

Exercices et problèmes de cryptographie

Damien Vergnaud

Professeur à Sorbonne Université

Préface de **Jacques Stern**

Professeur à l'École normale supérieure

4^e 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^o et 3^o 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, intimement 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

Préface	I
Avant-propos	IX
Notations	XI
1 Cryptographie classique	1
1.1 Chiffrement par substitution monoalphabétique	1
📖 Exercice 1.1 Chiffrement de César	3
📖 Exercice 1.2 Chiffrement affine	4
📖 Exercice 1.3 Substitution monoalphabétique	6
1.2 Chiffrement par substitution polyalphabétique	8
📖 Exercice 1.4 Chiffrement de Vigenère - test de Kasiski	9
📖 Exercice 1.5 Chiffrement de Vigenère - indice de coïncidence . .	11
📖 Exercice 1.6 Chiffrement autoclave de Vigenère	12
🔗 Exercice 1.7 Chiffrement de Playfair - nombre de clés	15
📖 Exercice 1.8 Chiffrement de Playfair - cryptanalyse ★	17
🔗 Exercice 1.9 Chiffrement de Hill - nombre de clés	21
🔗 Exercice 1.10 Chiffrement de Hill - attaque à clair connu	22
📖 Exercice 1.11 Chiffrement de Hill - attaque à clair partiellement connu	24
1.3 Chiffrement par transposition	26
📖 Exercice 1.12 Scytale	26
📖 Exercice 1.13 Chiffrement par transposition par colonnes	28
1.4 Chiffrement parfait	29
🔗 Exercice 1.14 Carré latin	29
📖 Exercice 1.15 Mauvaise utilisation du chiffrement jetable	31
🔗 Problème 1.16 Algorithme de Viterbi	32
1.5 La machine Enigma	34
🔗 Exercice 1.17 Enigma - Nombre de clés	36
📖 Exercice 1.18 Enigma - Tableau de connexions	37
🔗 Problème 1.19 Enigma - Indice de coïncidence	38
2 Chiffrement par bloc	41
2.1 Modes opératoires	41
🔗 Exercice 2.1 Modes opératoires et propriétés de sécurité	44

🔧 Exercice 2.2	Mode opératoire CBC*	46
🔧 Exercice 2.3	Mode CBC et processus de bourrage RFC 2040 . . .	48
2.2	Schémas de Feistel	50
🔧 Exercice 2.4	Schéma de Feistel à un ou deux tours	51
🔧 Exercice 2.5	Sécurité du schéma de Feistel à trois tours ★	53
🔧 Exercice 2.6	Attaque contre un schéma de Feistel à trois tours . .	54
2.3	Chiffrement DES	56
🔧 Exercice 2.7	Clés faibles et semi-faibles du chiffrement DES . . .	57
🔧 Exercice 2.8	Propriété de complémentation du chiffrement DES .	59
🔧 Exercice 2.9	Chiffrement DES avec blanchiment	60
🔧 Exercice 2.10	Chiffrement double	61
🔧 Exercice 2.11	Chiffrement Triple – DES avec deux clés indépen- dantes	63
2.4	Réseaux de substitution-permutation	64
🔧 Exercice 2.12	Construction de Even-Mansour	65
🔧 Exercice 2.13	Construction minimaliste de Even-Mansour	66
🔧 Exercice 2.14	Réseau de substitution-permutation à un tour	67
🔧 Exercice 2.15	Réseau de substitution-permutation à deux tours . .	68
🔧 Exercice 2.16	Réseau de substitution-permutation LowMC	71
2.5	Chiffrement AES	72
🔧 Exercice 2.17	Boîte S de l’AES	74
🔧 Exercice 2.18	Opération MixColumns	77
🔧 Exercice 2.19	Propriétés de l’opération MixColumns	78
🔧 Exercice 2.20	Diversification de clé de l’AES	81
3	Fonctions de hachage cryptographiques	83
3.1	Généralités sur les fonctions de hachage	83
🔧 Exercice 3.1	Propriétés des fonctions de hachage	84
🔧 Exercice 3.2	Construction de Merkle-Damgård	85
🔧 Exercice 3.3	Collision sur la fonction MD5 tronquée	87
3.2	Chiffrement par bloc et fonction de compression	89
🔧 Exercice 3.4	Chiffrement par bloc et fonction de compression . .	89
🔧 Exercice 3.5	Construction de Matyas-Meyer-Oseas et DES	90
🔧 Exercice 3.6	Attaque en pré-image pour la construction de Rabin ★	91
3.3	Attaques génériques sur les fonctions de hachage itérées	94
🔧 Exercice 3.7	Multicollisions pour les fonctions de hachage itérées	94
🔧 Exercice 3.8	Attaque en collision contre fonctions de hachage concaténées	95
🔧 Problème 3.9	Attaque de Kelsey-Schneier	97
3.4	Fonctions éponges et SHA-3	100
🔧 Exercice 3.10	Attaques en collision sur les fonctions éponges . . .	102
🔧 Exercice 3.11	Attaques en seconde pré-image sur les fonctions éponges	104

🔧 Exercice 3.12	Attaque en pré-image sur les fonctions éponges . . .	106
4	Techniques avancées en cryptanalyse symétrique	111
4.1	Cryptanalyse différentielle	111
📖 Exercice 4.1	Table des différences du DES	112
🔧 Problème 4.2	Cryptanalyse différentielle de FEAL – 4 ★	114
4.2	Cryptanalyse différentielle impossible	118
🔧 Exercice 4.3	Attaque par différentielle impossible contre DEAL .	119
🔧 Problème 4.4	Attaque par différentielle impossible contre l’AES ★	122
4.3	Cryptanalyse linéaire	126
📖 Exercice 4.5	Table d’approximation linéaire du DES	126
🔧 Exercice 4.6	Approximation linéaire de l’addition	128
🔧 Problème 4.7	Cryptanalyse linéaire de SAFER ★	130
🔧 Exercice 4.8	Biais de la parité d’une permutation	133
4.4	Attaques par saturation	134
🔧 Problème 4.9	Attaque par saturation contre l’AES ★	135
🔧 Exercice 4.10	Attaque par distingueur sur Ladder – DES	138
5	Chiffrement par flot	141
5.1	Registres à décalage à rétroaction linéaire	141
🔧 Exercice 5.1	LFSR et polynômes de rétroaction	143
🔧 Exercice 5.2	Propriétés statistiques d’une suite produite par un LFSR	144
🔧 Exercice 5.3	Reconstruction du polynôme de rétroaction minimal	145
5.2	Chiffrement par flot par registres à décalage irrégulier	146
📖 Exercice 5.4	Distingueur sur le générateur à signal d’arrêt	147
🔧 Problème 5.5	Propriétés du générateur par auto-rétrécissement . .	150
5.3	Chiffrement par flot par registre filtré	151
🔧 Exercice 5.6	Attaque « deviner et déterminer » sur Toyocrypt . .	152
🔧 Exercice 5.7	Attaque algébrique sur Toyocrypt ★	153
5.4	Chiffrement par flot par registres combinés	155
🔧 Exercice 5.8	Attaque par corrélation sur le générateur de Geffe . .	155
🔧 Exercice 5.9	Attaque « deviner et déterminer » sur le générateur de Geffe	157
🔧 Exercice 5.10	Attaque algébrique sur le générateur de Geffe	158
5.5	Le chiffrement par flot A5/1	159
🔧 Exercice 5.11	États internes de A5/1	160
🔧 Exercice 5.12	Attaque par compromis temps-mémoire sur A5/1 . .	162
🔧 Problème 5.13	Attaque « deviner et déterminer » sur A5/1	163
5.6	Le chiffrement par flot RC4	166
🔧 Exercice 5.14	Cryptanalyse de RC4 sans opération d’échange ★ . .	167
🔧 Exercice 5.15	Biais de la suite chiffrente produite par RC4	168
🔧 Problème 5.16	Attaque par recouvrement de clé sur RC4	171

6	Problème du logarithme discret	173
6.1	Logarithme discret dans un groupe générique	173
🔧	Exercice 6.1 Multi-exponentiation	174
🔧	Exercice 6.2 Algorithme de Shanks	176
🔧	Exercice 6.3 Algorithme ρ de Pollard	178
🔧	Exercice 6.4 Algorithme de Pohlig-Hellman	181
📖	Exercice 6.5 Application de l'algorithme de Pohlig-Hellman . . .	183
6.2	Problème du logarithme discret dans $(\mathbb{Z}/p\mathbb{Z})^*$	185
🔧	Exercice 6.6 Entiers friables	185
🔧	Problème 6.7 Méthode de Kraitichik - Calcul d'indice $\star$	188
6.3	Problèmes algorithmiques liés au logarithme discret	192
🔧	Exercice 6.8 Auto-réductibilité du problème du logarithme discret	192
🔧	Exercice 6.9 Problème de la représentation	193
🔧	Exercice 6.10 Algorithme λ de Pollard	196
🔧	Exercice 6.11 Variantes du problème du logarithme discret	198
🔧	Problème 6.12 Logarithme discret de petit poids de Hamming . . .	201
6.4	Interpolation polynomiale de logarithme discret	205
🔧	Exercice 6.13 Polynôme interpolateur du logarithme discret	205
🔧	Exercice 6.14 Degré d'un polynôme interpolateur du logarithme discret	207
7	Factorisation des entiers et primalité	209
7.1	Tests de primalité	209
🔧	Exercice 7.1 Certificats de primalité de Pratt	210
🔧	Exercice 7.2 Nombres pseudo-premiers de Fermat en base a . . .	211
🔧	Problème 7.3 Nombres de Carmichael - Critère de Korselt	212
📖	Exercice 7.4 Recherche de nombres de Carmichael	214
🔧	Exercice 7.5 Test de primalité de Solovay-Strassen	219
🔧	Exercice 7.6 Nombres pseudo-premiers forts en base 2	221
🔧	Exercice 7.7 Solovay-Strassen et Miller-Rabin pour $n \equiv 3 \pmod{4}$	223
🔧	Exercice 7.8 Solovay-Strassen et Miller-Rabin	224
🔧	Exercice 7.9 Identité de Agrawal-Kayal-Saxena	226
7.2	Méthodes exponentielles de factorisation	227
📖	Exercice 7.10 Factorisation par divisions successives	227
📖	Exercice 7.11 Factorisation par la méthode de Fermat	228
🔧	Exercice 7.12 Algorithme de Lehman $\star$	229
🔧	Exercice 7.13 Méthode $p - 1$ de Pollard	231
📖	Exercice 7.14 Factorisation par la méthode $p - 1$ de Pollard	233
🔧	Exercice 7.15 Algorithme ρ de Pollard	233
7.3	Multi-évaluation de polynômes et algorithme de Pollard-Strassen . . .	235
🔧	Exercice 7.16 Division euclidienne rapide par la méthode de Newton	235
🔧	Exercice 7.17 Multi-évaluation d'un polynôme univarié	237
🔧	Exercice 7.18 Algorithme de Pollard-Strassen	239

7.4	Racine carrée modulaire et factorisation	241
	✎ Exercice 7.19 Extraction de racine carrée modulo p	241
	✎ Exercice 7.20 Extraction de racine carrée modulo p^ℓ	243
	✎ Exercice 7.21 Extraction de racine carrée modulo N	245
	✎ Problème 7.22 Carrés modulaires friables	246
	✎ Exercice 7.23 Factorisation et logarithme discret	251
8	Chiffrement à clé publique	253
8.1	Fonction RSA	253
	✎ Problème 8.1 Fonction RSA, exposant et factorisation	254
	✎ Exercice 8.2 Auto-réductibilité du problème RSA	257
	✎ Exercice 8.3 Points fixes de la fonction RSA	258
	✎ Problème 8.4 Sécurité des bits de la fonction RSA	259
8.2	Chiffrement RSA	261
	✎ Exercice 8.5 Sécurité du protocole de chiffrement RSA naïf	262
	✎ Exercice 8.6 RSA avec module commun	263
	✎ Exercice 8.7 Diffusion de données chiffrées avec RSA	264
	✎ Exercice 8.8 Attaque de Wiener	265
	✎ Exercice 8.9 Application de l'attaque de Wiener	267
	✎ Exercice 8.10 RSA et clairs liés	269
	✎ Exercice 8.11 RSA et petits textes clairs	270
	✎ Problème 8.12 Implantation de RSA et théorème chinois des restes	272
	✎ Problème 8.13 Chiffrement de Paillier	274
	✎ Exercice 8.14 Chiffrement fondé sur l'identité de Cocks $\star$	278
8.3	Mise en accord de clé de Diffie-Hellman	281
	✎ Exercice 8.15 Attaque par le milieu	282
	✎ Problème 8.16 Logarithme discret et Diffie-Hellman $\star$	284
8.4	Chiffrement d'ElGamal et variantes	286
	✎ Exercice 8.17 Sécurité du chiffrement d'ElGamal naïf	287
	✎ Exercice 8.18 Sécurité des bits du logarithme discret	288
	✎ Exercice 8.19 « Petits » sous-groupes et chiffrement d'ElGamal	291
9	Signatures numériques	293
9.1	Signatures fondées sur la primitive RSA	293
	✎ Exercice 9.1 Sécurité du protocole de signature RSA naïf	294
	✎ Exercice 9.2 Sécurité de $\mathcal{F}$ -RSA et propriétés de $\mathcal{F}$	295
	✎ Exercice 9.3 Sécurité de $\mathcal{F}$ -RSA pour la recommandation CCITT	297
	✎ Exercice 9.4 Sécurité de $\mathcal{F}$ -RSA avec encodage PKCS #1 v1.5	300
	✎ Exercice 9.5 Redondance linéaire et contrefaçon existentielle	302
	✎ Exercice 9.6 Redondance linéaire et contrefaçon universelle $\star$	303
	✎ Problème 9.7 Sécurité du protocole de signature de Boyd	305
9.2	Signatures d'ElGamal et variantes	308
	✎ Exercice 9.8 Contrefaçon existentielle du schéma d'ElGamal naïf	308

✎ Exercice 9.9	Contrefaçon universelle du schéma d'ElGamal naïf .	309
✎ Exercice 9.10	Vérification des signatures d'ElGamal	310
✎ Exercice 9.11	Fonction de hachage et sécurité des signatures de Schnorr	312
📖 Exercice 9.12	Paramètres publics dans le protocole DSA	313
✎ Exercice 9.13	Clé temporaire et sécurité des signatures d'ElGamal	314
9.3	Signatures de Lamport et variantes	315
✎ Exercice 9.14	Sécurité et efficacité des signatures de Lamport . . .	316
✎ Exercice 9.15	Signatures de Lamport avec plusieurs signatures . .	316
✎ Exercice 9.16	Messages de longueur variable et signatures de Lamport	317
✎ Exercice 9.17	Espace des messages des signatures de Lamport . . .	318
✎ Exercice 9.18	Arbres de Merkle	320
✎ Exercice 9.19	Signatures de Winternitz	323
✎ Problème 9.20	Sécurité du protocole de signature de Groth	325
Bibliographie		329
Index		337

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 (*). 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 $p_1 = 2, p_2 = 3, \dots$). 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 $\{0, \dots, n-1\}$. Pour un entier $a \in \mathbb{Z}$, $(a \bmod n)$

désignera reste de la division euclidienne de a par n (dans $\{0, \dots, n-1\}$). 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 certaines 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 $x \in \mathbb{R}$ ($x > 0$)
$\log_{\text{disc}_g}(h)$	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 ($\#\{n \in \mathbb{N}, n \leq x \text{ et } n \text{ est } y\text{-friable}\}$)
$\binom{n}{m}$	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) = (\mathbb{Z}/n\mathbb{Z})^* $

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 $x \in \{0, 1\}^*$
$\bar{x}$	chaîne binaire complémentaire de x ($\bar{x} = \neg x$)
$x y$	concaténation des chaînes x et y
x^n	concaténation de la chaîne x n fois $\underbrace{(x \dots x)}_{n \text{ fois}}$
$x[a..b]$	sous-chaîne de x formée des bits situés entre les positions a et b (incluses).
$\lll i$	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 $a \leftarrow \boxed{\cdot} \boxed{\cdot} \boxed{\cdot} \boxed{\cdot}$ 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.

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-