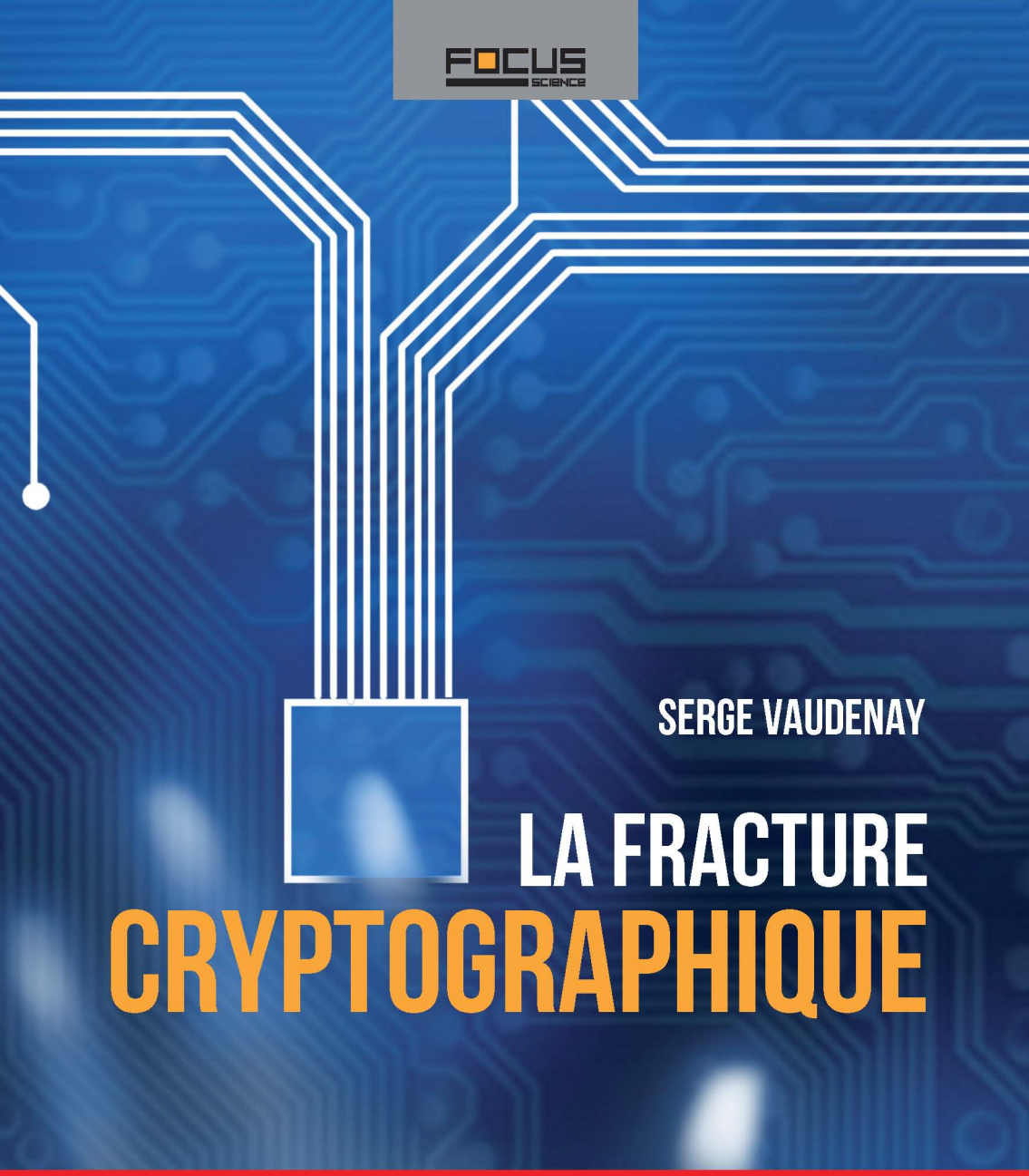
FOCUS SCIENCE



SERGE VAUDENAY

LA FRACTURE CRYPTOGRAPHIQUE

INSÉCURITÉ NUMÉRIQUE: NOS VIES PRIVÉES EN LIBRE ACCÈS?

Presses polytechniques et universitaires romandes

La fracture cryptographique

e-isbn: 978-2-88914-051-0

Version imprimée »

FOCUS SCIENCE

La fracture cryptographique

Serge Vaudenay

Presses polytechniques et universitaires romandes

Collection «focus science»

Technocivilisation
Pour une philosophie du numérique
René Berger, Solange Ghernaouti-Hélie

Vivre dans les champs électromagnétiques
Pierre Zweiacker

Morts pour la science
Pierre Zweiacker

Surprenante gravité
François Rothen

Fluide vital
Contes de l'ère électrique
Pierre Zweiacker

Et pourtant, elle tourne!
François Rothen

Le huitième jour de la création
Jacques Neirynck

300 questions à un astronome
Anton Vos

Science est conscience
Jacques Neirynck

Illustration de couverture: © foolish
Mise en page: Marlyse Audergon

Les Presses polytechniques et universitaires romandes sont une fondation scientifique dont le but est principalement la diffusion des travaux de l'Ecole polytechnique fédérale de Lausanne ainsi que d'autres universités et écoles d'ingénieurs francophones. Le catalogue de leurs publications peut être obtenu par courrier aux Presses polytechniques et universitaires romandes, EPFL – Rolex Learning Center, CH-1015 Lausanne, par E-Mail à ppur@epfl.ch, par téléphone au (0)21 693 41 40, ou par fax au (0)21 693 40 27.

www.ppur.org

ISBN 978-2-88074-830-2

CH – 1015 Lausanne
Imprimé en Italie

Sommaire

Préambule

Le besoin de communiquer davantage et de plus en plus vite nous pousse à réfléchir à ce qui différencie les communications directes d'humain à humain de celles utilisant des intermédiaires technologiques. Qu'est-ce qui nous assure la fiabilité de la communication ? Qu'est-ce qui assure les interlocuteurs de l'aboutissement d'un accord dans une discussion ? Qu'est-ce qui assure la sécurité du mode de discussion en général ?

Un premier constat s'impose : la communication d'un être humain à un autre être humain est extrêmement redondante. Elle utilise de nombreux canaux d'information simultanés. L'information transmise par la voix est enrichie par d'autres sens comme la vision des gestes, des mouvements des muscles du visage, la dilatation des pupilles et parfois aussi l'émission d'odeurs. Ces signaux ne semblent pas nécessaires à la communication mais apportent fiabilité et confort. La voix transporte aussi des tics de langage et des expressions qui enrichissent la communication sans ajouter d'information essentielle. Pendant un discours, le fait de hocher la tête, un simple « oui », voire un « mmm mmm » au bon moment assurent que l'interlocuteur est toujours à l'écoute et motivent l'orateur à poursuivre.

Du point de vue de la confiance, ce type de communication part avec un avantage. Par défaut, un être humain fait confiance à un autre être humain lorsqu'ils sont face à face et se comportera avec bienveillance. Même par téléphone, bien que de nombreux signaux soient coupés, le son de la voix de l'interlocuteur humain fidèlement retransmis (ou presque) et l'interaction en temps réel suscitent une réaction aimable. Par email, cependant, le contact humain est bien moins fort. De nombreux canaux de redondance ont disparu et le délai de transmission supprime tout sentiment d'être en contact avec un correspondant humain. Même si un email reçu porte le nom d'un expéditeur qui semble humain, voire que l'on connaît, il peut très bien avoir été émis par un automate, un spammeur ou une personne malveillante. Sans contact véritablement humain, l'échange laisse plus de place au doute.

Prenons l'exemple d'une personne qui doit transmettre un courrier important. En se présentant au guichet de La Poste, une fois que le préposé a

pris le courrier et a regardé le client dans les yeux en disant « c'est tout bon ! », la personne repart avec l'assurance que son courrier sera traité avec diligence par un être humain. D'ailleurs, en cas de négligence, l'employé serait irrémédiablement taraudé par sa conscience professionnelle. A défaut, l'employé finirait (en principe) par être licencié. Le système est donc assez robuste pour corriger ses propres erreurs. Paraxodalement, on associe souvent les failles au facteur humain. On dit souvent que l'erreur est humaine. Il arrive donc au courrier de se perdre pendant le transport. De l'encre peut être renversée dessus, rendant à la fois l'adresse du destinataire et de l'expéditeur illisible[1]. Suite à un problème, on trouve plus rassurant de rejeter la responsabilité sur le facteur humain car l'homme apprend par ses erreurs. La machine pas.

Si maintenant la personne envoie le courrier par email et que son ordinateur le regarde dans les yeux en disant « c'est tout bon ! », elle peut légitimement en douter car il est tout à fait possible que l'ordinateur ait choisi de détruire froidement l'email sans le traiter une fraction de seconde après. Bien qu'un ordinateur exécute sans faille le code qu'il contient, il n'exécute ni plus ni moins que ce code. Celui-ci peut avoir été infecté par un virus, être régi par un système d'exploitation ou un logiciel mal fait, se planter de temps en temps, ne pas réaliser que la communication avec l'extérieur est coupée, etc. De plus, des filtres antispam trop zélés auront pu détruire le message dans la boîte du destinataire (si ce n'est celui-ci qui aura délibérément effacé le message et malicieusement feint d'être victime d'un tel filtre). La machine détruit le courrier sans un brin de remords ni le moindre risque d'être mise au rebut. La déshumanisation est source de perte de confiance. Elle offre un champ fertile au développement de toute sorte de comportement malicieux.

Dans le cas de La Poste, le client a besoin que la compagnie s'engage sur un service, que son courrier reste confidentiel, qu'il arrive dans le même état qu'au moment de l'expédition. Il peut avoir besoin d'un reçu pour pouvoir déposer une réclamation. Il peut aussi nécessiter un accusé de réception. Les interactions automatisées sont soumises aux mêmes problèmes de sécurité. Ce qui les caractérise, c'est leur plus grande densité et fréquence. Les hommes communiquent entre eux au travers de machines (par email, pour faire du commerce sur Internet, pour les besoins de la cyber-administration, etc). Les machines communiquent entre elles par des réseaux sans fil, donc en terrain hautement vulnérable. Il est nécessaire d'utiliser des outils pour renforcer leur sécurité. C'est le rôle de la cryptographie.

1 Ce n'est pas de chance mais c'est du vécu.

Comme on le verra, il existe une fracture entre la protection souhaitée et celle qui est réellement atteinte. Reste donc à la réduire.

Le présent ouvrage se veut accessible au lecteur astucieux familier des mathématiques que l'on enseigne à l'école et utilisateur curieux des technologies de l'information. Le technicien avancé pourra l'utiliser comme un outil de réflexion sur la sécurité dans les moyens de communication, qu'ils soient entre êtres humains ou entre machines. Il a une vocation éducative. Son ambition est également de tordre le cou à un certain nombre de préjugés tenaces :

- La cryptographie résout les problèmes de sécurité. Un spécialiste utilisant ses outils cryptographiques est invulnérable.
- La sécurité cryptographique est une vérité mathématique immuable : soit un procédé est sûr, soit il ne l'est pas.
- La cryptographie résout les problèmes de la sphère privée. Elle est au service des hommes.
- La cryptographie que l'on utilise tous les jours intègre les derniers progrès de la recherche.
- La cryptographie est le domaine réservé de quelques mathématiciens érudits.

Tout cela est faux comme on le verra au fil des chapitres. La vérité, c'est que même un utilisateur averti de la cryptographie est tout aussi vulnérable qu'un autre. La sécurité d'un procédé cryptographique ne fait que diminuer au fil des progrès de la technologie et de la recherche. Elle repose sur des hypothèses non vérifiées (et peut-être non vérifiables). Elle est au service de gouvernements ou d'entreprises et offre de nouvelles prises aux intrusions dans la sphère privée. La cryptographie que l'on utilise actuellement date principalement des années 1980 et serait largement dépassée d'un point de vue académique. La cryptographie que l'on nous prescrit silencieusement est comme un médicament contre l'insécurité qui ne serait pas toujours très efficace et très vite dépassé par l'évolution des menaces. L'utilisateur n'a pas le choix. On lui impose une cryptographie pharmaceutique de qualité médiocre non couverte par les assurances maladies. Enfin, la maîtrise des mathématiques n'est ni une condition nécessaire ni une condition suffisante pour comprendre la cryptographie. Même si la cryptographie fait un usage abondant des mathématiques, la cryptographie reste peu accessible, même aux mathématiciens érudits. En fait, la cryptographie revêt une dimension multidisciplinaire. Elle fait aussi appel aux domaines de l'ingénierie, de l'informatique théorique et de la logique. Elle a aussi une composante qui lui est propre. La cryptographie doit être davantage considérée comme une « science de la malice » qui importe des outils provenant de nombreuses disciplines (y compris les mathématiques).

Finalement, l'astuce est la seule notion qui devrait vraiment être nécessaire pour comprendre la cryptographie.

La cryptographie appliquée est victime d'une quadruple fracture. Tout d'abord, il y a un écart entre les objectifs de sécurité désirés et ceux théoriquement accessibles. Certains objectifs sont en effet impossibles à atteindre. Ensuite, ce que l'état de l'art permet de réaliser n'est pas exactement en adéquation avec les objectifs théoriquement accessibles parce que la science n'est pas assez avancée. De plus, les nombreuses contraintes et les inévitables erreurs de conception éloignent davantage les systèmes de ces objectifs théoriques. Enfin, l'usage que l'on fait de ces systèmes est en décalage avec celui qui était prévu par les concepteurs. L'utilisateur ignore le plus souvent les problèmes de sécurité. Il a une conception floue de ce qu'est la sécurité. Il souhaite la sécurité de ses communications mais ne veut pas être importuné par des procédures ennuyeuses.

Cet ouvrage cherche à réduire la « fracture cryptographique » en présentant la cryptographie de manière aussi peu technique que possible. Il montre aussi comment en étant correctement utilisée, la cryptographie peut améliorer la sécurité des communications, gérer correctement les problèmes de sphère privée et espérer une évolution dans le bon sens des outils disponibles. Il présente également la recherche en cryptographie comme un processus vivant en expliquant les progrès, découvertes, expériences, preuves et corrections qui sont réalisés jusqu'à présent.

Structure du livre

Au long de ce parcours, les concepts cryptographiques seront illustrés par des résultats de la recherche. La bibliographie donne une liste de références dans l'ordre alphabétique de leurs auteurs. Pour plus de lisibilité, le numéro de la référence ne figurera dans le texte que si elle ne peut être retrouvée dans la bibliographie par une recherche sur le nom de l'auteur mentionné. Vu la richesse et la profusion de la littérature en cryptographie, il fut difficile de choisir les thèmes et les articles à mentionner. On aura favorisé quelques thèmes de prédilection. Inévitablement, cet ouvrage met souvent l'accent sur les avancées produites à l'Ecole polytechnique fédérale de Lausanne (EPFL) et notamment les propres contributions de l'auteur. De manière discutable, elles se retrouvent placées à côté des références majeures que constituent les piliers fondateurs de la cryptographie. Le lecteur pardonnera ces choix.

Les problèmes cryptographiques seront l'objet de scènes interprétées par quelques personnages. On retrouvera les aventures d'Anne, de son com-

pagnon Bernard, de son frère Cyril, de son associé Daniel (dans le cadre de leur société Megacrypto) et de sa rivale Elodie.

Le livre commence par présenter la problématique du chiffrement et les principes de base en cryptographie. Le deuxième chapitre traite des différentes définitions possibles de confidentialité. Par comparaison avec le thème de l'assurance et des différentes options à inclure dans une police, les différents types de confidentialité sont exposés. Il est alors temps d'effectuer une visite dans le zoo cryptologique et d'observer quelques espèces de fonctions primitives. On retrouvera bien évidemment les fonctions de chiffrement mais aussi des fonctions permettant d'authentifier des documents, de découper un secret en plusieurs parts, de prouver sans divulguer, etc. Le chapitre 4 apporte un regard plus critique, où plusieurs raisons qui peuvent conduire à l'effondrement de la sécurité sont présentées.

Plusieurs chapitres thématiques sont ensuite abordés. Le chapitre 5 raconte comment Anne et Bernard se sont rencontrés par voie électronique et se sont fiancés de manière sécurisée. Les notions d'engagement et de non-répudiation sont ainsi abordées. Les infrastructures permettant de développer la confiance dans les communications sont ensuite présentées. On montre notamment comment Anne devrait faire pour effectuer des achats en ligne en toute sécurité tout en montrant que c'est peu réaliste. Le chapitre 7 traite des différentes formes de contrôle d'accès. La sécurité des diverses technologies sans fil est ensuite abordée. On y présente les téléphones mobiles, les réseaux WiFi, la technologie Bluetooth et le fameux passeport biométrique.

Les derniers chapitres établissent le triste bilan de l'impact de toutes ces technologies sur la liberté. Dans le chapitre 9, on présente différents aspects sur le thème de la protection de la sphère privée et les quelques techniques qui permettraient de la mettre en œuvre si cela figurait sur l'agenda des fabricants. Le chapitre final ébauche une faible liste des fléaux qui s'abattent sur l'homme : l'espionnage permanent des utilisateurs, le spam, la subversion psychologique, la perte de l'individualité par abus de techniques biométriques, la fin de l'anonymat, la chute de la démocratie, l'exploitation par les diffuseurs d'œuvres artistiques et leur piratage.

Comment en est-on arrivé là ? En faisant un usage mauvais et non maîtrisé de la cryptographie. Réduisons donc la fracture. Apprenons à utiliser correctement les moyens cryptographiques, à refuser ceux qui sont mal conçus ou qui résolvent de faux problèmes tout en en créant de nouveaux, à développer ceux qui font défaut. Comment ? Ce livre n'a la prétention d'apporter aucune réponse. Le lecteur se posera certainement plus de questions après l'avoir refermé qu'avant d'être passé à la page suivante. S'il a désormais conscience des problèmes, l'un des objectifs aura été atteint.

Remerciements

Cet ouvrage doit beaucoup aux relecteurs et à leurs nombreux commentaires. Notamment : Gildas Avoine, Henri Gilbert, Jean Monnerat, David Naccache, Sylvain Pasini et David Pointcheval. Je remercie particulièrement Martine Croval qui me seconde depuis de nombreuses années, qui a soigneusement annoté l'intégralité du manuscrit et qui m'a fait part de commentaires constructifs. Merci également à l'Ecole polytechnique fédérale de Lausanne (EPFL) pour le cadre de travail qui a rendu ce projet possible et à mon laboratoire (le LASEC) pour son ambiance conviviale. Je suis toujours redevable envers mon épouse Christine qui a souffert sur les premières versions du document ainsi qu'à mon fils Emilien pour m'avoir laissé travailler. Puisse la fracture se réduire pour le bien de son avenir.

Serge Vaudenay

1 Le chiffrement

Anne est une adolescente qui a pour habitude de raconter ses aventures quotidiennes dans son journal intime. En aucun cas elle n'accepterait que son contenu tombe entre les mains de quiconque, même de sa meilleure amie. Pour cela, elle le rédige en utilisant un code secret qu'elle a créé elle-même. Même si le journal venait à être subtilisé, la personne qui chercherait à le lire ne pourrait comprendre le sens du contenu. La protection de la vie privée d'Anne est ainsi assurée par le chiffrement.

Code et chiffre

Pour envoyer des marchandises d'un point à l'autre de la planète, on les emballe et on les transporte. Pour transmettre de l'information, on fait de même. L'emballage est effectué au moyen d'un *code* adapté au moyen de transport. Par exemple, le message contenu dans le présent ouvrage est codé grâce au dictionnaire français et imprimé sur du papier. La parole est codée suivant le langage parlé et véhiculée par des ondes acoustiques. L'information numérique, sur un CD ou dans un ordinateur, est codée au moyen d'une séquence de chiffres.

Jusqu'ici, l'action de *coder* ou *décoder* n'est liée en rien à la notion de confidentialité. Le journal d'Anne est un document qui doit rester confidentiel. Il doit être protégé contre toute lecture non autorisée. C'est le petit frère qui jouera le rôle de l'« adversaire ». Cyril aimerait bien, en effet, percer les secrets du journal intime de sa sœur. Comme il est un garçon intelligent, la sécurité d'Anne nécessite des moyens de protection sophistiqués. En fait, devoir faire face à la malice est ce qui caractérise fondamentalement la cryptographie.

Un *code* peut être collectivement connu ou privé. Par exemple, la langue française est connue du monde de la francophonie. Des dictionnaires ou des moyens de traduction sont universellement disponibles. En revanche, le code utilisé pour transmettre nos communications téléphoniques sans

fil est destiné à être connu seulement de notre téléphone personnel et du réseau téléphonique car on n'aimerait sûrement pas que n'importe qui puisse capter les ondes radio et écouter nos conversations. On parle alors d'un *code secret*. Pour semer un peu la confusion, un code secret s'appelle parfois un *chiffre*. Le codage se dit alors *chiffrement*. Il consiste à changer le mode de représentation d'une information d'un code public (une information « en clair ») vers un code secret (une information « chiffrée »), le *déchiffrement* étant l'opération inverse.

Le terme « décryptage » n'a pas exactement la même signification que « déchiffrement ». C'est la même différence qu'entre « fracturer » une porte et la « déverrouiller ». Pour rentrer chez soi, on ouvre une porte d'entrée en la déverrouillant. Un voleur qui ne possède pas la clef cherchera néanmoins à l'ouvrir en la fracturant. Le destinataire légitime du message accède à l'information par le déchiffrement tandis qu'un espion cherche à récupérer l'information par une opération de décryptage, sans avoir de clef a priori.

Un système de chiffrement nécessite trois types d'opérations : l'initialisation, le chiffrement et le déchiffrement. Ces opérations sont décrites par des « algorithmes ». Autrement dit : par un protocole d'instructions à suivre pour transformer des informations. Tout comme une recette de cuisine donne une suite de tâches pour transformer des ingrédients en un plat pouvant être ingéré par tout estomac délicat, l'algorithme de chiffrement précise comment « emballer » une information claire sous une forme qui pourrait être confiée à un messager lambda sans compromettre la confidentialité. L'algorithme de déchiffrement explique l'opération de « déballage ». Enfin, l'algorithme d'initialisation spécifie comment fabriquer le code secret lui-même en fonction du niveau de confidentialité requis.

Le principe de Kerckhoffs

On pourrait croire que, pour communiquer des informations confidentielles, il suffit d'établir un code secret qui ne soit connu que des interlocuteurs légitimes. Créer un code qui assure réellement la protection des communications n'est cependant pas aisé. Avant de créer son code secret, Anne a étudié longuement plusieurs manuels de cryptographie. De plus, ce travail est voué à être répété car pour échanger des messages secrets avec sa meilleure amie (qui, rappelons-le, n'est pas supposée pouvoir lire le journal d'Anne), elle devra fabriquer un nouveau chiffre. Lorsqu'elle aura un petit ami, ils devront en établir un troisième. A chaque fois, l'opération est mathématiquement complexe.

Prenons le cas de son téléphone mobile.

Dès que le téléphone est allumé, il cherche l'antenne la plus proche et établit avec elle un nouveau code secret. Le code est compris par le réseau auquel il est connecté. Il est destiné à changer souvent, notamment lorsque Anne se déplace hors du champ de cette antenne.

On imagine mal Anne se présenter à chaque fois à l'antenne la plus proche et négocier un nouveau code secret. Ceci est effectué automatiquement par le téléphone et le réseau. Cela signifie que les développeurs du système, à la fois du côté du téléphone mobile et du côté du réseau, ont anticipé l'établissement du code et ont préparé sa mise en œuvre. Pour des raisons de compatibilité, le téléphone doit être utilisable dans tous les pays qui utilisent la même norme de protocole. Cela signifie que beaucoup de personnes connaissent potentiellement le code qui sera établi à la communication : les fabricants de téléphone, les opérateurs de tous pays et leurs équipementiers. Cela ne doit pas nuire à la sécurité. Ces observations conduisent au fameux *principe de Kerckhoffs*.

Auguste Kerckhoffs naquit en 1835 sous le nom de Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs von Nieuwenhof. Pour d'obscures raisons, il décida par la suite de raccourcir son nom[1]. Il devint professeur d'allemand à l'école HEC à Paris et participa au développement du Volapük. En dehors de la linguistique, il s'intéressa à la cryptographie et publia en 1883 le fameux article « La cryptographie militaire » dans lequel il énonça plusieurs principes fondamentaux :

1. « Le système doit être matériellement, sinon mathématiquement, indéchiffrable.
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants.
4. Il faut qu'il soit applicable à la correspondance télégraphique.
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer. »

Le second principe est communément appelé *LE principe de Kerckhoffs* de nos jours.

---

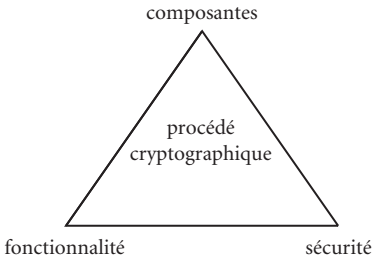
1 Voir Kahn, *The Codebreakers* 1996.

Suivant ce principe, la sécurité du chiffrement ne doit pas dépendre de la confidentialité du mécanisme utilisé. En fait, le mécanisme de chiffrement doit être prévu pour admettre un paramètre qui peut être facilement choisi a posteriori : la « clef de chiffrement ». Lorsque l'on étudie la sécurité d'un système de chiffrement, on admet l'hypothèse que l'adversaire connaît déjà le procédé mais ignore seulement la clef qui a été choisie. Bien que les communications numériques émergeaient à peine en 1883, ce principe est fondamental dans la cryptographie moderne.

Certaines personnes défendent le principe que le procédé de chiffrement soit toujours rendu public en invoquant Kerckhoffs. C'est soit une erreur de compréhension soit un amalgame grossier. Le principe de Kerckhoffs n'a pas une exigence aussi forte. D'ailleurs, il y a des cas où l'emploi d'un procédé non public peut se défendre. Tout d'abord, si le procédé est maintenu confidentiel, l'adversaire doit faire face à une difficulté supplémentaire et il ne faut jamais négliger les opportunités de l'enquiquiner. De plus, si le procédé est légalement protégé par une clause de confidentialité tout en étant notoirement connu, une protection de type juridique pourra être utile devant la Justice contre l'adversaire. En revanche, les partisans des procédés publics soulignent que ceux-ci bénéficient d'une expertise publique : si un chercheur s'y s'intéresse, il va publier des travaux qui amélioreront la compréhension de sa sécurité. Même s'il découvre une faiblesse, celle-ci peut être corrigée avant sa publication. Ce n'est pas possible pour un procédé non publié et légalement protégé car le chercheur se placerait lui-même dans l'illégalité en étudiant un système qu'il est supposé ignorer ! La question de savoir si un procédé cryptographique doit être rendu public ou non est sujet à controverse. Elle doit être examinée au cas par cas. On prendra seulement pour acquis que Cyril connaît le système de chiffrement des téléphones mobiles dans le cadre de l'analyse de sécurité.

Chiffrement à clef secrète

Tous les procédés cryptographiques se décrivent par leurs composantes, leur fonctionnalité et leur sécurité. Un système de chiffrement à clef secrète est un procédé cryptographique composé de trois algorithmes : un algorithme appelé « générateur » qui fabrique les clefs de chiffrement, un algorithme qui permet de chiffrer un message clair au moyen d'une clef et un algorithme qui permet de déchiffrer un message chiffré au moyen de la même clef. Comme la clef est la même pour chiffrer et pour déchiffrer, le chiffrement à clef secrète est aussi appelé *chiffrement symétrique* ou *chiffrement conventionnel*.



La fonctionnalité d'un procédé est ce qui caractérise son usage normal. Dans le cas du chiffrement symétrique, la fonctionnalité est bien simple : pour toute clef engendrée et tout message clair, l'opération consistant à chiffrer le message puis à en déchiffrer le résultat en utilisant la même clef conduit à retrouver le message d'origine. Lorsqu'Anne écrit ses aventures dans son journal intime, elle doit pouvoir les relire dans le futur. Lorsqu'elle parle dans son téléphone, sa voix est chiffrée, transmise par ondes radio, puis déchiffrée par le réseau avant de suivre son chemin dans le circuit téléphonique. Jusque-là, rien d'extraordinaire. Pour la sécurité, cela se gâte.

Contrairement à la fonctionnalité qui décrit ce qui se passe normalement, la sécurité spécifie ce qui *ne doit pas* se passer : ce qu'un adversaire ne doit pas être capable de faire. Lorsqu'une attaque contre un procédé cryptographique a lieu, on peut souvent juger a posteriori si c'est une attaque que le système aurait dû éviter ou si la responsabilité est ailleurs. Définir a priori ce que le système doit éviter est une tâche délicate. Pour le chiffrement, il doit être impossible de retrouver l'information du message clair mais il faut cependant que le destinataire y parvienne : il faut que la fonctionnalité soit réalisable. Il faut donc décrire en termes suffisamment généraux les types d'attaques considérés comme illicites, sans rendre la sécurité inutilement exigeante. Faute de quoi, l'existence d'un procédé sûr serait compromise.

La sécurité du chiffrement garantit la confidentialité du message clair. Intuitivement, l'adversaire qui connaît le système de chiffrement (suivant le principe de Kerckhoffs) et qui voit transiter des messages chiffrés ne peut pas extraire d'information effective sur le message clair. Ce cas, illustré sur la figure 1.1, suit le principe du « message chiffré seulement » : l'adversaire cherche à violer la confidentialité à partir d'observations de messages chiffrés qui transitent dans le canal de communication. Cyril aimerait décrypter le journal de sa grande sœur Anne à partir du texte chiffré uniquement. Dans le cas où une partie du message clair est prévisible ou obtenue par d'autres moyens, on peut considérer un adversaire qui connaît déjà des informations sur le message clair, voire des échantillons de messages clairs et de messages chiffrés correspondants. C'est le principe du « message clair

connu ». Dans le cas du téléphone mobile, si Cyril capte les communications chiffrées d'Anne qui téléphone à sa meilleure amie et s'il se trouve à proximité de sa sœur, il entend les paroles d'Anne et capte leur résultat chiffré. Il cherchera à décrypter l'autre partie : les paroles de son amie. D'autres modèles offrent plus de pouvoir à l'adversaire en lui permettant de choisir le message qui sera chiffré. On imagine facilement Cyril criant à côté d'Anne, forçant ainsi son téléphone à transmettre le chiffré d'une information qu'il aurait choisie. C'est le modèle du « message clair choisi ». Enfin, on peut considérer un adversaire qui peut également demander le déchiffrement de messages qu'il a lui-même choisis suivant le modèle du « message chiffré choisi ». Nous reviendrons sur ce dernier modèle et sur une définition plus formelle de la sécurité du chiffrement dans le chapitre 2.

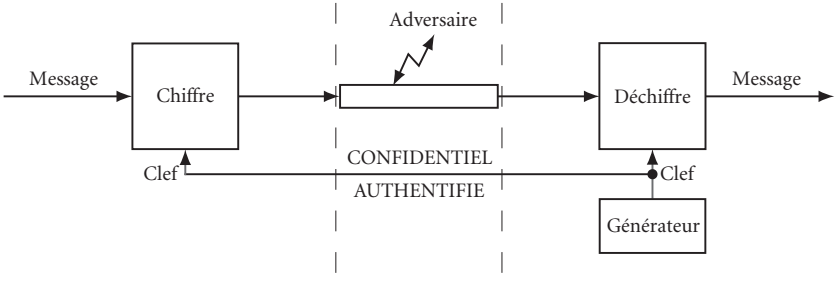


Fig. 1.1 Procédé de chiffrement à clef secrète.

Pour exemple de système de chiffrement à clef secrète, mentionnons le procédé standard AES inventé par les chercheurs Joan Daemen et Vincent Rijmen de l'Université de Louvain. Ce standard fut adopté en 2001. Il permet de chiffrer des « blocs » de message qui sont des nombres de longueur standard. Pour chiffrer des messages de longueur arbitraire à l'aide du « chiffrement par blocs », on utilise un « mode opératoire » qui spécifie comment découper le message en blocs et comment les chiffrer séquentiellement.

Recherche exhaustive

Comme on l'a vu, la clef de chiffrement doit être facilement configurable. Le plus souvent, c'est un nombre arbitraire de taille fixée en fonction du niveau de sécurité requis. Le nombre de clefs possibles dépend de cette taille. Dans le cas de nombres décimaux de 6 chiffres, le nombre de possibilités est d'un million : ce sont tous les nombres de 0 à 999 999. Un million vaut 10^6 : c'est égal au nombre de chiffres possibles (10) élevé à une

puissance égale à sa longueur (6). Les ordinateurs n'ont pas appris à compter sur dix doigts comme les êtres humains mais avec des chiffres binaires (0 ou 1) : des « bits ». Un nombre de 20 bits admet $2^{20} = 1\,048\,576$ possibilités (soit environ un million) : ce sont les nombres 0, 1, 10, 11, 100, 101, 110, 111, 1000, … jusqu'à 1111 1111 1111 1111 1111. Pour convertir un nombre de chiffres en nombre de bits, on utilise comme règle simple que 3 chiffres décimaux correspondent environ à 10 bits.

Pour casser la sécurité du chiffrement, une stratégie consiste à essayer toutes les combinaisons possibles de la clef jusqu'à obtenir le déchiffrement correct de messages chiffrés. Cette suite d'opérations répétitives porte le nom de « recherche exhaustive ». Elle est assez fastidieuse pour un être humain. L'*homo sapiens* pèche naturellement par paresse. Cela le rend intelligent. Pour effectuer une recherche exhaustive, il tentera donc d'automatiser le travail. C'est ainsi qu'Alan Turing inventa l'ordinateur. COLOSSUS, l'un des premiers véritables ordinateurs de l'histoire, fut construit pour casser des codes secrets pendant la Seconde Guerre mondiale.

Comme la recherche exhaustive ne dépend pas du système de chiffrement choisi, on dit que c'est une méthode « générique » d'attaque. Evidemment, plus la taille de la clef est longue, plus la recherche est laborieuse. En 2007, un ordinateur typique permet facilement de tester un million de clefs par seconde. Donc, si la clef admet 20 bits, une recherche exhaustive pourra compromettre la sécurité après environ une seconde. Si la clef admet maintenant 40 bits, le nombre de combinaisons possibles sera

$$2^{40} = 2^{20} \times 2^{20}$$

Il sera donc multiplié par environ un million. La recherche exhaustive prendra donc un million de secondes, soit une douzaine de jours. Si la clef admet 60 bits, le temps de recherche exhaustive est encore multiplié par un million et l'on obtient 35 millénaires. L'homme pèche aussi par impatience. Cela le rend encore plus malin. On peut en effet chercher à paralléliser la recherche exhaustive : plutôt que d'utiliser un ordinateur, on peut faire travailler un millier d'ordinateurs. Le temps de la recherche sera ainsi divisé par mille. On obtient donc 35 ans, ce qui est encore bien long. Finalement, on peut aussi chercher à optimiser le travail de tous ces processeurs ou construire une machine dédiée à ce type de travail pour l'effectuer plus rapidement qu'un ordinateur destiné a priori à des tâches quelconques. Vraisemblablement, le temps de recherche final sera de l'ordre de quelques jours. Cela signifie que des clefs d'une soixantaine de bits sont déjà trop courtes pour offrir une sécurité face à un adversaire qui a la capacité de construire une telle machine. Actuellement, on considère qu'il faut une clef secrète d'au moins 128 bits pour obtenir une bonne sécurité.

Le nombre de secondes écoulées depuis le Big Bang est (environ) de 473 millions de milliards[2]. Pour faire une recherche exhaustive sur une clef de 128 bits pendant cette durée, il faudrait pouvoir tester 720 milliards de milliards de clefs par seconde. Avec des processeurs testant laborieusement un million de clefs par seconde, il en faudrait donc 720 000 milliards pour faire cette recherche. On aurait donc pu casser une clef de 128 bits si l'on avait fait travailler 720 000 milliards d'ordinateurs depuis le Big Bang. On verra au chapitre 4 comment faire mieux. En attendant, cela donne une idée de la sécurité d'une clef de 128 bits.

Le chiffrement de Vernam

En 1926, Gilbert Vernam a publié aux Bell Labs un système de chiffrement qui assure parfaitement la confidentialité mais qui est soumis à des contraintes drastiques :

1. Tout d'abord, la clef de chiffrement doit être parfaitement aléatoire.
2. Ensuite, la clef doit être au moins aussi longue que le document à chiffrer.
3. Enfin, la clef ne doit être utilisée que pour un seul chiffrement, après quoi elle doit être jetée sans état d'âme.

On peut expliquer simplement comment le système fonctionne pour chiffrer des messages. Pour simplifier, on se restreindra à un alphabet de 27 lettres qui comprend tous les caractères usuels de « a » à « z » ainsi qu'un caractère d'espace que l'on notera « ␣ ». On ne considère donc pas de différences entre minuscules et majuscules ni de caractères de ponctuation ou de caractères accentués. On définit dans cet alphabet une opération d'addition. En ajoutant un caractère du message clair à un caractère de la clef on obtient un caractère du message chiffré. Par exemple, D + i = M suivant la table d'addition ci-contre.

On définit également une opération de soustraction correspondante. Par exemple, pour retrancher « K » à « B », il faut chercher dans la ligne « K » quelle colonne contient un « B » et l'on obtient la colonne « r ». Autrement dit, B – K = r.

Pour chiffrer un message comme « cyril␣est␣un␣affreux », on utilise pour clef un nombre aléatoire de même taille. Admettons que la clef soit

[2] Dans 30 millions d'années, cet ouvrage sera tombé dans le domaine public depuis longtemps. Que le lecteur désireux de le rééditer à ce moment-là ait la gentillesse de remplacer ce nombre par 474 millions de milliards car l'auteur aura sûrement d'autres préoccupations à ce moment-là.