu'au second Empire.

Les révélations d'Edward Snowden (né en 1963) montrent que l'agence de sécurité américaine NSA est une digne héritière de ces cabinets noirs.

La Curie Papale disposait, elle aussi, de son propre service de cryptographie. Blaise de Vigenère a fait partie des rares personnes à être initiées aux secrets de ses chiffreurs. La confrérie des cryptologues garde alors jalousement secret son savoir-faire. Vigenère écrit dans son traité des chiffres : « *L'écriture est double : la commune dont on use ordinairement, et l'occulte secrète qu'on déguise d'infinies sortes selon sa fantaisie pour ne la rendre intelligible qu'entre soi et ses consachants. Les yeux de l'âme du commun peuple ne sauraient bonnement supporter les lumineux étincellements de la divinité. (…) Afin de les garantir et soustraire du profanement de la multitude, et en laisser la connaissance aux gens dignes, à peu de gens divulguez artifices.* »

Avant lui, le savant arabe Al Kindi (801-873), auteur d'un manuscrit sur l'extraction de l'obscur – comprendre un traité sur le décryptement du chiffre – avait énoncé dans sa *préface : « J'aurais préféré suivre la voie des savants qui m'ont précédé et qui pensaient à obscurcir les trésors de la signification plutôt que de les afficher et de les révéler (…) Par conséquent, j'ai écrit sur ce sujet ce que je pensais être assez clair pour les fils de la sagesse, tout en restant hors de portée des personnes non informées. Que Dieu m'apporte le succès* ».

Le fonctionnement de la cryptographie dans des cercles fermés a longtemps empêché la diffusion de sa connaissance et a conduit des procédés à être souvent réinventés.

C'est ainsi que ce qu'on appelle aujourd'hui le chiffrement de Vigenère a été publié pour la première fois par Giovan-Baptista Belaso (1505-…) en 1553 dans un petit opuscule « La cifra del signor Belaso ». Il a été réinventé par le maréchal de l'armée impériale du Saint Empire Joan Franz Graf Gronsfeld-Bronkhorst (1640-1719), par l'amiral anglais Sir Francis Beaufort (1774-1857) et, dans l'Angleterre du dix-neuvième

siècle, il était toujours attribué à l'ecclésiastique John Wilkins (1614-1672), évêque de Chester. Longtemps considéré comme indécryptable, ce système de chiffrement a fini par être résolu. La première publication de cette résolution est celle de l'officier prussien à la retraite Friedrich Wilhelm Kasiski (1805-1881) dans son ouvrage paru en 1863 « l'écriture secrète ou l'art du déchiffrement » exactement 310 ans après son apparition. Mais on sait également qu'il a été résolu par Charles Babbage dans les années 1850. Ce dernier n'a rien publié de ce travail probablement tenu au secret en raison de l'implication de l'Angleterre dans la guerre de Crimée.

Signe de la difficulté de diffuser la connaissance en cryptologie, ce chiffre était présenté comme nouveau (*A new cipher code*) et infaillible (*Impossible of translation unless the keyword is known*) dans la revue *Scientific American* du 27 janvier 1917.

L'argument du nombre et de la complication

Un des arguments majeurs pour avancer la robustesse d'un procédé de chiffrement est d'énumérer les innombrables combinaisons à explorer pour le résoudre. Jérôme Cardan (1501-1576) a été l'un des premiers à utiliser cet argument. Il a en effet établi le nombre d'alphabets de substitution :

$$26 \times 25 \times \cdots \times 1 = 403\,291\,466\,112\,665\,635\,584\,000\,000$$

Ce nombre colossal assoit la confiance dans le procédé mais suppose que l'exploration exhaustive par force brutale est la seule voie de résolution, et ne préjuge pas de l'habileté des cryptanalystes.

Un autre argument repose sur la complexité du procédé. Si l'image du chiffrement est d'enfermer le message dans une enveloppe, une idée naturelle est d'insérer ce cryptogramme dans d'autres enveloppes pour multiplier les difficultés de résolution. Le recours au surchiffrement est avancé comme une sécurité supplémentaire. Vigenère avait déjà mis en garde sur la vanité de ce procédé : « *Mais je dirai bien davantage, car non que de trois enveloppes tant seulement, ainsi de cinquante, voire cent mille, et encore plus jusqu'en infini que cela s'étend, que puissent être réitérés ces surchiffrements, d'alphabet en alphabet les uns sur les autres, il n'importe de rien auquel de tous vous vous preniez pour le déchiffrer, étant en cela tous égaux, autant le dernier comme le premier ou second* ».

Le chiffre soviétique utilisé pendant la guerre russo-polonaise de 1920 était une substitution bigrammique surchiffrée. Cela n'a pas empêché le service du chiffre polonais, avec à sa tête Jan Kowalewski (1892-1965), aidé de mathématiciens comme Wacław Sierpiński (1882-1969) de décrypter leur chiffre, ce qui a conféré un avantage décisif aux Polonais pour éloigner la menace russe de Varsovie au cours de ce qui a été appelé le Miracle de la Vistule.

Bien que leur résolution ne soit pas notablement plus complexe qu'une simple transposition, les doubles transpositions étaient encore pratiquées dans les armées pendant les années 1930, compliquant davantage le chiffrement des missives que leur résolution.

Le télégraphe et le besoin pressant de chiffrer.

Le développement du télégraphe à la fin du dix-huitième siècle, d'abord optique,

puis électrique au milieu du dix-neuvième siècle, a multiplié les échanges, modifiant en profondeur la nature du chiffrement, qui évolue de la protection du message secret à celui du système de communications.

Le besoin de chiffrer se montre pressant. On peut lire dans la revue *Quaterly Review* en 1853 : « *Des mesures devront être prises pour parer à une sérieuse objection que l'on soulève à propos des communications privées par télégraphe – la violation du secret – car, dans tous les cas, une demi-douzaine de personnes sont amenées à connaître chaque mot adressé par une personne à une autre. Les employés de la Compagnie Anglaise du Télégraphe s'engagent au secret sous serment, mais nous écrivons souvent des choses que nous ne supporterions pas de voir lues par d'autres avant nous. C'est encore un grave défaut du télégraphe, et il faut y remédier d'une manière ou d'une autre* ».

La législation a suivi cette nécessité. En France, la loi du 13 juin 1866 accorde au public la faculté de correspondre en chiffres. La convention de Saint-Petersbourg du 22 juillet 1875 permet l'emploi du chiffre dans les communications internationales.

La taxation des messages au nombre de caractères conduit à l'utilisation de codes compressifs pour réduire le nombre de caractères transmis. Ces codes permettent aussi de cacher l'information. L'un des premiers pour cet usage est le code Sittler de 1868. Les mots et les expressions courantes sont rangés par pages où ils sont numérotés de 0 à 99. Un télégramme est alors constitué d'une suite de nombres de quatre chiffres indiquant le numéro de la page et l'index du mot dans la page.

Les amateurs rivalisent d'imagination pour proposer leur propre système de chiffrement. L'un d'eux, John H.B. Thwaites, dentiste à Bristol, propose un mécanisme qu'il qualifie d'inviolable et de révolutionnaire et dont il revendique la paternité. Il écrit un article au *Journal of the Society of Arts* en date du 11 août 1854 (pp 668-669) pour présenter son procédé qu'il estime utile aux *organismes publics et aux personnes privées qui ont l'habitude de traiter à distance par télégraph*e. Il donne l'exemple d'une faillite qui aurait pu être évitée si une information confidentielle avait pu être télégraphiée. Le procédé est réalisé à partir de tiges coulissantes. Thwaites écrit au journal afin que la Society aide à en promouvoir l'usage.

Charles Babbage (1791-1871), connu pour ses connaissances en cryptographie, est appelé comme expert pour évaluer le procédé. Il a une réponse assez sèche dans les colonnes du numéro en date du 1er septembre 1854 du même journal (pp 707-708) : Il reconnaît sans le nommer le chiffre de Vigenère : « *Ce chiffre est très ancien et peut être trouvé dans la plupart des ouvrages. Il n'est pas facile, mais a été souvent résolu sous des formes plus difficiles* ».

Babbage conclut : « *On peut poser comme principe qu'il ne vaut pas la peine de considérer un chiffrement comme impénétrable à moins que son auteur ait lui-même résolu des chiffres très difficiles* ».

Il s'ensuit des échanges au cours desquels Thwaites pose un défi que Babbage résoudra. Twaites propose un surchiffrement avec deux clés. Babbage lui fait remarquer que cela ne change rien à la sécurité, mais a pour défaut majeur de rendre seulement plus compliqué l'usage du procédé.

Le développement des communications par télégraphe et la défaite française dans la guerre de 1870 contre la Prusse vont conduire Auguste Kerckhoffs à écrire un article fondateur de la cryptographie moderne en 1883 dans lequel il remet en cause

le secret du procédé. Un chiffre qui repose sur le secret du procédé perd toute sécurité dès l'instant où le procédé vient à être connu. Il conclut son article ainsi : « *Je tiens en terminant, à insister sur ce point, que la valeur d'un système de cryptographie destiné aux besoins de la guerre est en raison inverse du secret qu'exige son maniement ou sa composition… [et] qu'un chiffre n'est bon qu'autant qu'il reste indéchiffrable pour le maître lui-même qui l'a inventé : Ars ipsi secreta magistro » (un art caché au maître lui-même)* ».

Cette exigence au premier abord paradoxale du non secret suppose un important travail de décrytement – le déchiffrement sans la clé – pour asseoir la confiance dans un chiffre, travail auquel Kerkhoffs s'attelle dans son article en passant en revue la plupart des procédés connus à son époque : substitutions à simple et double clé, transpositions, dictionnaires, etc.

Pourtant la tradition du secret perdurera encore longtemps et jusqu'à une période récente. Kerckhoffs lui-même a admis que les circonstances pouvaient ne pas rendre pertinente la divulgation du procédé. Dans la conclusion de son article, il écrit : « *Il vient d'être présenté à la Commission de télégraphie militaire un nouveau système de cryptographie qui me paraît réaliser tous les desiderata que j'ai exposé en commençant : indéchifrabilité complète, simplicité, non nécessité du secret ; des considérations de haute convenance m'empêchent d'en dire davantage pour le moment (sic)* ».

Malgré les travaux de Kerckhoffs, les procédés secrets ont longtemps perduré et connaîtront bien des déboires. Un chiffre conçu dans le secret d'une officine qui ne comporte que quelques concepteurs, même très brillants, a peu de chance d'être d'une grande robustesse. Lorsque l'algorithme vient à être révélé, par l'analyse d'un équipement, par espionnage, ou par étude mathématique, les failles apparaissent immanquablement et sont exploitées jusqu'à remettre en cause la sécurité de l'ensemble du système.

Les livres de code sont l'exemple archétypique du procédé qui exige le secret et dont Kerchoffs veut bannir l'usage.

Le 25 août 1914, le croiseur léger allemand Magdebourg s'échoue en eaux peu profondes dans le golfe de Finlande. Le navire est évacué en catastrophe. Les Russes récupèrent le livre de code de la marine, oublié dans la cabine du capitaine. Dans ses mémoires, Winston Churchill (1874-1965) raconte une version plus romancée : « *Le corps de l'un des sous-officiers allemands fut repêché par les Russes quelques heures plus tard et, serrés contre sa poitrine par des bras rendus rigides par la mort, étaient le chiffre et le livre de code de l'armée allemande* ».

Quoi qu'il en soit, les Russes transmettent ce livre de codes aux Anglais qui en feront un bon usage. La *Room 40* décryptera de nombreux messages allemands chiffrés avec des codes proches, en particulier le Télégramme Zimmermann dont la révélation accélérera l'entrée en guerre des États-Unis d'Amérique.

La machine Enigma militaire.

Ces déboires ont conduit l'armée allemande à se doter d'une machine à chiffrer qui n'exigeait pas le secret. L'inventeur et promoteur de cette machine, Arthur Sherbius (1878-1929), avait avancé : « *La solution d'un télégramme est impossible si la machine tombe dans des mains non autorisées puisqu'elle nécessite le positionnement préalable*

d'une clé ».

Cette machine, initialement destinée au marché commercial, est constituée de trois tambours rotatifs appelés rotors et d'un réflecteur qui réalisent chacun une permutation par leur câblage interne. La clé est constituée par le choix et la position initiale des trois rotors, soit : nombre de façons de placer dans l'ordre les trois rotors fois le nombre de positionnement de chaque rotor : 6 x 26 x 26 x 26 = 105 456, valeur considérée à l'époque suffisante pour dissuader la recherche exhaustive.

La machine est adoptée dès 1926 par la Reichsmarine, puis en 1928 par la Reichswehr. Mais pour adapter la machine aux besoins militaires et rendre son fonctionnement secret, la machine est personnalisée. Le câblage interne des rotors est spécifique, et un tableau de fiches, qui n'existe pas sur la machine commerciale est ajouté. Au début de l'exploitation, il fallait insérer six câbles dans ce tableau de fiches pour échanger 12 lettres par paire. Le nombre de combinaisons s'en trouve alors considérablement multiplié, puisque le nombre de façons d'insérer ces fiches est de l'ordre de 10^{11}.

Le nombre total de clés possibles passe alors à 10^{16}, ce qui est considérable. Ce nombre est en effet supérieur au nombre de millièmes de secondes depuis l'apparition de l'homo sapiens sur terre il y a 300 000 ans (homme de Djebel Irhoud).

Cette valeur gigantesque a contribué de façon majeure à la confiance qu'attribuaient les armées allemandes à leur chiffre. Les nazis avaient bien eu des alertes concernant des messages mystérieusement retrouvés en clair alors qu'ils avaient été chiffrés, mais avaient attribué ces déboires à l'espionnage.

Les mathématiciens polonais qui les premiers se sont lancés dans l'attaque de cette machine ont réussi à reconstituer les caractéristiques de la machine militaire par des méthodes mathématiques. Maintenir la machine secrète n'a même pas contribué à retarder la résolution, puisque les méthodes développées pour retrouver le câblage interne ont servi ensuite à reconstituer les clés journalières.

De plus, leurs méthodes de résolution reposaient sur l'analyse de la structure cyclique des permutations réalisées par la machine, et il se trouve que cette structure ne dépend pas du positionnement des fiches. En termes mathématiques, le tableau de fiches ne change pas la classe de conjugaison des permutations réalisées par la machine. Le tableau de fiches constituait ce qu'il faut bien ne considérer que comme une complication illusoire.

Ajouter des rotors aurait certainement contribué davantage à augmenter la sécurité, mais hélas aussi le coût. Des machines dotées de 10 à 15 rotors ont continué à être exploitées après la guerre, rendues finalement obsolètes par l'électronique et l'informatique.

Comment alors asseoir la confiance ?

Les déboires rencontrés jusqu'à une période très récente par les méthodes secrètes pousseront les concepteurs à renoncer définitivement au secret et à publier leurs spécifications. Voici quelques exemples. Aux débuts de la téléphonie GSM, le flux vocal était chiffré par un algorithme appelé A5/1. Introduit en 1987, sa définition est longtemps restée secrète. En 1994, des fuites révèlent l'architecture générale de l'algorithme, en 1999, une ingénierie inverse en reconstitue tous les détails. Après

leurs divulgations, de nombreuses failles sont mises en évidence. En 2000, une attaque en temps réel est découverte, nécessitant deux minutes de trafic au prix d'un lourd précalcul. Une amélioration de 2003 se passe du précalcul et ne demande que quelques secondes de flux chiffré. Le nouvel algorithme, appelé Kasumi, est désormais publié.

Les fournisseurs d'accès conditionnel aux programmes de télévision à péage ont longtemps tenté de protéger leurs procédés par le secret. Cela n'a pas empêché la vague de piratage qui a sévi au début du siècle. L'algorithme de chiffrement du flux vidéo, le *DVB common scrambling*, introduit en 1994, est resté secret jusqu'en 2002. Des failles ont été alors découvertes et exploitées en 2004 pour conduire une attaque par faute, puis en 2011 en exploitant la connaissance du programme en clair.

Dans les années 1980, les spécifications des premières cartes bancaires étaient demeurées intentionnellement secrètes. Cela n'a pas empêché, en 1998, l'informaticien et électronicien Serge Humpich (né en 1963), de désassembler le logiciel d'un terminal bancaire acheté au rebut. Il découvre alors que le secret de fabrication des cartes repose sur une clé RSA de 320 chiffres binaires, valeur convenable à l'origine, mais devenue trop faible pour résister à la nouvelle puissance des machines. Il révèle cette faiblesse, mais se retrouve condamné pour falsification. La leçon a été comprise. Aujourd'hui la norme EMC – Europay Mastercard Visa – des cartes bancaires est publique et librement accessible sur internet `https://www.emvco.com`. L'avantage est de bénéficier de l'expertise de nombreux cryptanalystes, mathématiciens, informaticiens, hackers, experts du monde entier pour révéler des failles de conception et ainsi de pouvoir les corriger. C'est dans cette optique qu'a été conçu le standard de chiffrement civil actuel, l'AES, *Advanced Encryption Standard*, qui est le résultat d'un appel d'offres public émis en 1997 et suivi de trois années d'attaques acharnées de la communauté des experts internationaux en cryptologie jusqu'à la sélection en 2001 de l'algorithme Rijndael. La conception et l'évaluation transparente sont la norme de conception aujourd'hui.

Mais même cette approche s'avère insuffisante. Après des itérations successives d'attaques et de correctifs, ne risque-t-on pas une nouvelle attaque qui remettra en cause la robustesse du procédé ? combien de temps faut-il pour asseoir la confiance ? Trois ans ? cinq ans ? Dix ans ? Et ensuite, combien de temps un procédé pourra-t-il être considéré comme sûr ? Le temps semble s'accélérer et des clés RSA réputées solides dans les années 1990 se factorisent aujourd'hui en quelques instants sur un ordinateur de bureau.

Pour tenter de répondre à cette objection et éviter la boucle infinie des attaques-corrections, une théorie cryptographique a émergé dans les années 1980 pour assortir la définition du chiffre d'arguments de sécurité. Cette théorie a établi qu'un chiffre sûr repose sur un axiome d'existence de fonctions dites à *sens unique*, facilement calculables, mais pour lesquelles il est illusoire de trouver un antécédent, tout comme il est impensable de trouver la clé d'un cryptogramme, même lorsque le clair est connu. Aujourd'hui, la multiplication de deux grands nombres premiers fait figure de telle fonction. Autant la multiplication est accessible, y compris sur des entiers gigantesques, autant la factorisation du produit reste inextricable. Le dernier record, en date de février 2020, concerne la factorisation d'un nombre de 250 chiffres décimaux qui a demandé autant d'énergie que 2 700 ordinateurs travaillant sans

discontinuer pendant un an. Il n'est d'ailleurs pas prouvé que cette difficulté soit réelle. Peut-être ne résulte-t-elle que de notre ignorance toute provisoire d'algorithmes plus efficaces.

Prouver la sécurité d'un chiffre consiste à démontrer que si un algorithme d'attaque existe, alors il peut être utilisé comme sous-programme pour résoudre un problème. La difficulté du problème constitue alors une preuve de l'impossibilité de l'adversaire. Mais l'existence de fonctions difficiles à inverser, comme l'est aujourd'hui la multiplication n'est qu'une hypothèse de travail qui peut, ou se confirmer, ou s'effondrer à tout instant. Par ailleurs, la sécurité étant fortement contingente, spéculative et même sociale, la nature de ces preuves est fortement remise en question par des chercheurs comme Neal Kobitz (né en 1948) et Alfred Menezes (né en 1965). L'édifice cryptographique est bien fragile.

Conclusion

Nous vivons aujourd'hui une situation paradoxale. Tout semble possible pour assurer une protection à toute épreuve et imaginer des applications sécurisées cryptographiques les plus variées. Certains problèmes sur lesquels repose la cryptographie, comme la factorisation et le logarithme discret restent inextricables. La loi de Moore, qui énonce une croissance exponentielle des performances des calculateurs, touche à sa fin. L'ordinateur quantique pour factoriser semble lointain. Dans un avenir proche, on ne peut pas attendre de progrès notables des moyens de calcul comme ceux qu'on a connus dans les décennies passées.

Mais les systèmes réels apparaissent toujours plus vulnérables. Le monde numérique est en situation de guerre, avec des hackers toujours plus nombreux, dont beaucoup sont recrutés par les états eux-mêmes. Les portes dérobées dans les systèmes et les équipements ne sont plus un mystère et sont même revendiquées pour rendre le contrôle possible sous couvert de lutte anti terroriste.

La conclusion prend la forme d'une question : si la confiance dans le chiffrement lui-même ne va pas de soi, que dire alors de celle dans les systèmes complexes interconnectés qui réalisent aujourd'hui nos échanges numériques ?