*Intellectica*, 2020/1, **72**, pp. 141-157

# Informatique et cryptologie : un déplacement des frontières

Philippe GUILLOT[*] & Marie-José DURAND-RICHARD[◊]

**RÉSUMÉ.** Les travaux de Turing ont montré les liens étroits qu'entretiendront cryptologie et mécanisation du calcul. Leur évolution parallèle va déplacer de nombreuses frontières : entre secret et transparence, entre sphère publique et sphère privée, entre contrôle social et liberté individuelle, entre art et science. Cet article explore ce mouvement à la lumière des domaines où il s'est manifesté. Depuis la Seconde Guerre mondiale, la cryptologie a évolué d'un usage presque exclusivement militaire à son ubiquité actuelle. Cette mutation d'usage s'est doublée d'une transformation de nature, en particulier sous l'angle du rapport à la science. Les techniques artisanales ont cédé la place à une nouvelle branche des mathématiques dont le caractère scientifique est autant revendiqué que controversé, tant la sécurité est matière à spéculation. Les questions ouvertes par la théorie de la complexité trouvent une illustration imagée avec les mondes virtuels de Russel Implagliazzo. L'impact sociétal de la cryptologie est aussi abordé du point de vue de la nature des échanges : contrôle institutionnel ou maintien au sein de cercles privés. L'histoire de l'opposition entre contrôle étatique et liberté d'usage sera exposé au regard du droit. Sont enfin abordées les nouvelles applications et menaces de la cryptologie, reculant les frontières du possible, de l'informatique en nuage aux monnaies virtuelles.

*Mots-clés* : Cryptologie, sécurité des systèmes d'information, portes dérobées, mondes d'Impagliazzo, complexité, P = NP ?, art et science.

**ABSTRACT. Computer Science and Cryptology: a Border Shift**. Turing's work shows the close links between cryptology and mechanization of computation. Their parallel evolution is still shifting many borders: between secrecy and transparency, between public and private spheres, between social control and individual freedom, between art and science. This article explores this movement in light of the areas in which it has manifested. Since World War II, cryptology has evolved from an almost exclusively military use to its current ubiquity. This change in use has been accompanied by a transformation in nature, particularly in terms of its relation to science. Handicraft techniques have given way to a new branch of mathematics whose scientific character is as much claimed as controversial, as security is matter for speculation. The questions opened by the theory of complexity find a pictorial illustration with the virtual worlds of Russel Implagliazzo. The societal impact of cryptology is also approached from the point of view of the nature of the exchanges: institutional control or maintenance within private circles. The history of the opposition between state control and freedom of use will be exposed under the law. Finally, the new applications and threats of cryptology, pushing back the boundaries of what is possible, from cloud computing to virtual currencies are discussed.

*Keywords*: Cryptology, computer science, information systems security, backdoors, Impagliazzo's worlds, complexity, P = NP ?, art and science.

[*] Université Paris 8 Vincennes-Saint-Denis, Département de Mathématiques et d'Histoire des Sciences. philippe.guillot<at>univ-paris8.fr

[◊] Université Paris 8 Vincennes Saint-Denis & laboratoire SPHERE UMR 7219 CNRS-Université Paris Diderot.

© 2020 Association pour la Recherche sur la Cognition.

## INTRODUCTION

La Cryptologie et l'Informatique sont deux domaines dans lesquels Turing a été fortement impliqué et qui ont bouleversé de nombreux pans de l'activité humaine depuis la Seconde Guerre Mondiale. La victoire contre le chiffre allemand à Bletchley Park a été rendue possible grâce à l'élaboration de modèles mathématiques et à la construction d'outils de calcul électro-mécaniques destinés à rendre possible une recherche exhaustive devenue manuellement illusoire. Cette évolution technique majeure a été prolongée jusqu'à l'élaboration du calculateur *Colossus* – à laquelle Turing n'a participé que de manière marginale – qui marque un premier rapprochement entre cryptologie et électronique, rapprochement qui va permettre ensuite le développement massif de l'informatique, tant sur l'aspect matériel que logiciel. Le développement des communications entre ordinateurs mis en réseau va donner une importance cruciale à la protection des informations transmises. Depuis lors, cryptologie et informatique vont évoluer parallèlement, l'une alimentant les besoins de l'autre. Leur rencontre va déplacer de nombreuses frontières, voire même tendre à les supprimer : entre secret et transparence, entre sphère publique et vie privée, entre contrôle social et liberté individuelle, entre art et science, entre monde réel et virtuel, entre autorité centrale et organisation décentralisée, entre entités nationales et mondiales. ,

Cet article se propose d'explorer ce mouvement des frontières à la lumière des domaines où il s'est manifesté. Nous clarifierons tout d'abord le contexte historique qui a conduit la cryptologie à accompagner le développement de l'informatique à partir d'un usage presque exclusivement militaire au sortir de la Seconde Guerre Mondiale jusqu'à son ubiquité actuelle. Cette mutation d'usage s'est doublée d'une transformation de la nature de cette activité. Nous aborderons cette question sous l'angle du rapport à la science. Les techniques artisanales des premiers chiffreurs ont cédé la place à une nouvelle branche des mathématiques dont le caractère scientifique des preuves est autant revendiqué avec force que controversé, tant la sécurité est matière à spéculation. Les questions ouvertes par la théorie de la complexité ont trouvé une illustration imagée sous forme de mondes virtuels définis selon les réponses supposées aux grandes conjectures de cette théorie. Imaginés par le chercheur Russel Implagliazzo, ces mondes diffèrent en particulier par le type de cryptologie qu'ils permettent.

Les aspects sociétaux sont ensuite abordés sous l'angle de la communication, nœud de toute activité sociale. Maîtriser la diffusion des informations, ou au contraire maintenir ses échanges au sein d'un cercle privé est une préoccupation majeure des acteurs de la société, qu'ils soient institutions ou individus. Comprendre ces enjeux appelle à un balayage historique sur l'opposition entre contrôle étatique et liberté d'usage au regard du droit.

Enfin, le champ d'application de la cryptologie apparaît aujourd'hui sans borne. Les innovations en la matière n'ont pour frontières que les limites de l'inventivité humaine : informatique en nuage, monnaies virtuelles décentralisées, code à exécution garantie. Un dernier chapitre examinera les menaces que soulève cette conquête au-delà des frontières de l'utopie.

## QUELQUES ÉTAPES MAJEURES DE LA RENCONTRE ENTRE CRYPTOLOGIE ET INFORMATIQUE

Les opérations de la Seconde Guerre Mondiale ont révélé combien le contrôle des communications ennemies a pu procurer un avantage décisif sur l'issue du conflit. Outre Atlantique, le travail que Claude Shannon (1915-2001) a mené sur le secret des communications (Shannon, 1949) l'a conduit à élaborer une théorie de l'information grâce à laquelle le développement des communications numériques a été rendu possible (Durand-Richard, 2014). Il a en particulier démontré la sécurité inconditionnelle du chiffrement par masque jetable des téléscripteurs proposé par l'ingénieur Gilbert Vernam[1] (1890-1960), où chaque caractère transmis est combiné avec un autre caractère, inscrit sur une bande perforée aléatoirement et jetée après usage. Deux bandes aléatoires sont nécessaires : l'une au chiffrement et l'autre identique au déchiffrement. Ce mécanisme, réservé aux communications hautement secrètes, a été utilisé dans le téléphone rouge mis en place entre Washington et Moscou après la crise des missiles de Cuba en 1962. Ce système requiert de partager préalablement une quantité de bandes aléatoires égale à la taille des échanges sécurisés qu'elles permettent.

Le développement des traitements informatisés et le stockage massif de données personnelles sur ordinateurs a conduit à poser la question de leur confidentialité pour le respect de la vie privée (Feistel, 1973). Auparavant cantonnée aux milieux militaires, la cryptographie va émerger dans le monde civil avec la publication en 1973 d'un appel d'offres par le *National Bureau of Standards* (NBS) américain pour définir un algorithme de chiffrement qui serait utilisable par les entreprises qui ont besoin de protéger leurs informations sensibles. Cet appel d'offres va conduire à la normalisation en 1976 du DES (*Data Encryption Standard*) pour l'usage civil, et à sa publication en janvier 1977. Cet algorithme est issu d'une famille d'algorithmes appelés *Lucifer*, conçus chez IBM (*International Business Machines*) par Horst Feistel (1915-1990). L'émergence du chiffre dans le monde civil va en faire évoluer les usages, la carte à puce verra son emploi se généraliser comme dispositif de traitement cryptographique, du paiement au téléphone mobile. L'augmentation considérable de la puissance de calcul des ordinateurs va obliger à reconsidérer le niveau de sécurité des mécanismes de protection. Leur mise en réseau au niveau mondial change la nature des communications et induit de nouveaux besoins pour établir la confiance dans les nouvelles relations inter personnelles ainsi créées. Les mécanismes de protection dans lesquels les utilisateurs doivent préalablement échanger une clé secrète connue d'eux seuls ne sont plus utilisables dans ce nouveau contexte d'interconnexion généralisée et ouverte. L'article fondateur (Diffie *et al*. 1976) de Whitfield Diffie (né en 1944) et Martin Hellman (né en 1945) va initier la *révolution des clés publiques*. Cette nouvelle cryptographie paradoxale a pour objet de sécuriser les communications entre ordinateurs et de résoudre le problème de protection des échanges sans accointance préalable. La cryptographie réduit la part secrète pour devenir asymétrique, distinguant la clé pour le chiffrement et la clé pour le déchiffrement. La première est publique, inscrite dans un annuaire ouvert à

[1] Brevet US1310719 A du 22 juillet 1919.

tous. Seule la seconde doit demeurer secrète et privée, connue du seul destinataire. Cette cryptographie asymétrique ouvre de nouveaux services comme la signature numérique non répudiable, au cœur de nombreuses relations contractuelles. Un document signé avec une clé privée peut être authentifié par tous grâce à la clé publique correspondante. Sans ces nouveaux mécanismes largement diffusés et rendus accessibles au grand public, le réseau Internet n'aurait jamais pu atteindre l'extraordinaire développement qu'on lui connaît. Maintenant qu'il est devenu le seul vecteur de communications électroniques, l'usage de la cryptologie n'est plus une option. Elle est la condition sans laquelle aucune confiance n'est possible dans ces échanges. Désormais, les évolutions de l'informatique et de la cryptologie ne peuvent plus être pensées séparément.

### ART OU SCIENCE

Au moins jusqu'au dix-neuvième siècle, les innovations en matière de chiffrement furent le plus souvent le fait d'amateurs, érudits certes, et proches des cercles du pouvoir et du savoir, mais qui pratiquaient la cryptologie en dehors de leur activité principale. Les inventeurs du chiffre polyalphabétique étaient architecte (Alberti, 1404-1472), moine (Trithème, 1462-1516), clerc proche du pouvoir (Belaso, 1501-?), physicien, mathématicien et naturaliste (Porta, 1535-1625) ou encore diplomate (Vigenère, 1523-1596). Les praticiens de la cryptologie, les secrétaires chiffreurs proches des rois, doivent pouvoir écrire une lettre en chiffres sans que cela ne leur demande plus d'attention qu'une dépêche ordinaire[2]. À l'opposé, les amateurs « ne sont pas prisonniers de la réalité et peuvent évoluer au firmament de la théorie » (Kahn 1996, p. 126). Ces concepteurs s'auréolaient volontiers du pouvoir de maîtriser le mystère des chiffres, propre à la recherche du sens caché d'un monde arrangé par le nombre. Comme c'est le cas pour bien des corporations de métiers, ces artisans réservaient l'exclusivité de leur savoir-faire à leur communauté : « Afin de les garantir et soustraire au profanement de la multitude, et en laisser la connaissance aux gens dignes, […] à peu de gens divulguez artifices »[3].

Concevoir des moyens de protection reste un métier qui combine art et science, comme en témoigne la section « l'art et la science de la cryptologie » dans l'article de John Jack Irving *From Hut 8 to Newmanry* (Copeland *et al.*, 2006). Les mécanismes de chiffrement restent encore aujourd'hui le résultat d'une coopération entre mathématiciens et ingénieurs, dont le travail a conservé son aspect bricoleur et artisanal qui fait autant appel à l'ingéniosité qu'au bagage mathématique des concepteurs. Les définitions récentes des derniers standards AES (*Advanced Encryption Standard,* algorithme Rijndael, 1998) et SHA3 (*Secure Hash Algorithm*, algorithme Keccak, 2012) montrent clairement l'application de tours de main propres à une méthode de conception qui met en avant savoir-faire et ingéniosité, inscrivant cette activité créatrice dans le domaine de l'art. À ce stade, les mathématiques sont un outil dont disposent ces artisans concepteurs, tout comme elle est une partie importante de la formation des ingénieurs.

---

[2] François de Caillère, *De la manière de négocier avec les Souverains*, Amsterdam, 1716.
[3] Blaise de Vigenère, *Traité des chiffres ou secrètes manières d'écrire*, 1585.

Une première étape vers la revendication d'une démarche scientifique a été franchie avec l'avènement de la cryptographie à clé publique (Diffie & Hellman, 1976). La théorie des nombres a été mobilisée pour concevoir le premier mécanisme qui met en application ce principe : le RSA. Les chercheurs Ronald Rivest (né en 1947), Adi Shamir (né en 1952) et Leonard Adleman (né en 1945) ont exploité ingénieusement la dissymétrie de difficulté entre multiplication et factorisation pour concevoir le moyen de camoufler une information[4] en utilisant comme paramètre public un entier égal au produit de deux facteurs premiers, soigneusement tenus dissimulés, pendant que ces facteurs sont mis à contribution pour résoudre le cryptogramme qui en résulte. Dès lors les mathématiques ont pris une part de plus en plus importante dans la conception de tels mécanismes, allant jusqu'à mobiliser des pans entiers de domaines d'études jusque là élaborés pour leur valeur intrinsèque, comme par exemple la géométrie algébrique et les courbes elliptiques (Koblitz, 2007).

La seconde étape qui renforce la relation entre cryptologie et mathématiques est l'élaboration controversée de fondements théoriques amenant à la notion de preuve de sécurité. Les auteurs de cette cryptographie qu'ils qualifient de moderne, comme Oded Goldreich (né en 1957), Jonathan Katz (né en 1974) ou Yehuda Lindell (né en 1971) revendiquent avec force le caractère scientifique de leur démarche, affirmant dans la préface de leur ouvrage (Katz *et al*., 2007) que « [cette approche moderne] a changé la cryptographie d'art en science ». Cette théorie est née du besoin d'avoir, dès la conception, des garanties de sécurité dans la durée afin d'échapper à la course sans fin entre codeurs et briseurs de codes, course qui conduit aux sempiternels correctifs de sécurité propres aux conceptions classiques. Un des apports fondamentaux de cette théorie est d'avoir établi que la cryptographie symétrique – avec clé secrète partagée par les deux correspondants – repose sur l'axiome d'existence de fonctions dites *à sens unique*, ces fonctions dont les valeurs sont facilement calculables grâce à la connaissance d'un algorithme efficace, alors que trouver un antécédent pour une valeur donnée au hasard se révèle en pratique inaccessible. La dissymétrie entre calcul de valeur et calcul d'antécédent est manifeste pour la multiplication : calculer le produit de deux nombres premiers se réalise facilement, alors que factoriser le résultat est considéré aujourd'hui encore comme extrêmement difficile dès lors que le nombre à factoriser dépasse quelques centaines de chiffres. La cryptographie à clé publique repose, elle, sur l'hypothèse plus forte d'existence de *fonctions à sens unique avec trappe* (*trapdoor functions*). Ces dernières sont des fonctions difficiles à inverser sauf à supposer la connaissance d'une information supplémentaire, la *trappe*, qui rend accessible le calcul d'un antécédent. C'est ainsi que le chiffre RSA est en pratique impossible à inverser, sauf à connaître les facteurs de l'entier qui constitue le paramètre public.

Cette notion de preuve de sécurité a été remise en cause par des mathématiciens comme Neal Koblitz (né en 1948). Ce dernier, tout en reconnaissant le fondement mathématique de cette théorie, s'insurge contre l'emploi de termes comme *preuve* et *théorème* utilisés par les thuriféraires de

[4] Publié pour la première fois dans la rubrique des jeux mathématiques de Martin Gardner, *Scientific American,* 1977, vol. *237-238*, 120-124.

cette cryptologie moderne. Ces mots induisent l'idée d'une certitude totale alors que la sécurité d'un système de confidentialité repose sur des éléments fortement subjectifs, où l'appréciation et la spéculation sont des éléments centraux : quels seront les progrès accomplis pour résoudre un problème considéré aujourd'hui comme pratiquement insoluble ? Comment évoluera la puissance de calcul des ordinateurs ? Quel sera l'angle d'attaque de l'adversaire ? Au regard de ces questions, des doutes sont permis sur le caractère exclusivement scientifique de la cryptologie. De fait, un chiffre est considéré comme sûr tant qu'il n'a pas été cassé, sa sécurité étant à mettre en rapport avec la durée ou la valeur du secret qu'il protège. L'historien de la cryptologie David Kahn (né en 1930) affirme par ailleurs que la cryptologie reste une activité de nature essentiellement sociale, dont l'objet est la communication secrète, communication et secret étant deux notions du ressort des sciences de l'homme au cœur du comportement culturel (Kahn, 1996, p. 752).

## LES FRONTIÈRES IMAGINAIRES DES MONDES D'IMPAGLIAZZO

Le développement d'une théorie de la complexité des algorithmes fait suite aux travaux de Turing sur la calculabilité (Turing, 1936). Son développement au cours de la deuxième moitié du vingtième siècle a conduit à distinguer plusieurs classes de problèmes selon la complexité des algorithmes pour les résoudre. La qualité d'un chiffre revendiquant l'impossibilité d'élucider un cryptogramme en l'absence de la clé de déchiffrement, les cryptologues se sont naturellement penchés sur cette théorie. Ainsi la classe P est celle des problèmes pour lesquels il existe un algorithme de résolution efficace, c'est-à-dire s'exécutant sur une machine de Turing déterministe, et dont la complexité est bornée par un polynôme de la taille des données traitées. Ces problèmes sont ceux que l'on sait résoudre en pratique, du moins tant que le degré du polynôme et la valeur du coefficient dominant restent raisonnables. Cela doit être le cas du chiffrement ou du déchiffrement en toute connaissance de la clé. Une autre classe remarquable est la classe NP, pour *Non-deterministic Polynomial.* Elle est celle des problèmes pour lesquels il existe un algorithme efficace s'exécutant sur une machine de Turing *non déterministe*, c'est-à-dire une machine qui, à chaque pas de son exécution, comporte plusieurs choix possibles de déroulements. Après avoir démontré l'équivalence des langages reconnus par les automates à mémoire finie déterministes et par les automates à mémoire fine non déterministes, la théorie s'est naturellement penchée sur cette question d'équivalence entre déterminisme et non déterminisme pour les machines de Turing. La difficulté de démontrer ou d'infirmer le moindre résultat a conduit finalement à la fameuse conjecture P = NP qui est l'un des grands problèmes encore non résolus du prix du millénaire, proposée en 2000 par l'Institut de Mathématiques Clay[5].

Une machine non déterministe peut être vue comme guidée par un oracle qui lui indique la marche à suivre, la direction à prendre parmi tous les choix ouverts à chaque pas du programme, afin d'aboutir au plus vite au résultat. Lorsque la solution au problème est connue, elle peut tenir lieu d'oracle, de telle sorte qu'un problème NP peut être considéré comme un problème dont la

[5] http://www.claymath.org/millennium-problems

vérification est réalisable avec un algorithme efficace. Mais nombre de problèmes difficiles qui présentent un intérêt pratique sont de ceux dont la solution est vérifiable en temps raisonnable, c'est-à-dire justement des problèmes NP.

Il existe encore aujourd'hui des problèmes, comme la factorisation des entiers, qui sont en pratique bien plus difficiles à résoudre qu'à vérifier. Cette dissymétrie est-elle intrinsèque au problème, ou bien n'est-elle due qu'à notre ignorance ? Découvrirons-nous dans l'avenir un algorithme efficace de factorisation ? Ou bien prouverons-nous que ce problème est d'une difficulté telle qu'il est illusoire de chercher un tel algorithme ? Nous sommes ainsi aujourd'hui en pratique dans un monde où $P \neq NP$. Mais cette appartenance reste virtuelle dans la mesure où elle n'est peut-être que provisoire – ou définitive – en attendant que ne soit prouvée – ou infirmée – l'identité des classes P et NP.

Un problème NP est appelé *complet* si tous les problèmes NP peuvent s'y ramener efficacement. Ils apparaissent ainsi parmi les problèmes les plus difficiles de cette classe. Mais ce niveau de difficulté est insuffisant pour traiter de ce qui survient en cryptographie. Dans leur article fondateur de la cryptographie à clé publique (Diffie *et al*., 1976), Diffie et Hellmann ont invité les chercheurs à fonder leur nouvelle cryptographie sur des problèmes NP complets, en proposant l'exemple du problème du sac à dos. Ce problème consiste à choisir dans une liste d'entiers quels sont ceux dont la somme atteint une valeur donnée. Plusieurs propositions en ont résulté, mais qui ont toutes été successivement cassées, les instances pratiques de ce problème étant en moyenne faciles à résoudre. Les chercheurs ont finalement abandonné toute velléité d'appliquer le problème du sac à dos à la cryptographie[6].

La difficulté attendue des problèmes cryptographiques est une difficulté *en moyenne* (Levin, 1986). Cette théorie a été développée par Leonid Levin (né en 1948) et a inspiré au chercheur Russel Impagliazzo (né en 1963) la possibilité de cinq mondes qui diffèrent selon le type de problèmes qu'il est possible ou non de résoudre avec efficacité dans chacun d'eux (Impagliazzo, 1995). Impagliazzo a vulgarisé cette théorie en illustrant la visite guidée de ses cinq mondes par l'usage de la cryptographie, mais aussi par une mise en scène métaphorique du personnage Grouse[7], professeur imaginaire du jeune élève Gauss, qui voulait poser à son élève une colle sévère en demandant la somme des entiers de 1 à 100. Après avoir été humilié par la réponse rapide du jeune Gauss, Impagliazzo raconte que le malheureux professeur a passé le reste de sa vie, jusqu'à la folie, à chercher sans succès un problème qui pourrait mettre fin à l'arrogant succès de son élève. Voici une présentation de ces cinq mondes hypothétiques dans laquelle l'accent est mis sur leur rapport à la cryptologie et sur les frontières qu'ils déterminent.

**Algorithmica.** Ce monde est celui dans lequel P = NP. Il y existe une méthode pour produire la solution d'un problème à partir d'un algorithme de vérification de cette solution. Grouse ne peut pas coller Gauss avec un

[6] La recherche bouillonne cependant d'applications d'autres problèmes NP complets à la cryptographie dite *post quantique* qui adviendra lorsque l'ordinateur quantique deviendra une réalité.

[7] *To grouse,* rouspéter.

problème dont il présenterait la solution au reste de la classe, puisque ce dernier pourrait trouver la solution directement à partir de l'algorithme de vérification. L'informatique s'en trouve révolutionnée. L'ordinateur peut se charger de tâches dévolues aux humains. Parler une langue naturelle se réduit à savoir lire et interpréter un corpus réduit de textes. Savoir multiplier revient à savoir factoriser. Déchiffrer et décrypter, avec ou sans la clé, sont des problèmes de difficulté équivalente. Aucune cryptographie n'y est possible autre que le masque jetable du téléphone rouge. Dans ce monde, de transparence maximale, il est impossible de réserver l'accès à une information à certaines personnes seulement sans que toutes ne puissent également y accéder. Le prix à payer, à savoir résoudre tous les problèmes algorithmiques de la vie courante, est l'impossibilité d'y conduire la moindre cryptographie efficace.

**Heuristica.** Heuristica est un monde ou les problèmes NP ne sont difficiles à résoudre que dans le pire des cas. En moyenne, la résolution reste accessible à un algorithme efficace. En pratique, ce monde est en presque tout point comparable à Algorithmica. La différence réside dans l'existence de rares problèmes pratiquement insolubles. Supposons par exemple que la recherche de l'expression mathématique d'un problème prenne un temps $t$, et sa résolution un temps $2t$. Comme tout chercheur le sait, la réponse à un problème conduit invariablement à un nouveau problème. En Heuristica, ce deuxième problème, qui survient au bout d'un temps $3t$ prend un temps $6t$ à être résolu. La récurrence est géométrique, et en quelques itérations, la frontière de l'infaisable est rapidement atteinte. Les instances difficiles des problèmes NP existent, mais sont également difficiles à trouver. Le temps moyen pour résoudre un problème NP reste comparable à celui pour en concevoir l'énoncé. Grouse peut coller Gauss avec un problème difficile, mais, raconte Impagliazzo, il lui faudra au moins deux fois plus de temps pour l'établir qu'à Gauss pour le résoudre – n'oublions pas que Gauss est un élève particulièrement brillant. D'un point de vue cryptographique, le temps passé à trouver un chiffre correspond au temps pendant lequel le secret est garanti. En Heuristica, il n'y a pas plus d'espoir qu'en Algoritmica de trouver une cryptographie efficace.

**Pessiland.** Selon Impagliazzo, ce monde est le pire qui soit. Il existe des problèmes difficiles à résoudre en moyenne, mais pour toute fonction efficacement calculable, il existe une façon efficace de trouver un antécédent à une valeur donnée. En d'autres termes, il n'existe pas en Pessiland de fonction à sens unique. Il est facile de produire des instances difficiles de problèmes NP, mais il n'est pas possible de produire des instances difficiles de problèmes dont la solution soit connue. En Pessiland, Grouse peut poser à Gauss une colle insoluble, mais rien, y compris la grande clairvoyance de Gauss, ne pourra en pratique conduire à une solution. L'humiliation de Grouse restera entière lorsque la classe demandera la réponse au professeur qui aura toutes les difficultés du monde pour en exhiber une. Comme la théorie cryptographique fonde le chiffrement symétrique – celui où les deux participants partagent la même clé – sur l'existence de fonction à sens unique, Pessiland n'autorise pas une telle cryptographie. Ce monde agaçant cumule tous les désavantages.

**Minicrypt.** En Minicrypt, les fonctions à sens unique existent. La cryptographie symétrique est possible, mais pas le chiffrement à clé publique. Deux correspondants devront préalablement s'accorder sur une clé secrète, fusse-t-elle de taille réduite, pour pouvoir échanger par la suite de façon tout à fait discrète une très grande quantité d'informations sur un canal public. Une fonction à sens unique $f$ peut être utilisée pour produire un problème difficile dont ont connaît une solution, par exemple en tirant un élément $x$ au hasard, en calculant $y = f(x)$ et en posant le défi de trouver un antécédent à $y$. Dans ce monde, Grouse garde la tête haute, car il peut poser à Gauss un problème que ce dernier aura bien du mal à résoudre. Il pourra même exhiber fièrement la solution à la classe ébahie et remporter une certaine victoire. La théorie cryptographique montre qu'en Minicrypt, les fonctions à sens unique permettent de produire des signatures à clés asymétriques, une clé privée pour produire la signature et une clé publique pour sa vérification. Contrairement à ce que suggéraient Diffie et Hellman, la frontière n'est pas entre cryptographie symétrique et asymétrique, mais entre Minicrypt, où les fonctions à sens unique n'ont pas de trappe, et le monde suivant : Cryptomania.

**Cryptomania.** Cryptomania est en pratique notre monde actuel. La cryptologie à clé publique y est possible. Deux correspondants peuvent s'accorder sur un secret partagé commun à partir de données qu'ils s'échangent publiquement. Cette cryptographie à clé publique repose sur des *fonctions à sens unique à trappe*. Ainsi, tout le monde peut chiffrer un message, mais le déchiffrement reste réservé au seul détenteur de la trappe qui tient lieu de clé privée. En Cryptomania, Grouse peut enfin asseoir son autorité en posant à la classe entière un problème pratiquement impossible à résoudre. Mieux, il peut humilier Gauss en révélant au reste de la classe une indication qui permettra aux autres élèves d'accéder à la solution, alors que pour le pauvre Gauss resté dans l'ignorance de cette indication, le problème restera définitivement insoluble. En Cryptomania, les possibilités de la cryptologie n'ont de limites que celles de l'imagination des concepteurs : vote électronique, monnaie digitale anonyme, manipulation de données chiffrées. Le niveau d'intimité de la sphère privée n'est pas limité par la technique, mais seulement par des décisions sociales ou politiques qui dictent la connaissance des trappes.

Cette visite guidée d'Impagliazzo se termine sur un cri d'alarme : si une façon efficace de factoriser ou de calculer des logarithmes discrets venait à être découverte, alors non seulement la plupart des systèmes cryptographiques à clé publique viendraient à être cassés, mais il n'y aurait aucune méthode systématique applicable pour concevoir une alternative sûre. Il n'y aucune raison théorique connue à la difficulté intrinsèque de la factorisation ou du logarithme discret[8]. Notre confiance dans leur difficulté repose sur notre ignorance de méthode efficace de résolution, après plus de quarante années d'intenses recherches sur cette question. Mais les progrès accomplis – surtout

[8] Le problème du logarithme discret consiste à trouver, pour un entier $y$, l'exposant $x$ tel que $y = g^x$ modulo $p$, où $p$ est un nombre premier et $g$ est un générateur du groupe multiplicatif des entiers modulo $p$. La difficulté de ce problème, lorsque l'entier $p$ est grand, permet aussi de construire une cryptographie à clé publique.

des progrès dans la puissance de calcul des ordinateurs – ont frappé d'obsolescence les clés publiques produites aux débuts de cette nouvelle cryptographie[9], et il est impossible de dire quelle taille de clé est convenable aujourd'hui pour garantir une sécurité pour les vingt prochaines années. L'édifice de la cryptographie à clé publique est bâti sur du sable. Cette fragilité semble inquiéter jusqu'en haut lieu, en témoigne la tenue du congrès annuel *Catacrypt*[10]*,* dont l'objet, depuis 2014, est d'anticiper un effondrement de la sécurité des fonctions cryptographiques actuelles. Ce congrès est parrainé par les plus grandes organisations dont la cryptologie à clé publique est au cœur de l'activité.

**SECRET ET TRANSPARENCE**

Bien qu'elle n'apparaisse pas explicitement, la cryptographie est présente dans la plupart des échanges quotidiens dès lors qu'ils sont traités numériquement ou qu'ils ont lieu sur des canaux de communication ouverts. Les échanges sur Internet n'ont pu se développer qu'à partir du moment où la cryptographie a pu en garantir la sécurité, que ce soit en matière de discrétion par le chiffrement des informations transmises, ou pour s'assurer de l'identité réelle de l'interlocuteur par son authentification. Ces deux types de mécanismes – chiffrement et authentification – sont mis en œuvre lors de toute communication par téléphone portable, même si l'utilisateur n'en a pas l'entière conscience. Cette banalisation du secret va pourtant à l'encontre de l'idée de la transparence, longtemps affirmée comme constitutive de la démocratie. Les décisions arbitraires rendues dans les sphères occultes d'un pouvoir secret sont en principe le fait de régimes qualifiés d'autoritaires, tyranniques ou dictatoriaux. Ce qui est caché et secret en politique est souvent considéré comme suspect. Aussi la transparence est-elle traditionnellement chargée d'une valeur positive, par opposition au secret chargé, lui, d'une valeur négative.

La relation entre secret et transparence devient d'autant plus problématique que les valeurs autour de ces notions tendent à s'inverser. Les États se font de plus en plus pressants pour limiter l'usage de la cryptologie dans le but d'exercer leurs prérogatives dans la nécessaire lutte contre le terrorisme. En la matière, le chiffrement des communications est considéré comme un facteur aggravant (Tréguer, 2019). En atteste par exemple la décision d'un juge madrilène de maintenir en prison sept personnes, dans le cadre de perquisitions menées en 2014 et visant le mouvement anarchiste, avec comme argument qu'ils « utilisaient des e-mails avec mesures de sécurité extrêmes, telles que l'utilisation d'un serveur Riseup »[11]. En réponse à cette décision de maintien en détention, le collectif Riseup, qui propose des outils de protection à destination des mouvements sociaux, a réagi en s'insurgeant contre une décision qui

[9] Le chiffrement RSA a été présenté en 1977 sous le titre « Un nouveau système de chiffrement qui prendrait des millions d'années à casser ». la clé de 129 chiffres décimaux a été factorisée en 1994 (Guillou, 2014).

[10] *Workshop on catastrophic events related to cryptography and their possible solutions, http://catacrypt.org.*

[11] http://www.x-pressed.org/?xpd_article=spain-judge-orders-the-detention-of-7-of-the-11-arrested-in-operation-pandora

assimile « la protection de la vie privée sur Internet à du terrorisme »[12]. Cette exigence d'ouverture notifiée à des pans entiers de la vie personnelle évolue comme un vecteur de surveillance dont la banalisation marque le caractère incontrôlé[13]. Elle est le signe d'un pouvoir dominateur, chargeant cette transparence imposée d'une valeur négative, tandis que la cryptographie opère comme un outil de défense de la vie privée, attribuant au secret qu'elle procure la valeur positive de préservation d'un espace de liberté personnelle. En témoignent les mots de Soljenitsyne : « notre liberté se bâtit sur ce qu'autrui ignore de nos existences » (cité par Huyghe, 2009, p. 12). En déplaçant la frontière entre sphère privée et domaine public, l'usage massif et souterrain de la cryptologie modifie ainsi la structure et la signification des relations sociales.

Et plus encore, une rupture s'introduit dans les grilles de lecture qui structurent notre représentation des connaissances. Ainsi, là où elle était porteuse d'universalité, la communication semble s'exercer au sein de communautés d'intérêt qui, si elles sont très vastes, n'en demeurent pas moins fermées, marquant plutôt l'appartenance à un groupe. Que la cryptologie intervienne pour garantir la sécurité des échanges signifie que ces échanges ont lieu entre partenaires sélectionnés. La cryptologie peut alors devenir un outil d'exclusion. De ce fait, le schéma dominant des communications au sein des réseaux sociaux favorise un entre soi qui élimine les oppositions, consacrant une démarche d'évitement des contradictions. Au lieu de conduire à un mouvement dialectique permanent de foisonnement et de renouvellement des idées, on observe au sein de ces communautés une convergence vers un point de vue figé et statique, voire régressif, accentuant les contradictions entre groupes sans perspective de résolution des conflits. Le résultat est davantage une opposition marquée entre communautés plutôt qu'une synthèse des points de vue. Cette évolution est bien loin de l'idéal d'un monde de communication universelle promue par les pionniers d'Internet portés par une vision utopiste d'ingénieurs, bien peu étayée par une réflexion philosophique ou sociologique.

La cryptologie, clé de voûte du droit à l'anonymat et du secret des correspondances, mais aussi outil de domination au service d'un pouvoir toujours plus intrusif, joue un rôle à la fois libérateur et sclérosant. La liberté se joue à l'intérieur d'un ensemble organisationnel qui est conçu, géré et donc contrôlé par les pouvoirs qui en organisent le fonctionnement systémique. Les comportements qui n'obéissent pas aux règles imposées sont éliminés. En rétablissant un espace de protection des données et des échanges personnels, la cryptologie agit comme un outil de préservation d'un espace de liberté. Cette fonction duale est particulièrement révélée à travers les soubresauts des lois et réglementations qui ont régi l'emploi du chiffre en France[14] – et dans la plupart des pays occidentaux –, entre le statut d'arme jusqu'en 1986 – date du premier décret permettant de déroger aux règles sur l'exportation des matériels de

[12] https://riseup.net/en/security-not-a-crime

[13] Il existe cependant quelques tentatives de limitation du caractère incontrôlé, à l'instar de la CNIL (Commission Nationale de l'Informatique et des Libertés) en France.

[14] Voir dans http://binaire.blog.lemonde.fr/2017/10/27/chiffre-securite-et-liberte/ l'interview du Général Jean-Louis Desvignes, ancien Directeur du Service Central de la Sécurité des Systèmes d'Information (SCSSI).

guerre s'agissant d'usages commerciaux de la cryptographie – et l'usage libre tel qu'il a été promulgué en 2004 dans la loi sur la « confiance dans l'économie numérique ». La section suivante développe cette évolution.

**DU CONTRÔLE ÉTATIQUE À LA LIBERTÉ D'USAGE**

Longtemps inscrite au registre des armes de guerre de deuxième catégorie, la cryptologie s'impose aujourd'hui dans les échanges commerciaux et privés, notamment en France depuis que l'usage en a été libéralisé. Cette libéralisation a initialement été menée contre l'avis des milieux militaires pour sécuriser le commerce électronique afin d'en favoriser le développement. La réglementation française de 1998 en matière de cryptologie montrait l'ambivalence de la politique à mener :

> « Dans le cadre de la protection des personnes et des biens, de la sécurité intérieure et de la défense nationale, l'État doit mettre en place les mesures nécessaires pour éviter que ces technologies ne facilitent, en toute impunité et en toute discrétion, le développement d'actions ou de trafics illégaux (petite et grande délinquance, terrorisme, mafia, pédophilie, blanchiment d'argent, fraudes financières, espionnage industriel…) […]. La réglementation française en matière de cryptologie établit un équilibre entre les besoins légitimes de protection des données privées et les missions publiques de protection des personnes et des biens et de la sécurité intérieure et extérieure »[15].

Comment en effet concilier les intérêts fondamentaux de défense et de sécurité des systèmes d'information des institutions avec la protection de la vie privée et le secret des correspondances, inscrits dans les principes de tout système démocratique ?

La question de la dualité des outils de protection des données se pose dans les mêmes termes en ce qui concerne l'anonymat. Ce dernier est reconnu comme une composante essentielle du droit fondamental à la vie privée dans le cyberespace, qui devrait fonctionner selon une logique de « moindre révélation »[16]. Un échange commercial sur Internet ne devrait pas révéler plus que ce qui est strictement nécessaire à la transaction. « Quand j'achète un magazine dans une boutique et que je paye en espèce au caissier, il n'a aucune raison de savoir qui je suis. […]. Lorsque mon identité est révélée par le mécanisme sous-jacent, ma vie privée n'est pas respectée »[17]. D'autre part, ce droit à l'anonymat est présenté comme un obstacle aux initiatives destinées à

---

[15] Christian Pierret, Secrétaire d'État à l'Industrie, *La réglementation française en matière de cryptologie*, juin 1998, cité par Georges Chatillon dans
http://www.pantheonsorbonne.fr/diplomes/master-droit-du-numerique/bibliotheque-numerique-du-droit-de-ladministration-electronique/tic/informatique/
cryptographie/la-nouvelle-liberte-de-crypter-en-1999-comment-la-dechiffrer/

[16] Lawrence Lessig, *Code is law – On liberty in Cyberspace*, Harvard Magazine, janvier 2000.

[17] Eric Hughesn 1993, *A cypherpunk manifesto*, https://www.activism.net/cypherpunk/manifesto.html

lutter contre la prolifération de contenus illicites, malveillants ou illégaux, les délits financiers ou les atteintes au droit d'auteur[18].

Des solutions ont été élaborées en France et aux États-Unis pour tenter de concilier d'une part les intérêts de défense et de sécurité des systèmes d'information des institutions et la protection de la vie privée, et d'autre part la capacité des services de police de mener à bien leur mission de renseignement. Le chiffrement d'échanges entre personnes surveillées peut en effet entraver les interceptions et dissimuler les communications des délinquants et des criminels. Il est accusé de « restreindre les prérogatives de l'État en lui interdisant d'exercer en totalité sa souveraineté.»[19]

Aux États-Unis, à partir de 1993, l'administration a voulu imposer le *clipper chip*, une puce électronique conçue par la *National Security Agency* (NSA), l'agence de sécurité américaine, et contenant un processeur de traitement cryptographique. Ce composant était destiné à doter tous les appareils de chiffrement destinés au grand public et devait permettre aux services gouvernementaux d'accéder aux clés L'administration aurait alors eu la capacité d'accéder aux communications en cas de besoin. La conception de cette puce a provoqué la levée de vives protestations de la part d'organisations qui, à l'instar de la compagnie *RSA Security*, ont fait campagne en faveur d'un usage libre de la cryptographie. Le projet a finalement été abandonné en 1996, conduisant de fait à un usage domestique libre des moyens de chiffrement.

En France, l'article 28 de la loi de réglementation des télécommunications du 29 décembre 1990 fixait deux régimes : un régime strict d'autorisation pour les moyens assurant une fonction de confidentialité, c'est-à-dire qui chiffre le contenu des communications pour les rendre inintelligibles aux tiers, et un régime de simple déclaration pour les moyens assurant des fonctions d'authentification et de signature sans permettre le chiffrement des données. Le développement d'Internet et l'intégration de fonctions cryptographiques dans la plupart des logiciels de navigation et de messagerie ont conduit la France à assouplir sa position[20] en matière de chiffrement et à rendre libre son utilisation dans deux cas :

- lorsque la cryptologie est affaiblie par une taille de clé réduite à 40 symboles binaires, ce qui permet de la retrouver par recherche exhaustive sur les $2^{40}$ clés possibles,
- lorsque les clés sont gérées par un organisme agréé appelé *Tierce Partie de Confiance* (TPC).

Ce système de contrôle des instruments de cryptographie a encore été jugé comme trop pesant, la libéralisation des moyens de chiffrement comme préalable à l'essor des technologies de l'information étant présentée comme une évidence. Elle a conduit successivement le législateur à autoriser l'usage

[18] Rapport du groupe de protection des personnes à l'égard du traitement des données à caractère personnel (groupe « Article 29 ») *L'anonymat sur Internet*. Rapp. 3/97. Bruxelles, Commission européenne, 1997.

[19] http://www.ssi.gouv.fr/archive/fr/sciences/fichiers/rapports/rapport_orientation_ssi_2008.pdf, Rapport public d'orientation des travaux de recherche et de développement en matière de sécurité des systèmes d'information, 2008.

[20] http://www2.droit.parisdescartes.fr/warusfel/articles/reglcrypto_warusfel.pdf

des clés de 56 symboles binaires en 1998, puis 128 en 1999. L'usage du chiffrement devenait de fait libre, ce qu'a consacré la *loi pour la confiance dans l'économie numérique* du 21 juin 2004, qui, dans son article 30, affirme que « l'usage des moyens de cryptologie est libre ».

Les attentats du 11 septembre 2001 ont bouleversé la situation. Les services de renseignement ont à nouveau réclamé un contrôle strict sur la cryptologie. L'opinion publique semblait accepter, pour sa sécurité, le sacrifice d'une partie de sa liberté. En témoigne le *Patriot Act*, du 26 octobre 2001 qui autorise les services de sécurité des États-Unis à accéder aux données détenues par les particuliers et les entreprises. Ce dispositif a été renforcé par le *Cloud Act* du 21 mars 2018 qui contraint les fournisseurs de services à fournir ces données. Mais le retour à la situation antérieure n'était plus possible. La cryptographie devenue forte empêchait désormais d'accéder directement aux données chiffrées. Elle ne pouvait donc qu'être contournée. Il s'en est suivi une politique officieuse et non dite de portes dérobées (*backdoor*), ces points d'accès occultes aux clés de chiffrement mis en place dans les équipements eux-mêmes, cachés à l'utilisateur mais connus des services gouvernementaux qui ont ainsi accès aux communications chiffrées. De nombreux journaux (Le Monde, Der Spiegel, The Guardian) ont ainsi évoqué dès 2013 la surveillance par les États-Unis des téléphones personnels de plusieurs « leaders internationaux », dont la chancelière allemande Angela Merkel (née en 1954), révélant implicitement un moyen d'accès à ces communications chiffrées.

Un autre moyen de contourner la force de la cryptographie résultant de la non limitation des tailles des clés autorisées est d'en réduire l'entropie réelle. Une clé constituée de 128 symboles binaires aléatoires a théoriquement une entropie de 128 bits, avec pour conséquence que la recherche exhaustive nécessite un travail de $2^{128}$ essais, ce qui est totalement hors de portée de toute machine imaginable. Mais si les 128 symboles binaires sont le résultat d'un calcul d'expansion sur une donnée plus courte, par exemple de 56 symboles aléatoires, complété par 72 symboles binaires redondants, alors l'entropie réelle n'est plus que de 56 bits, et la recherche exhaustive devient accessible aux institutions disposant de moyens de calcul suffisants. Ainsi en 2012, des chercheurs de l'*University of California San Diego*, et de l'*University of Michigan* (Heninger *et al.*, 2019) ont testé un grand nombre de clés publiques RSA disponibles sur Internet. Le résultat a été surprenant : en calculant le PGCD (plus grand commun diviseur) de treize millions de clés publiques prises deux-à-deux, dix-neuf mille – soit 0,14 % – ont pu être factorisées, faisant apparaître un nombre anormal de collisions parmi les facteurs. Ce taux anormalement élevé montre, pour des clés de 1024 symboles binaires, une entropie réelle de 57 bits au lieu des 503 théoriques si les clés étaient vraiment choisies au hasard. Ce niveau d'entropie est largement accessible aujourd'hui à la recherche exhaustive pour qui connaît le processus utilisé pour générer les nombres premiers. Cette situation peut certes être le résultat d'implémentations irréfléchies par des programmeurs mal formés aux subtiles contraintes du développement sécurisé, mais le soupçon d'une faille intentionnelle guidée par une directive étatique ne peut être écarté.

Ce tournant marque le début d'une remise en question de la confiance accordée aux systèmes de protection ainsi qu'une prise de contrôle totale des réseaux par

les pays dont les fournisseurs de produits de cryptologie ont une place dominante sur le marché – États-Unis et Chine – contrôle confirmé par les révélations d'Edward Snowden (né en 1983) de décembre 2013 (Snowden, 2019). Le résultat est une fragilisation de la protection pour la plupart des utilisateurs contre laquelle s'insurgent de nombreux défenseurs des droits humains[21].

**AUX FRONTIÈRES DE L'UTOPIE**

Chaque innovation numérique fait apparaître de nouvelles menaces et la cryptologie est mise à contribution pour les contrer. Une part de plus en plus importante de l'activité humaine est concernée par un traitement algorithmique de données connectées demandeuse de sécurité : diagnostic médical, vote électronique, informatique en nuage, etc. Emblématique de cette évolution, le *bitcoin*, nouvelle monnaie virtuelle crée en 2009, vise à garantir des transactions anonymes en l'absence de banque centrale. Le principe repose sur une chaîne de blocs (*blockchain*), qui est un fichier contenant des pages chaînées les unes aux autres et reproduite à l'identique sur de nombreuses machines d'un réseau non hiérarchique. Ces pages sont protégées par des signatures numériques, le chaînage par une fonction à sens unique. Une preuve de travail assoit la chaîne dans le monde réel et empêche la création d'une copie falsifiée. Produire ce faux prendrait en moyenne le même temps que la production de l'original.

De même que le réseau Internet a permis l'échange et la circulation des informations entre individus sans dispositif centralisé de collecte et de distribution des messages, les *blockchains* permettent la circulation de valeurs entre individus, sans banque centrale ni chambre de compensation, dans la droite ligne du rêve d'un Internet expurgé des hiérarchies sociales. Cet échange de valeur n'est qu'une des fonctionnalités offertes par les *blockchains*, on peut y adjoindre du code exécutable qui en fait une entité programmable. On peut décider par exemple de la date future de la transaction et de conditions pour son exécution comme par exemple l'accord de deux signataires parmi trois. La *blockchain* Ethereum pousse plus loin cette fonctionnalité en incluant sur chaque page du code qui a la garantie de s'exécuter, associant transparence et sûreté. Le réseau devient lui-même une machine de calcul ouverte à tous et sur laquelle l'algorithme s'exécute sans qu'il ne soit possible de l'arrêter ni de le modifier. Il est encore trop tôt pour évaluer combien cette décentralisation remet en question l'organisation d'ensemble de la société. Les preuves de travail nécessaires pour interdire la reproduction d'une fausse chaîne qui apparaîtrait valide sont extrêmement consommatrices en énergie et ne peuvent pas être considérées comme écologiquement durables. Par ailleurs, l'existence d'une organisation *bitcoin core* pour centraliser la production du code des clients du réseau bitcoin montre les limites de la décentralisation et pose la question du contrôle démocratique sur une loi dictée par le code. À l'heure où la neutralité du net subit une profonde remise en cause, le problème du transfert de pouvoir posé en 2000 par le juriste Lawrence Lessig (né en 1961) reste d'une brûlante actualité :

[21] https://www.laquadrature.net/2017/01/24/oln-positionnement-chiffrement/

> « Le code régule. Il implémente un certain nombre de valeurs. Il garantit certaines libertés ou les empêche. Il protège la vie privée ou promeut la surveillance. Des gens décident comment le code va se comporter. Des gens l'écrivent. La question n'est donc pas de savoir qui décidera de la manière dont le cyberespace est régulé : ce sont les codeurs. La seule question est de savoir si nous aurons collectivement un rôle dans leur choix – et donc dans la manière dont ces valeurs sont garanties – ou si nous laisserons aux codeurs le soin de choisir nos valeurs à notre place ».

## RÉFÉRENCES


Copeland B.J. (éd) [2006]. *Colossus, the Secrets of Bletchley Parks's Codebreaking Computers*. Oxford University Press, 2010.

Durand-Richard, M.-J. (2014). Du message chiffré au système cryptographique. In Durand-Richard & Guillot (éds.), *Cryptologie et mathématiques, une mutation des enjeux*. Paris, L'Harmattan, pp. 107-151.

Durand-Richard, M-J & Guillot, Ph. (éd.) (2014). *Cryptologie et mathématiques, une mutation des enjeux*. Paris, L'Harmattan.

Feistel, H. (1973). Crytography and Computer Privacy. *Scientific American, 228*, *5*, 15-23.

Guillou, L. (2014). Pourquoi et comment la cryptologie vient de surgir dans le domaine public : le rôle de la carte à puce. In Durand-Richard et Guillot (éd.), *Cryptologie et mathématiques, une mutation des enjeux*. Paris, L'Harmattan, pp. 203-243.

Heninger, N., Durumeric, S., Wustrow, E. & Halderman, J.A. (2012). Mining Your Ps and Qs: Detection of Widespread Weak Keys in Netword Devices, Actes du 21e *USENIX Security Symposium*, Août 2012.

Huyghe, F.-B. (2009). *Les écoutes téléphoniques*. Paris, Presses Universitaires de France, collection Que sais-je ?

Impagliazzo, R. (1995). A Personnal View of Average-Case Complexity, Actes de la 30e conférence annuelle IEEE *Structure in Complexity Theory*.

Kahn, D., (1996). *The Code-Breakers*. New-York ,NY, Scribner.

Katz, J. & Lindel, Y. (2007). *Introduction to Modern Cryptography*. Boca Rato, FL, CRC Press.

Koblitz, N. [2007]. The Uneasy Relationship between Mathematics and Cryptography. *Notices of the AMS, 54*, *8*, 972-979. Traduit dans Durand-Richard & Guillot (éd.), *Cryptologie et mathématiques, une mutation des enjeux*. Paris, L'Harmattan, 2014, pp. 287-303.

Levin, L. (1986). Average Case Complete Problem. *SIAM Journal of Computing*, *15(1)*, 285-286.

Shannon, C.E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, *28*, 656-715, (oct. 1949.

Snowden, Ed. ( 2019). *Mémoires vives*. Paris, Seuil.

Tréguer, F., (2019). Anonymat et chiffrement, composantes essentielles de la liberté de communications. In Q. Van Enis & C. De Terwange (éd.), *L'Europe de droits de l'homme à l'heure d'Internet*. Bruxelles, Bruylant.

Turing, A.M. (1936). On Computable Numbers, with an Application to the *Entscheidungsproblem*. *Proceedings of the London Mathematical Society*, *42*, *2*, 230-267.

Whitfield, D. & Hellman, M.E. [1976]. New Directions in Cryptography. *IEEE Transactions on Information Theory*, *22*, *6*, 644-54. Traduit dans M.-J. Durand-

Richard & Ph. Guillot (éd.), *Cryptologie et mathématiques, une mutation des enjeux*. Paris, L'Harmattan, 2014, pp. 172-202.