Exercices et problèmes de cryptographie

Damien Vergnaud
Professeur à Sorbonne Université

Préface de **Jacques Stern**
Professeur à l'École normale supérieure

4e édition

DUNOD

Illustration de couverture : © faithie/Shutterstock

© Dunod, 2023
11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-085923-8

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).
Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

PRÉFACE

« Pour devenir habile en quelque profession que ce soit, il faut le concours de la nature, de l'étude et de l'exercice ». Cette maxime d'Aristote semble bien mal s'appliquer à la cryptologie tant l'exercice y est absent. Il existe de multiples ouvrages de référence de qualité mais, pour la plupart, ils sollicitent très peu l'initiative des étudiants. Et même ceux – rares – qui sont accompagnés d'un véritable choix de problèmes à résoudre, par exemple sous forme d'un livre compagnon, ne couvrent pas totalement une discipline qui connaît une évolution rapide. C'est donc un réel manque que vient combler le recueil que propose Damien Vergnaud.

Le livre que j'ai le plaisir de présenter est issu d'un vrai travail de terrain puisqu'il est le résultat de plusieurs années d'enseignement de la cryptologie à l'Ecole normale supérieure. À l'évidence, l'auteur a beaucoup de talent pour éveiller l'intérêt des étudiants et les conduire, pas à pas, à s'approprier les concepts et les méthodes de la science du secret. Beaucoup de culture également, puisque les sujets choisis sont extrêmement variés à l'image d'une science qui emprunte à l'algèbre, à la théorie des probabilités, à l'algorithmique, à la théorie de l'information. D'ailleurs, ils débordent largement le cadre strict de la cryptographie. Ce talent et cette culture conduisent à un choix d'exercices qui ne demandent pas simplement à l'étudiant de faire des gammes mais lui proposent de s'attaquer à de véritables compositions : ici un effort raisonnable de programmation illustre des cryptanalyses célèbres comme celle de l'Enigma ou celle du programme Venona qui a permis l'interception de communications où les services russes mettaient incorrectement en oeuvre le chiffrement jetable ; là une invitation à « mettre la main à la pâte » permet d'entrer de plain pied dans les méthodes modernes de cryptanalyse – différentielle et linéaire – des algorithmes conventionnels tels que le DES ou l'AES ; là encore, une initiation progressive aux méthodes de factorisation d'entiers, intiment liées à la sécurité du RSA est proposée.

Présenter un tel ouvrage comme un simple livre d'exercices est le reflet de la modestie de son auteur. Certes, il permet la pratique nécessaire à l'acquisition des éléments essentiels de la cryptologie. Mais il va au-delà de cet objectif : chaque chapitre inclut une présentation qui est un véritable cours d'introduction et l'ensemble constitue de fait une forme d'ouvrage d'enseignement avancé fondé sur la pratique. En d'autres termes, le lecteur qui va au terme de tous les exercices proposés est

déjà un véritable spécialiste, capable de se confronter aux multiples concepts que la cryptologie moderne a développés ces trente dernières années. À un moment où la cryptologie est au cœur de la société de l'information, de l'internet aux moyens de paiement en passant par les téléphones portables, une telle expertise est indispensable et il faut souhaiter au livre de Damien Vergnaud des lecteurs à la fois nombreux et actifs.

Jacques Stern, Professeur à l'Ecole normale supérieure

TABLE DES MATIÈRES

AVANT-PROPOS

La cryptologie est un ensemble de techniques permettant d'assurer la sécurité des systèmes d'information. Cette discipline permet notamment de conserver aux données leur caractère de confidentialité, de contrôler leur accès ou d'authentifier des documents. L'utilisation de la cryptographie est de plus en plus répandue et les utilisateurs des systèmes cryptographiques doivent être en mesure non seulement de comprendre leur fonctionnement mais aussi d'en estimer la sécurité.

Cet ouvrage s'adresse aux étudiants de second cycle d'informatique ou de mathématiques. Il s'est développé à partir de textes de travaux dirigés et de travaux pratiques proposés à des étudiants du *Master Parisien de Recherche en Informatique* et aux élèves de première année de l'*École normale supérieure*. Il a été conçu pour aider à assimiler les connaissances d'un cours d'introduction à la cryptologie et à se préparer aux examens. Il présente les outils mathématiques et algorithmiques utiles en cryptographie et les fonctionnalités cryptographiques de base dans le cadre de la cryptographie symétrique et asymétrique.

Cet ouvrage est destiné directement aux étudiants de « master 1 » mais certains exercices pourront être abordés par un étudiant motivé de licence ayant un goût pour l'algorithmique dans ses aspects mathématiques et pratiques. À l'intention des étudiants plus avancés, nous avons inclus des énoncés plus difficiles qui sont alors signalés par une étoile ($\star$). Enfin, l'ouvrage sera utile aux enseignants de cryptologie qui y trouveront un support pour leurs travaux dirigés.

La cryptologie est liée à d'autres disciplines mathématiques et informatiques comme l'arithmétique, l'algèbre, l'algorithmique, ou la théorie de la complexité. Le bagage informatique et mathématique requis pour aborder ce livre est celui que l'on acquiert lors des deux premières années de licence ou en classes préparatoires scientifiques augmenté de quelques notions de théorie des nombres de niveau 3ème année. Ces notions plus avancées font l'objet de brefs rappels qui n'ont cependant pas pour ambition de remplacer un livre de cours.

Le but de cet ouvrage est de permettre à ceux qui le souhaitent de s'initier à la cryptographie par l'exemple. Il propose plus de 140 exercices et problèmes entièrement utilisés dans le cadre de travaux dirigés, de travaux pratiques ou d'examens. Ces exercices sont entièrement corrigés mais le lecteur ne tirera profit de ce livre que s'il cherche des solutions personnelles avant d'en étudier les corrections. L'étude de la cryptologie moderne ne peut se concevoir sans un ordinateur à portée de main et le

livre propose de nombreux exercices de programmation qui ont pour but notamment d'acquérir une pratique de la cryptanalyse. Ces exercices sont signalés par le symbole ⌨ alors que les exercices qui ne nécessitent pas de programmation sont indiqués par le symbole ✍. Les données numériques des exercices de programmation sont disponibles en ligne sur le site

https://www.dunod.com/EAN/9782100852840

pour épargner au lecteur la tâche fastidieuse consistant à recopier les énoncés des exercices avant de les traiter. Le lecteur trouvera également des exercices supplémentaires et des références complémentaires sur ce site.

Avant propos de la quatrième édition. Cette nouvelle édition a été inspirée par les nombreuses demandes et remarques que m'ont envoyées des étudiants et collègues, utilisateurs des éditions précédentes. Elle m'a donné l'occasion de modifier et réécrire des parties importantes du texte en suivant ces remarques sur le contenu, le style et l'organisation de l'ouvrage. En plus d'épurer le texte de ses inévitables erreurs typographiques et coquilles, j'ai simplifié et clarifié une grande partie des énoncés des exercices et de leurs solutions. J'ai notamment ajouté des questions intermédiaires pour simplifier la résolution de certains exercices et détaillé certains points techniques dans des solutions d'exercices complexes. J'ai supprimé certains exercices jugés trop difficiles et j'en ai également ajouté de nouveaux. Enfin, les compléments en ligne qui accompagnent l'ouvrage ont été enrichis de nombreux exercices supplémentaires et d'autres exercices et compléments de cours seront ajoutés progressivement.

Remerciements. J'adresse un chaleureux merci à CH. BOUILLAGUET, D. NACCACHE et J. STERN avec qui j'ai eu le plaisir d'enseigner la cryptologie à l'ENS et à Sorbonne Université. Ma gratitude va également aux étudiants et aux élèves normaliens qui ont testé, malgré eux, la majorité des exercices présentés dans ce livre. Ce texte doit beaucoup à des conversations de couloirs et je tiens également à remercier les doctorants, post-doctorants et membres permanents de l'équipe Cryptographie de l'ENS - et particulièrement P.-A. FOUQUE - et de l'équipe ALMASTY de Sorbonne Université pour toutes les discussions que nous avons pu avoir. Je tiens à remercier J. JEAN pour la création et la maintenance du dépôt *TikZ for Cryptographers* [46] à partir duquel certaines figures de ce livre ont été adaptées. Enfin, je voudrais remercier A. BAUER, J.-L. BLANC, O. BLAZY, G. CASTAGNOS, C. CHEVALIER, P.-A. FOUQUE, A. GUILLEVIC, A. HUCHET, M. JALLIER-LUNDGREN, L. KHATI, F. LAGUILLAUMIE, R. LESCUYER, N. LIONET, B. MARTIN, F. MARTINEZ, A. PASSELÈGUE, D. H. PHAN, A. VALENCIA, J. VERGNAUD et V. ZUCCA pour la rigueur et la pertinence de leurs nombreux commentaires.

NOTATIONS

Les conventions et notations suivantes sont utilisées dans cet ouvrage.

Ensembles. Nous utilisons les notations ensemblistes classiques : $\emptyset$ désigne l'ensemble vide ; $x \in A$ signifie que x est un élément de l'ensemble A. Pour deux ensembles A et B, $A \subseteq B$ indique que A est un sous-ensemble de B (alors que $A \subset B$ indique que A est un sous-ensemble strict de B). De plus, $A \cup B$ désigne la réunion de A et B, $A \cap B$ désigne l'intersection de A et B, $A \setminus B$ l'ensemble des éléments de A qui ne sont pas dans B et $A \times B$ le produit cartésien des ensembles A et B. Le cardinal d'un ensemble A est noté $\#A$.

Nous utilisons les notations classiques suivantes pour désigner certains ensembles :

$\mathbb{N}$	ensemble des entiers naturels
$\mathbb{P}$	ensemble des nombres premiers
$\mathbb{Z}$	anneau des entiers relatifs
$\mathbb{Q}$	corps des nombres rationnels
$\mathbb{R}$	corps des nombres réels
$\mathbb{C}$	corps des nombres complexes
$(\mathbb{Z}/n\mathbb{Z})$	anneau des résidus modulo un entier $n \geq 1$
$\mathbb{F}_q$	corps fini à q éléments
$\mathfrak{S}_A$	groupe de permutations de l'ensemble A
A^*	groupe des éléments inversibles d'un anneau A
$\mathcal{M}_{n,m}(A)$	ensemble des matrices carrées $n \times m$ à coefficients dans un anneau A
$\mathcal{M}_\ell(A)$	anneau des matrices carrées $\ell \times \ell$ à coefficients dans un anneau A
$A[X]$	anneau des polynômes à une indéterminée X à coefficients dans un anneau A

La lettre p désigne le plus souvent un nombre premier $p \in \mathbb{P}$ et nous notons $(p_n)_{n\geq 1}$ la suite croissante des nombres premiers (avec $p_1 = 2$, $p_2 = 3$, ...). Pour un polynôme $P \in A[X]$, nous notons $\deg P$ le degré de P.

La notation $\mathbb{G}$ désigne un groupe dont la loi est notée multiplicativement. L'élément neutre pour la multiplication dans $\mathbb{G}$ est noté $1_\mathbb{G}$. L'ordre d'un groupe $\mathbb{G}$ est noté $|\mathbb{G}| = \#\mathbb{G}$ et $\langle g \rangle$ désigne le sous-groupe de $\mathbb{G}$ engendré par $g \in \mathbb{G}$.

Pour un entier $n \geq 2$, un élément de l'anneau $(\mathbb{Z}/n\mathbb{Z})$ sera identifié avec l'unique membre de sa classe de l'ensemble $\{0, \ldots, n-1\}$. Pour un entier $a \in \mathbb{Z}$, $(a \bmod n)$

désignera reste de la division euclidienne de a par n (dans $\{0, \ldots, n-1\}$). Pour deux entiers $a, b \in \mathbb{Z}$, la relation $a \equiv b \pmod{n}$ indique que a est congru à b modulo n (c.-à-d. que n divise $a - b$) et $a \not\equiv b \pmod{n}$ que a n'est pas congru à b modulo n.

Fonctions. Nous notons $f : A \longrightarrow B$ pour indiquer que f est une fonction d'un ensemble A dans un ensemble B. Pour un sous-ensemble $A' \subseteq A$, nous notons $f(A') = \{f(a), a \in A'\} \subseteq B$. Pour un sous-ensemble $B' \subseteq B$, nous notons $f^{-1}(B') = \{a \in A, f(a) \in B'\} \subseteq A$.

La composition de fonctions est notée $\circ$. Pour une fonction $f : A \longrightarrow A$, f^0 est la fonction identité sur A et $f^{i+1} = f^i \circ f$ pour $i \in \mathbb{N}$.

Nous utilisons les notations classiques suivantes pour désigner certains fonctions :

$\lfloor x \rfloor$	partie entière par défaut de $x \in \mathbb{R}$ ($\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$)
$\lceil x \rceil$	partie entière par excès de $x \in \mathbb{R}$ ($\lceil x \rceil - 1 < x \leq \lceil x \rceil$)
$\ln(x)$	logarithme népérien de $x \in \mathbb{R}$ ($x > 0$)
$\log(x)$	logarithme en base 2 de $x \in \mathbb{R}$ ($x > 0$)
$\text{logdisc}_g(h)$	logarithme discret de $h \in \langle g \rangle$ en base $g \in \mathbb{G}$
$\pi(x)$	nombre de nombres premiers inférieurs ou égaux à x ($\#\{p \in \mathbb{P}, p \leq x\}$)
$\Psi(x, y)$	fonction de Dickman-De Bruijn ($\#\{n \in \mathbb{N}, n \leq x$ et n est y-friable$\}$)
$\binom{n}{m}$	coefficient binomial $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ pour $0 \leq m \leq n$
$\left(\frac{x}{m}\right)$	symboles de Legendre et de Jacobi
$a \mid b$	a divise b
$a \nmid b$	a ne divise pas b
$\text{pgcd}(a, b)$	plus grand commun diviseur de $a, b \in \mathbb{Z}$
$\text{ppcm}(a, b)$	plus petit commun multiple de $a, b \in \mathbb{Z}$
$\mathbf{P}(E)$	probabilité d'un événement E
$\mathbb{E}(X)$	espérance d'une variable aléatoire X
$\varphi(n)$	fonction indicatrice d'Euler $\varphi(n) = \lvert(\mathbb{Z}/n\mathbb{Z})^*\rvert$

Chaînes binaires. Dans les chapitres 2,3 et 4, nous utilisons une fonte de type « machine à écrire » pour représenter la valeur d'un octet avec deux chiffres hexadécimaux : `00` $= 0$, `01` $= 1$, …, `0A` $= 10$, …, `10` $= 16$, …, `FF` $= 255$.

Nous utilisons les notations classiques suivantes sur les chaînes binaires :

$\{0,1\}^n$	ensemble des chaînes de binaires de longueur n
$\{0,1\}^*$	ensemble des chaînes de binaires de longueur finie
$\wedge$	et logique (bit-à-bit pour deux chaînes de même longueur)
$\vee$	ou logique (bit-à-bit pour deux chaînes de même longueur)
$\oplus$	« ou exclusif » (bit-à-bit pour deux chaînes de même longueur)
$\neg$	non logique (bit-à-bit)
$\|x\|$	longueur binaire d'une chaîne $x \in \{0,1\}^*$
$\overline{x}$	chaîne binaire complémentaire de x ($\overline{x} = \neg x$)
$x\|\|y$	concaténation des chaînes x et y
x^n	concaténation de la chaîne x n fois ($\underbrace{x\| \ldots \|x}_{n \text{ fois}}$)
$x[a..b]$	sous-chaîne de x formée des bits situés entre les positions a et b (inclues).
$\lll i$	rotation à gauche d'une chaîne de bits de i positions

Notations algorithmiques. Les algorithmes sont présentés sous forme de pseudo-code simple (notamment en s'affranchissant des problèmes de mémoire). Les entrées et les sorties sont toujours précisées. Les structures de contrôle classiques sont notées en gras (**tant que** condition **faire** instructions, **si** condition **alors** instructions **sinon** instructions, ...).

Les commentaires dans les algorithmes sont signalés par le symbole $\triangleright$. Le symbole $a \leftarrow b$ indique l'assignation algorithmique (c.-à-d. a prend la valeur de b) et le symbole $a \xleftarrow{\text{⚄⚄}} A$ l'assignation d'un élément tiré uniformément aléatoirement (c.-à-d. un élément est tiré uniformément aléatoirement dans l'ensemble A et la valeur obtenue est enregistrée dans a).

Dans ce livre, nous n'étudierons que des algorithmes classiques et pas les algorithmes conçus pour être exécutés sur un ordinateur *quantique* (c.-à-d. qui exploite les phénomènes de la mécanique quantique). La construction d'un ordinateur quantique à grande échelle semble lointaine en raisons de difficultés techniques mais un tel ordinateur présenterait un danger en cryptographie.
Des encadrés de ce type seront utilisés pour mentionner (sans détails) des résultats importants liés aux algorithmes quantiques en cryptographie.

CRYPTOGRAPHIE CLASSIQUE

1

La cryptologie est une science très ancienne : les hommes ont toujours eu besoin de dissimuler des informations et de transmettre des messages en toute confidentialité. Le terme cryptologie vient du grec *kruptos* (κρυπτός) signifiant *secret, caché* et de *logos* (λογός) signifiant *discours*. La cryptologie est donc la *science du secret*. Elle regroupe la cryptographie et la cryptanalyse : la première a pour but de concevoir des systèmes visant à assurer la sécurité des communications sur un canal de communication public et la seconde vise à trouver des failles dans ces systèmes.

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs et le chiffrement des communications militaires a depuis l'Antiquité été une préoccupation majeure des diverses forces armées. Le *chiffrement* regroupe les techniques mises en œuvre pour brouiller la signification d'un message qui est matériellement visible. Le contenu du message ne doit alors être récupérable que par les personnes auxquelles le message est adressé. Le chiffrement fait appel à deux processus élémentaires de transformation du message pour satisfaire ces propriétés :

— la *substitution* qui consiste à remplacer, sans en modifier l'ordre, les symboles d'un texte clair par d'autres symboles,
— et la *transposition* qui repose sur le bouleversement de l'ordre des symboles (mais pas leur identité).

Dans ce chapitre, nous allons étudier des systèmes de chiffrement relativement simples qui ont été utilisés de l'Antiquité (*chiffrement de César* ou *scytale*) jusqu'au début du XX^{e} siècle (*chiffrement de Vernam*, *chiffrement de Hill*, *machine Enigma*).

1.1 Chiffrement par substitution monoalphabétique

Le *chiffrement par substitution* consiste à remplacer dans un message un ou plusieurs symboles par un ou plusieurs symboles (généralement du même alphabet) tout en conservant l'ordre de succession des symboles du message. Dans cette section, nous considérons le chiffrement par substitution *monoalphabétique* qui consiste à remplacer chaque symbole individuel du message par un autre symbole de l'alphabet. Nous allons étudier des techniques de cryptanalyse permettant d'attaquer un tel système.

Elles reposent sur l'analyse des fréquences des symboles utilisés dans le texte chiffré et utilisent le fait que, dans chaque langue, certains symboles ou combinaisons de symboles apparaissent plus fréquemment que d'autres. Les systèmes de chif-