1. Introduction

> « On a inventé l'art d'écrire avec des chiffres ou avec des caractères inconnus pour dérober la connaissance de ce qu'on écrit à ceux qui interceptent des lettres, mais l'industrie des hommes, qui s'est raffinée par la nécessité & l'intérest, a trouvé des règles pour déchiffrer ces lettres & pour pénétrer par ce moyen dans les secrets d'autruy. »
>
> François de Callières (1645 - 1717)

Ce livre est le chaînon manquant de la cryptographie. En effet, quand on parle de codes secrets (on ose à peine parler de cryptographie, car la plupart des gens, même les libraires, ignorent la signification de ce terme quelque peu effrayant), on a d'un côté des livres d'histoire ou des livres pour les enfants, et de l'autre côté des livres de niveau universitaire remplis de formules et de théorèmes souvent difficilement compréhensibles pour le commun des mortels.

L'ambition de ce livre est de faire le lien entre ces deux mondes. Il s'adresse à tous les curieux qui ont encore un vague souvenir des messages secrets qu'ils échangeaient sur les bancs de l'école, aux créateurs d'énigmes et aux chasseurs de trésors. Les enseignants pourront aussi y trouver une matière qui passionne les élèves, et qui permet d'aborder par la pratique certains concepts mathématiques dont l'utilité ne saute pas aux yeux, comme les matrices ou les nombres premiers.

La cryptographie est à la fois une science et un art. C'est une science, car la résolution des problèmes exige la connaissance de certaines règles, lesquelles, tout en admettant beaucoup d'exceptions, n'en sont pas moins fixes et définies ; ces règles entraînent une suite de raisonnements logiques. La cryptographie est aussi un art, car elle fait appel aux talents d'intuition, d'imagination et d'invention

du chercheur, ces facultés étant elles-mêmes secondées par des connaissances linguistiques approfondies.

Ce livre peut se lire à plusieurs niveaux. Certains paragraphes raviront les enfants, d'autres demanderont un effort plus grand avec un peu de réflexion, et d'autres enfin demanderont quelques connaissances appronfondiées en mathématiques. Plus vous avancerez dans ce livre, et plus les systèmes de chiffrement deviendront complexes.

Je voulais écrire un livre qui s'inscrirait dans la ligne de ceux des grands cryptologues du début du XX^{e} siècle : **Baudouin**, **Givierge**, **Langie**, **Sacco**, **Fouché Gaines, Sinkov**, et quelques autres. Leurs livres ne se contentaient pas de présenter des systèmes de chiffrement, ils montraient aussi leurs faiblesses et comment les décrypter. Malheureusement, tous les livres en français de ces auteurs sont aujourd'hui introuvables.

À travers mon livre, je vous invite à un voyage dans le temps, depuis l'Antiquité jusqu'à nos jours, où vous découvrirez les systèmes de chiffrement qui ont marqué leur époque. Impossible de les étudier tous, car il y en a un nombre infini. Nous regarderons donc plus d'une centaine de chiffres où l'on n'a besoin que d'un papier et d'un crayon.

Les codes secrets ne sont pas l'apanage des militaires et des diplomates. Des auteurs célèbres, férus de cryptographie - **Edgar Allan Poe**, **Jules Verne**, **François Rabelais** - ont écrit des romans dans lesquels le décryptement d'un message secret jouait un rôle central. En les étudiant de près, nous verrons à quel point ces textes sont réalistes.

En revanche, nous ne ferons qu'effleurer la cryptographie moderne, car elle fait appel à des notions mathématiques et informatiques complexes, que j'essaierai de simplifier au maximum. J'espère que les puristes me pardonneront. Nous ne parlerons pas non plus des machines à crypter qui ont connu un bel essor dans les années 1920 à 1970, car c'est un sujet trop technique et trop vaste qui pourrait faire l'objet d'un livre à lui tout seul.

Par rapport aux livres de mes glorieux prédécesseurs, la grande originalité de celui-ci est d'être couplé avec un site compagnon dont l'adresse est : www.apprendre-en-ligne.net/crypto. J'ai commencé ce site en 2001 déjà, avec l'intention d'en faire un cours en ligne pour des élèves de lycée. Le sujet est tellement passionnant que ce site a grandi, grandi... et a trouvé son aboutissement dans ce livre. L'avantage indéniable d'Internet est de permettre l'interactivité : vous pourrez donc mettre les « mains dans le cambouis » et tester tous les codes secrets que vous trouverez dans ce livre. Vous y verrez aussi de nombreuses illustrations, des références à d'autres sites Internet et aussi des jeux de décryptement.

1.1. Définition de termes courants

Avant de commencer, il est bon de définir précisément certains termes couramment utilisés en cryptologie. Certains de ces termes sont si spécifiques qu'on ne les trouve même pas dans des dictionnaires !

Algorithme
Suite d'opérations élémentaires à appliquer à des données pour aboutir à un résultat désiré. Par exemple, une recette de cuisine est un algorithme.

Antigramme
Texte déjà chiffré qui va être surchiffré.

Attaque
Tentative de décryptement.

Bigramme
Séquence de deux lettres consécutives. Exemples : ee, th, ng, ... Adjectif : bigrammique, bigrammatique dans certains ouvrages.

Casser
Dans l'expression « casser un code », trouver la clef du code ou le moyen d'accéder à ce qu'il protégeait.

Chiffre
Code secret.

Chiffrement
Opération qui consiste à transformer un texte clair en cryptogramme. On parle de chiffrement car, à la Renaissance, on utilisait principalement des chiffres arabes comme caractères de l'écriture secrète.

Clair (ou message clair)
Version intelligible d'un message et compréhensible par tous.

Clef
Dans un système de chiffrement, elle correspond à un nombre, un mot, une phrase, etc. qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message.

Code
Système de symboles permettant d'interpréter, de transmettre un message, de représenter une information, des données.

Cryptanalyse
Art d'analyser un message chiffré afin de le **décrypter**. On parle aussi de **décryptement**.

Cryptogramme
Message écrit à l'aide d'un système de chiffrement.

Cryptographie
(du grec κρυπτος : caché et γραφειν : écrire)
Art de transformer un message clair en un message inintelligible pour celui qui ne possède pas les clefs de chiffrement. Cependant, on utilise souvent le mot **cryptographie** comme synonyme de **cryptologie**.

Cryptologie
(du grec κρυπτος : caché et λογος : science)
Science des messages secrets. Elle se décompose en deux disciplines : la **cryptographie** et la **cryptanalyse**.

Déchiffrement
Opération inverse du chiffrement. Opération qui consiste à obtenir la version originale d'un message qui a été précédemment chiffré **en connaissant la méthode de chiffrement et les clefs** (contrairement au décryptement).

Décryptement
Opération qui consiste à retrouver le clair **sans disposer des clefs** théoriquement nécessaires. Il ne faut pas confondre **déchiffrement** et **décryptement**.

Double clef (chiffre à)
Autre terme pour chiffre polyalphabétique.

Monoalphabétique
Se dit d'un chiffre où une lettre du message clair est toujours remplacée par le même symbole. On parle aussi de substitution simple.

Nomenclateur
Synonyme de répertoire.

Nulles
Symboles sans signification rajoutés dans un message pour certains algorithmes. On les emploie soit pour compléter un message de manière à atteindre une certaine longueur, soit pour tromper ceux qui cherchent à décrypter le message en noyant les informations utiles au milieu de caractères, mots ou phrases inutiles.

Polyalphabétique
Se dit d'un chiffre où plusieurs alphabets de chiffement sont utilisés en même temps. Une lettre n'est plus chiffrée par un seul symbole, comme c'est le cas pour un chiffre monoalphabétique.

Polygramme
Séquence de n lettres. Adjectif : polygrammique.

Polygrammique
Se dit d'un chiffre où un groupe de n lettres est chiffré par un groupe de m symboles. Souvent $n = m$. On ne chiffre donc pas des lettres mais des polygrammes.

Répertoire
Table mettant en correspondance un code (par exemple un nombre, mais cela peut aussi être un mot) et sa signification. Exemple :

12	Les navires promis sont au port
341	Pape
442	Roi
2221	Nous sommes découverts

Sémagramme
Dans un sémagramme, les éléments du texte codé ou chiffré ne sont ni des lettres, ni des chiffres : le sens est véhiculé par diffé-

rents éléments, par exemple des points de jetons de dominos, l'emplacement d'objets sur une image, etc.

Stéganographie

(du grec στεγανος : couvert et γραφειν : écrire)
Branche particulière de la cryptographie qui consiste non pas à rendre le message inintelligible, mais à le camoufler dans un support (un texte, une image, les mailles d'un tricot, etc.) de manière à masquer sa présence.

Substitution

Un chiffre de substitution remplace les caractères du message en clair par des symboles (caractères, nombres, signes, etc.) définis à l'avance.

Surchiffrement

Fait de chiffrer un message déjà chiffré.

Tétragramme

Séquence de quatre lettres consécutives. Exemples : eche, this, pong, ...

Tomogrammique

Dans les systèmes tomogrammiques, chaque lettre est tout d'abord représentée par un groupe de plusieurs symboles. Ces symboles sont ensuite chiffrés séparément ou par groupes de taille fixe.

Transposition

Un chiffre de transposition ne modifie pas les caractères mais les mélange selon une méthode prédéfinie.

Trigramme

Séquence de trois lettres consécutives.
Exemples : ehe, thi, ong, ...

1.2. Repères historiques

• Les 3000 premières années (de 2000 av. J.-C. à 1000 ap. J.-C.)

Les écritures secrètes semblent être nées spontanément dès que, dans un pays, une partie importante de la population a su lire.

Env. 1900 avant J.-C.	Un scribe égyptien emploie des hiéroglyphes non conformes à la langue correcte dans une inscription. L'historien spécialiste de la cryptographie **David Kahn**[1] le qualifie de premier exemple documenté de cryptographie écrite.
1500 avant J.-C.	Une tablette mésopotamienne contient une formule chiffrée pour la fabrication de vernis pour les poteries.
600-500 avant J.-C.	Des scribes hébreux mettant par écrit le livre de Jérémy ont employé un simple chiffre de substitution connu sous le nom d' « Atbash ». C'était un des chiffres hébreux de cette époque.
487 avant J.-C.	Les Grecs emploient un dispositif appelé la « scytale » , un bâton autour duquel une bande de cuir longue et mince était enveloppée et sur laquelle on écrivait le message. Le cuir était ensuite porté comme une ceinture par le messager. Le destinataire avait un bâton identique permettant d'enrouler le cuir afin de déchiffrer le message.
Env. 150 avant J.-C.	L'historien grec **Polybe** (env. 200-125 av. J.-C.) invente le « carré de Polybe », dont s'inspireront plus tard bien des cryptosystèmes.
60-50 avant J.-C.	**Jules César** (100-44 avant J.-C.) emploie une substitution simple avec l'alphabet normal (il s'agissait simplement de décaler les lettres de l'alphabet d'une quantité fixe) dans les communications du gouvernement. Ce chiffre n'est pas robuste, mais à une époque où très peu de personnes savent lire, cela suffit. César écrit aussi parfois en remplaçant les lettres latines par les lettres grecques.
V e siècle ?	On trouve dans le *Kama-sutra* le *mlecchita-vikalpa*, l'art de l'écriture secrète, qui doit permettre aux femmes de dissimuler leurs liaisons.

1 Voir [KAHN96] dans la bibliographie.

855 **Abu Bakr ben Wahshiyya** publie plusieurs alphabets secrets utilisés à des fins de magie, dans son livre *Kitab shauk almustaham fi ma'arifat rumuz al aklam* (le livre de la connaissance longuement désirée des alphabets occultes enfin dévoilée).

IX[e] siècle **Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòmran ibn Ismaïl al-Kindi** rédige le plus ancien texte connu décrivant la technique de décryptement appelée « analyse des fréquences ».

• L'éveil de l'Occident (de 1000 à 1800)

Jusque-là largement devancé par la science arabe, l'Occident développe la cryptographie et la cryptanalyse.

1226 À partir de cette date, une timide cryptographie politique apparaît dans les archives de Venise, où des points ou des croix remplacent les voyelles dans quelques mots épars.

Env. 1250 **Roger Bacon** décrit plusieurs chiffres. Il écrit : « Il est fou celui qui écrit un secret de toute autre manière que celle qui le soustrait à la connaissance du vulgaire. »

1379 **Gabriel de Lavinde** compose un recueil de clefs, dont plusieurs combinent code et substitution simple. En plus d'un alphabet de chiffrement, souvent avec des nulles, on trouve un petit répertoire d'une douzaine de noms communs et de noms propres avec leurs équivalents en bigrammes. C'est le premier exemple d'un procédé qui prévaudra pendant 450 ans en Europe et en Amérique : le « nomenclateur ».

1392 Dans un ouvrage intitulé *L'Équatorial des planètes*, qui décrit le fonctionnement d'un instrument astronomique, **Geoffrey Chaucer** incorpore six courts cryptogrammes écrits de sa propre main.

1412 La science arabe en matière de cryptologie est exposée dans la *subh al-a sha*, une énorme encyclopédie en 14 volumes, écrite pour fournir à la bureaucratie une connaissance exhaustive de toutes les principales branches du savoir. Son auteur, qui vit en Égypte, est **Abd Allah al-Qalqashandi**. La section intitulée *De la dissimulation des informations secrètes dans les lettres* comporte deux parties, l'une traitant des représentations symboliques et du langage convenu, l'autre des encres invisibles et de la cryptologie.

1466-1467 **Leon Battista Alberti** invente et publie le premier chiffre polyalphabétique. Il conçoit un cadran chiffrant pour simplifier le processus. Cette classe de chiffre n'a pas été cassée jusqu'aux années 1800. Alberti écrit aussi largement sur l'état de l'art dans des chiffres. Ces chiffres polyalphabétiques sont beaucoup plus robustes que le nomenclateur qu'utilisent les diplomates de l'époque. Alberti invente aussi le surchiffrement codique.

1474 Un contemporain d'Alberti, **Sicco Simonetta**, cryptanalyste au service du duc de Milan, écrit *Liber Sifrorum*, un traité de cryptanalyse.

1506 Le premier grand cryptanalyste européen est peut-être **Giovanni Soro**, qui devient secrétaire du Chiffre de Venise en 1506. Le Vatican lui-même teste ses chiffres sur Soro, qui les perce à jour une première fois. Le pape envoie d'autres textes chiffrés à Soro afin de savoir si le meilleur cryptanalyste peut battre son chiffre.

Soro renvoie les textes en écrivant qu'il n'a pas réussi à les déchiffrer mais on ne saura jamais s'il a dit la vérité ou s'il a menti pour pouvoir décrypter sans difficulté tout message émanant des autorités pontificales...

1518 Le premier livre imprimé sur la cryptologie est publié deux ans après la mort de son auteur, **Jean Trithème**. Cet abbé invente un chiffre stéganographique dans lequel chaque lettre est représentée par un mot.

Le résultat ressemble à une prière. Il décrit aussi des chiffres polyalphabétiques sous la forme désormais standard de tables de substitution rectangulaires.

1550 env. **Jérôme Cardan** invente le premier procédé autoclave, mais ce système est imparfait, et c'est finalement un autre procédé qui porte son nom : « la grille de Cardan » (voir § 2.3).

1553 **Giovan Batista Belaso** fait paraître un petit livre intitulé *La cifra del. Sig. Giovan Batista Belaso*. Il y propose, pour le chiffrement en substitution polyalphabétique, l'emploi de clefs littérales, faciles à garder en mémoire et à changer. Il les appelle « mots de passe ».

Les clefs littérales sont immédiatement adoptées et l'innovation de Belaso est à l'origine de certains systèmes actuels très complexes où plusieurs clefs – et non pas une seule –sont utilisées et changées de façon irrégulière.

1563 **Giovanni Battista Della Porta** écrit *De Futivis Literarum Notis*. Ces quatre livres, traitant respectivement des chiffres anciens, des chiffres modernes, de la cryptanalyse et des caractéristiques linguistiques qui favorisent le déchiffrement, représentent la somme des connaissances cryptologiques de l'époque.
Parmi les procédés modernes, dont beaucoup sont de son invention, apparaît la première substitution bigrammique : deux lettres sont représentées par un seul symbole. Il invente aussi le premier chiffre polyalphabétique. Il est le premier à classer les deux principes cryptographiques majeurs : la substitution et la transposition.

1578 **Marins**, un des décrypteurs de la République de Venise, fait paraître *Del mondo di extrazar le cifre*.

1585 **Blaise de Vigenère** écrit son *Traicté des chiffres ou secrètes manières d'escrire*. Il présente entre autres un tableau du type Trithème, que l'on dénomme aujourd'hui à tort « carré de Vigenère ». On considérera longtemps ce chiffre comme indécryptable, légende si tenace que même en 1917, plus de cinquante ans après avoir été cassé, le Vigenère était donné pour impossible à décrypter par la très sérieuse revue *Scientific American*.

1623 Sir **Francis Bacon** (que l'on soupçonne par ailleurs fortement d'être William Shakespeare) est l'inventeur d'un système stéganographique qu'il expose dans *De dignitate et augmentis scientiarum*. Il appelle son alphabet « bilitère », car il utilise un arrangement des deux lettres A et B en groupes de cinq.

1641 **John Wilkins** publie anonymement *Mercury, or the Secret and Swift Messenger*, le premier livre de cryptographie en langue anglaise.

1660-1669 **Samuel Pepys** tient son *Journal* qui fera de lui un des diaristes les plus connus, en nous livrant un témoignage inestimable sur l'Angleterre de cette époque.
Pour le garder secret, il l'écrit dans un langage codé connu sous le nom de *tachygraphie*, une forme de sténographie. Comme l'usage de la tachygraphie s'est perdu avec le temps, on a longtemps cru que ce journal était chiffré. C'est le révérend **John Smith** qui le transcrira en anglais de 1819 à 1822.

1691 **Antoine Rossignol** et son fils **Bonaventur**e élaborent le « Grand Chiffre de Louis XIV » qui tombera en désuétude après la mort de ses inventeurs, et ses règles précises seront rapidement perdues. Le Grand Chiffre est si robuste qu'on sera encore incapable de le lire à la fin du XIX^{e} siècle, jusqu'à ce qu'**Étienne Bazeries** réussisse à la casser.

• L'essor des communications (de 1800 à 1970)

Les nouvelles techniques de communications (moyens de transports rapides, journaux, télégraphe, télégraphie sans fil) donnent une nouvelle impulsion à la cryptologie. Pour la première fois de l'histoire de l'humanité, une parole va plus vite qu'un messager à cheval. La transmission d'un message se libère du transport. Forcément, les guerres modernes utilisent abondamment les télécommunications ; l'interception devient simple et le décryptement des informations devient vital. La cryptologie entre dans son ère industrielle.

Les années 1790 — **Thomas Jefferson**, futur président des États-Unis, invente son cylindre chiffrant, si bien conçu qu'après plus d'un siècle et demi de rapide progrès technique, il sera encore utilisé. C'est certainement le moyen de chiffrement le plus sûr de l'époque, et pourtant il sera classé et oublié. Il sera réinventé en 1891 par **Étienne Bazeries**, qui ne parviendra toutefois pas à le faire adopter par l'armée française. L'armée américaine mettra en service un système presque identique en 1922.

1854 — **Charles Wheatstone**, un des pionniers du télégraphe électrique, invente le chiffre Playfair, du nom de son ami **Lyon Playfair** qui popularisera ce chiffre.

1854 — **Charles Babbage** casse le chiffre de Vigenère, mais sa découverte reste ignorée, car il ne la publie pas. Ce travail ne sera mis en lumière qu'au XX^{e} siècle, lors de recherches effectuées sur l'ensemble des papiers de Babbage.

1857 — Après la mort de l'amiral Sir **Francis Beaufort**, son frère publie le chiffre de Beaufort (une variante du chiffre de Vigenère).

1859 — **Pliny Earl Chase** publie dans *Mathematical Monthly* la première description d'un chiffre tomogrammique.

1861 — **Friedrich W. Kasiski** publie *Die Geheimshriften und die Dechiffrierkunst* (les chiffres et l'art du déchiffrement), qui donne la première solution générale pour le déchiffrement d'un chiffre polyalphabétique à clef périodique, marquant ainsi la fin de plusieurs siècles d'invulnérabilité du chiffre de Vigenère.

1917 **Gilbert S. Vernam**, travaillant pour AT&T, invente une machine de chiffre polyalphabétique pratique capable d'employer une clef qui est totalement aléatoire et ne se répète jamais – un « masque jetable ». C'est le seul chiffre, dans nos connaissances actuelles, dont on a prouvé qu'il était indécryptable en pratique et en théorie. Ce procédé ne sera cependant jamais utilisé par l'armée, car il exige de devoir produire des millions de clefs différentes (une par message), ce qui est impossible en pratique. En revanche, il sera utilisé par les diplomates allemands dès 1921.

1918 Le système ADFGVX est mis en service par les Allemands à la fin de la Première Guerre mondiale. Il sera cassé par le lieutenant français **Georges Painvin**.

1918 **Arthur Scherbius** fait breveter sa machine à chiffrer ENIGMA. Il est à noter que trois autres inventeurs, dans trois pays, ont, chacun de son côté et presque simultanément, l'idée d'une machine basée sur des rotors : **Hugo Alexandre Koch**, **Arvid Gerhard Damm** et **Edouard Hugh Hebern**.

1925 **Boris Caesar Wilhelm Hagelin** (1892-1983) propose à l'armée suédoise la machine B-21, qui sera pendant une décennie la machine la plus compacte capable d'imprimer des messages chiffrés. Pendant la Seconde Guerre mondiale, les Alliés fabriquèrent une autre machine de Hagelin, la Hagelin C-36 (appelée M-209 aux États-Unis), à 140 000 exemplaires. Après la guerre, Boris Hagelin créera à Zoug, en Suisse, Crypto AG, qui est aujourd'hui encore l'un des principaux fabricants d'équipements cryptographiques.

1929 **Lester S. Hill** publie son article *Cryptography in an Algebraic Alphabet*, dans *American Mathematical Monthly*, 36, 1929, pp. 306-312. Il y décrit le chiffre qui porte son nom. C'est un chiffre polygraphique où l'on utilise des matrices et des vecteurs.

1931 **Herbert O. Yardley** publie *The American Black Chamber*, un des livres les plus célèbres sur la cryptologie. Avant cela, il avait décrypté entre autres les codes japonais (avant leur machine PURPLE).

1933-1945 La machine ENIGMA n'est pas un succès commercial (son prix a découragé de nombreux acheteurs potentiels), mais elle est reprise et améliorée pour devenir la machine cryptographique de l'Allemagne nazie. Elle est cassée par le mathématicien polonais **Marian Rejewski**, qui s'est basé seulement sur un texte chiffré et une liste des clefs quotidiennes obtenues par un espion. Pendant la guerre, les messages sont régulièrement décryptés par **Alan Turing**, **Gordon Welchman** et d'autres à Bletchley Park, en Angleterre, à l'aide des premiers ordinateurs (les fameuses « bombes »).

1940 **William Frederick Friedman**, plus tard honoré comme le père de la cryptanalyse américaine, à la tête de son équipe du Signal Intelligence Service (S.I.S.), réussit le décryptement de la machine de cryptage japonaise PURPLE. Avec sa femme, il s'intéressera beaucoup aux chiffres shakespeariens.

• La cryptologie moderne (de 1970 à nos jours)

Les ordinateurs et le réseau Internet font entrer la cryptologie dans son ère moderne. La grande invention de ces dernières décennies est la cryptographie à clef publique.

Le futur sera peut-être la cryptographie quantique, définitivement indécryptable.

1970 Au début des années 1970, **Horst Feistel**, un des premiers cryptographes universitaires, mène un projet de recherche à l'IBM Watson Research Lab et développe le chiffre *Lucifer*, qui inspirera plus tard le chiffre DES et d'autres algorithmes de chiffrement symétrique par blocs.

1976 **Whitfield Diffie** et **Martin Hellman** publient *New Directions in Cryptography*, article qui introduit l'idée de cryptographie à clef publique. Ils donnent une solution entièrement nouvelle au problème de l'échange de clefs. Ils avancent aussi l'idée d'authentification à l'aide d'une fonction à sens unique. Ils terminent leur papier avec une observation intéressante : « L'habileté dans la cryptanalyse a toujours été lourdement du côté des professionnels, mais l'innovation, en particulier dans la conception des nouveaux types de systèmes cryptographiques, est venue principalement d'amateurs. »

Nov. 1976 DES, pour Data Encryption Standard (en français : standard de cryptage de données), est un algorithme très répandu à clef privée dérivé du chiffre Lucifer de Feistel dans sa version à 64 bits. Il sert à la cryptographie et l'authentification de données. Il est jugé si difficile à percer par le gouvernement des États-Unis qu'il est adopté par le ministère de la Défense des États-Unis, qui contrôle depuis lors son exportation. Cet algorithme a été étudié intensivement et est devenu l'algorithme le mieux connu et le plus utilisé dans le monde à ce jour. Bien que DES soit très sûr, certaines entreprises préfèrent utiliser le triple-DES, qui n'est rien d'autre que l'algorithme DES appliqué trois fois, avec trois clefs privées différentes.

Avril 1977 RSA signifie Rivest-Shamir-Adleman, en l'honneur de ses trois inventeurs : **Ron Rivest**, **Adi Shamir** et **Leonard Adleman**, qui l'ont inventé en 1977. Le brevet de cet algorithme appartient à la société américaine RSA Data Security, qui fait maintenant partie de Security Dynamics, et aux Public Key Partners (PKP à Sunnyvale, Californie, États-Unis), qui possèdent les droits en général sur les algorithmes à clef publique. RSA est un algorithme à clef publique qui sert aussi bien à la cryptographie de documents qu'à l'authentification. Comme il est très sûr, l'algorithme RSA est devenu un standard *de facto* dans le monde.

1978 L'algorithme RSA est publié dans les *Communications de l'ACM*.

1990 **Xuejia Lai** et **James Massey** publient *A Proposal for a New Block Encryption Standard*, un algorithme de cryptage des données International (l'IDEA : International Data Encryption Algorithm) – pour remplacer le DES. L'IDEA emploie une clef de 128 bits et utilise des opérations convenant bien à tout type d'ordinateurs, permettant donc une programmation plus efficace. Il s'agit d'un des meilleurs algorithmes de chiffrement, si ce n'est le meilleur. Personne n'a déclaré à ce jour avoir cassé d'une manière ou d'une autre le moindre bloc de texte chiffré par IDEA. Il est actuellement exploité par la société Mediacrypt.

1990 **Charles H. Bennett** et **Gilles Brassard** publient leurs résultats expérimentaux sur la cryptographie quantique, qui emploie des photons pour communiquer un flot de bits qui serviront de clefs pour un cryptage de type Vernam (ou d'autres utilisations). En supposant que les lois de la mécanique quantique se vérifient, la cryptographie quantique offre non seulement le secret, mais permet aussi de savoir si la ligne a été écoutée.

1991 **Phil Zimmermann** sort sa première version de PGP (Pretty Good Privacy) en réponse à la menace du FBI d'exiger l'accès au message clair des citoyens. PGP offre une haute sécurité au citoyen, et cela gratuitement.

Août 1999 Onze sites répartis dans six pays factorisent le premier nombre ordinaire de 155 chiffres décimaux (512 bits). Un tel nombre aurait pu servir de clef dans un système de chiffrement moderne de type RSA, qui est utilisé dans le commerce électronique. Un tel record remet en question l'utilisation de clefs trop petites dans de tels systèmes.

2000 *Rijndael* a été conçu par **Joan Daemen** et **Vincent Rijmen**, deux chercheurs belges, dans le but de devenir un candidat à l'*Advanced Encryption Standard* (AES) du NIST (National Institute of Standards and Technology). *Rijndael* a été choisi comme standard en 2000, prenant la place du premier véritable standard de la cryptographie : le DES.

1.3. Conventions

Dans la plupart des livres, les lettres d'un message codé sont en majuscules, celle d'un message clair en minuscules. Nous avons aussi adopté cette convention.

Sauf exception, les messages clairs ne contiennent pas de lettres accentuées, ni d'espaces, ni de signes de ponctuation. On ne chiffrera donc que les lettres de *a* à *z*.

Traditionnellement, on regroupe les lettres d'un cryptogramme par groupes de cinq, car ainsi le nombre de lettres se compte plus rapidement. D'autre part, on complique un peu la tâche du casseur de code en ne respectant pas les espaces entre les mots du clair.

On utilisera des abréviations du style [ABCD12] pour se référer à un livre de la bibliographie, où ABDC sont, en principe, les quatre premières lettres de l'auteur et 12 les deux derniers chiffres de l'année de parution du livre.

1.4. QR Codes

Cette deuxième édition est un « livre augmenté ». Vous trouverez au fil des pages des « QR Codes » ressemblant à ceci :

Pour les utiliser, il vous faudra tout d'abord installer sur votre smartphone une application qui lit les QR Codes. Vous pointerez ensuite un QR Code avec la caméra de votre appareil pour accéder à la page web qui vous permettra d'essayer le système de chiffrement présenté.