PDF Sommaire pour 26781

Le présent fichier PDF **Sommaire** reproduit des extraits du livre

Théorie des codes
Compression, cryptage, correction

Les auteurs de ce livre sont : Jean-Guillaume Dumas , Jean-Louis Roch, Eric Tannier, Sébastien Varrette.
Il s'agit d'une 3ème édition par Dunod, daté de 2018.

Cet ouvrage est disponible sous le numéro **AC 26781** dans l'inventaire de la collection de l'ACONIT, Association pour un conservatoire de l'informatique et de la télématique, Grenoble.

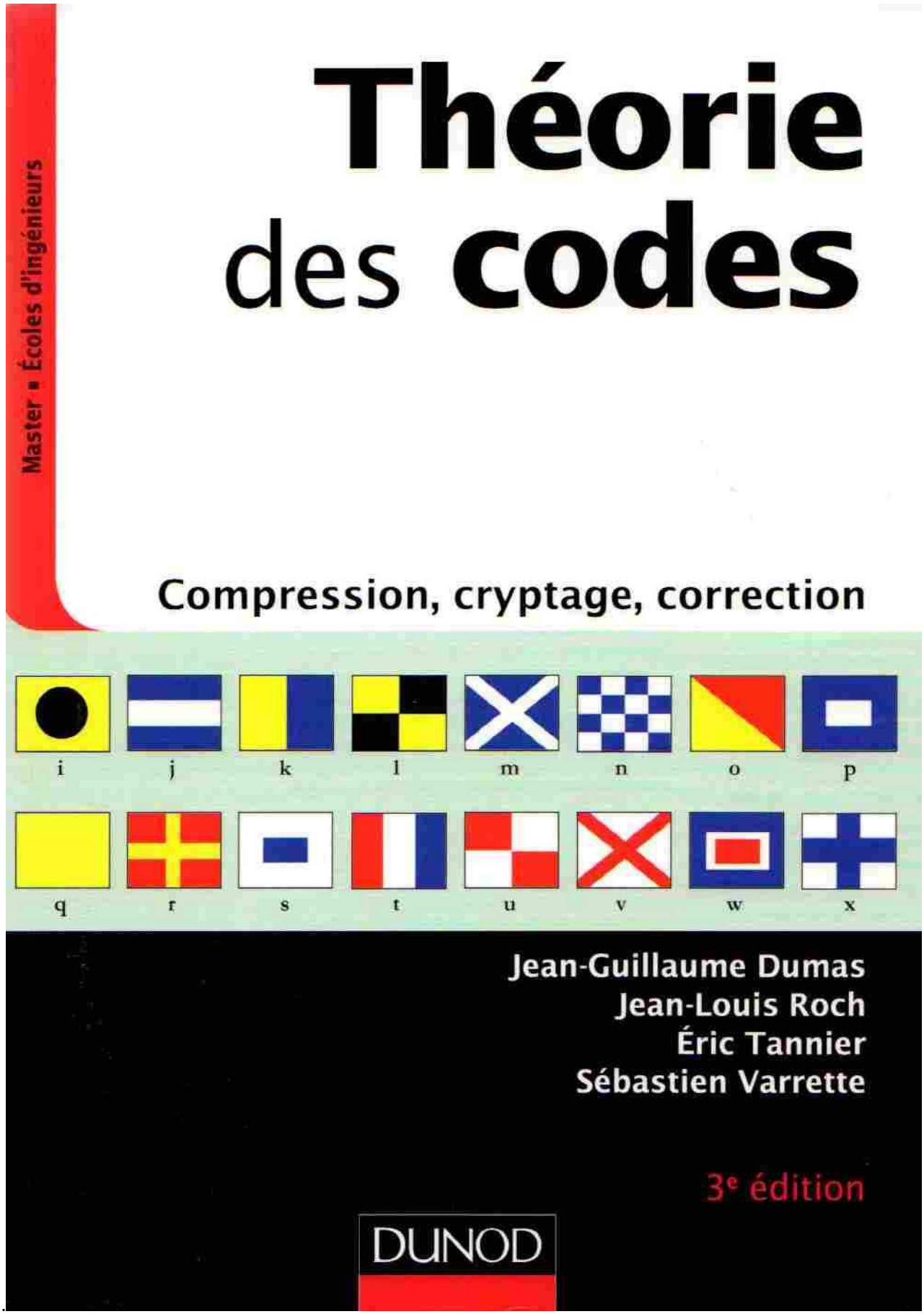
Il comprend 401 pages, structurées en 4 parties, avec de nombreux schémas, et des descriptions d'algorithmes et de normes. Sont aussi donnés des exercices à faire, leur correction étant en fin du livre.

Les extraits fournis dans le présent PDF donnent en copie :

- Les pages de couverture, dont la 4ème page de couverture indiquant les orientations du texte et qui sont les auteurs
- Le préambule (2 pages) qui indique l'origine du livre et ses différentes éditions,
- La table des Matières/sommaire (8 pages),
- La liste des figures, tables, algorithmes et acronymes (7 pages),
- La bibliographie (3 pages)

Fiche rédigée le 8/3/2019 par Jean Ricodeau.

Page de couverture



4ème page de couverture

Info Sup

Jean-Guillaume Dumas · Jean-Louis Roch
Éric Tannier · Sébastien Varrette

3e édition

Théorie des codes

Compression, cryptage, correction

Cet ouvrage est destiné aux étudiants en master de mathématiques appliquées ou d'informatique ainsi qu'aux élèves ingénieurs. Il sera également utile à tous ceux qui travaillent dans les télécommunications ou la cybersécurité.

L'**efficacité**, la **sécurité**, l'**intégrité** sont les trois préoccupations essentielles de ceux qui conçoivent des méthodes de transmission de l'information.

Pour y parvenir la théorie des codes s'appuie sur un certain nombre d'outils issus de l'algèbre linéaire, de l'arithmétique, des probabilités et de l'algorithmique qui sont présentés de manière pédagogique et approfondie dans ce livre.

Les notions de cours sont illustrées par près de **150 exercices corrigés.**

Jean-Guillaume Dumas
est professeur à l'université Grenoble Alpes.

Jean-Louis Roch
est maître de conférences à l'ENSIMAG.

Éric Tannier
est chercheur de l'INRIA Rhône-Alpes à l'université Lyon I.

Sébastien Varrette
est chercheur à l'université du Luxembourg.

LES + EN LIGNE

Ce livre est prolongé par des contenus en ligne librement accessibles à l'adresse :
https://theoriedescodes.imag.fr.

Vous y trouverez des solutions interactives à certains exercices qui sont mises en œuvre avec le logiciel mathématique Sage, ainsi que des compléments d'information et le moyen de contacter les auteurs.

9 782100 781096

2228297
ISBN 978-2-10-078109-6

LICENCE MASTER DOCTORAT
1 2 3 4 5 6 7 8

Les actus du savoir

DUNOD
dunod.com

Préambule

Ce livre est un manuel pour étudiants en master, en mathématiques appliquées ou informatique. Il peut être utilisé comme référence par des enseignants, chercheurs ou ingénieurs, par des entreprises impliquées dans la télécommunication et la sécurité des informations.

Nous avons veillé à ce que cet ouvrage puisse être le plus indépendant possible, en particulier tous les termes utilisés sont définis, les notions de bases rappelées. Néanmoins ces rappels ne remplacent pas un cours complet d'algèbre, d'algorithmique ou de probabilités, et la maîtrise préalable de ces notions sera utile à la lecture.

Cet ouvrage a été initié au printemps 2000, avec la création du département ENSIMAG-ENSERG télécommunications à l'Institut national polytechnique de Grenoble (INPG) et la construction d'un cours général d'introduction aux codes et à leurs applications. Il a évolué en devenant un support de référence pour différents cours des universités de Grenoble, à la fois à l'INPG et à l'université Joseph Fourier, puis l'université Grenoble Alpes (UGA) pour paraître sous forme de livre chez Dunod en 2007, en version corrigée et augmentée en 2009, puis dans une nouvelle édition en 2013. Il a été traduit en anglais et est paru dans cette langue chez Wiley en 2015 sous le titre "*Foundations of Coding*".

Nous remercions chaleureusement nos collègues Gilles Debunne, Yves Denneulin, Dominique Duval, Grégory Mounié et Karim Samaké qui ont participé à ces enseignements et ont contribué par leurs commentaires à améliorer notre support de cours. Mouloud Aït-Kaci, Éric Bourre, Cécile Canovas-Dumas, Rodney Coleman, Mélanie Favre, Françoise Jung, Madeline Lambert, Benjamin Mathon, Clément Pernet, Marie-Aude Steineur, Antoine Taveneaux et Romain Xu ont également relu des parties de cet ouvrage et nous ont aidé à corriger plusieurs erreurs.

Pour la seconde, puis la présente édition, nous avons actualisé l'ouvrage en intégrant des techniques récentes, comme les courbes elliptiques, les codes à faible densité ou les codes-barres bidimensionnels, nous avons abordé l'utilisation de la cryptographie dans les applications mobiles (Facebook Messenger,

WhatsApp, Telegram) et les réseaux sociaux (Keybase), et nous avons élaboré des guides de bonnes pratiques de sécurité pour les utilitaires dorénavant incontournables comme GPG ou SSH. Nous avons également mis à jour plusieurs parties, incluant la stéganographie et le tatouage d'images, les attaques par saturations, la cryptographie post-quantique, les chiffrements homomorphes, les preuves à divulgation nulle de connaissance, le partage de secret et les codes d'interpolation, ou encore les standards récents comme le hachage de Galois, le portfolio e-stream et le standard de hachage SHA-3 (Keccak) ainsi que le règlement européen eIDAS.
Par ailleurs, 26 nouveaux exercices complètent les 120 exercices originaux et, pour plusieurs d'entre eux, des solutions interactives utilisant le logiciel libre de calcul mathématique Sage sont dorénavant disponibles sur le site internet compagnon du livre : `https://theoriedescodes.imag.fr`.

Grenoble, Lyon, Luxembourg, le 23 avril 2018.
Jean-Guillaume Dumas, Jean-Louis Roch, Éric Tannier, Sébastien Varrette.

Ce livre est accompagné d'un site internet :

https://theoriedescodes.imag.fr

Ce site donne plus de détails sur les auteurs, notamment des liens pour les contacter, leurs pages internet personnelles, etc.
Le sujet étant en constante évolution, on trouvera également sur le site une bibliographie plus détaillée.
*Enfin, pour plusieurs des exercices de livre, la solution de fin d'ouvrage pourra s'accompagner d'une solution interactive avec le logiciel libre de calcul mathématique Sage (**http://www.sagemath.org**). La présence d'une telle solution interactive est repérée à la page de la solution par la mention du site internet, comme dans l'exemple : Exercice 4.43, page 303 (theoriedescodes.imag.fr/Ex/#4.43).*
*L'utilisateur pourra consulter les captures d'écran en pdf, ou utiliser directement le code source de chaque exercice, soit dans sa propre installation du logiciel Sage, soit au travers d'un serveur Sage de calcul collaboratif, comme **https://cocalc.com**.*

Sommaire

Préambule V

Introduction 1

1 Théorie des codes 7

1.1 De Jules César à la télécopie 7

1.1.1 La source : de l'image à la suite de pixels 7

1.1.2 La compression du message 8

1.1.3 La détection d'erreurs 9

1.1.4 Le chiffrement 10

1.1.5 Le décodage 11

L'attaque et le déchiffrement 11

La décompression et les pertes 12

1.1.6 Les défauts de ce code 12

1.1.7 Ordres de grandeur et bornes de complexité des algorithmes 14

Taille des nombres 14

La vitesse des ordinateurs 14

Taille et âge de l'univers 15

Complexité des algorithmes 15

1.2 Codage par flot et probabilités 17

1.2.1 Vernam et le chiffrement à clef jetable (one-time-pad) . 17

1.2.2 Un peu de probabilités 18

Évènements et mesure de probabilité 19

Probabilités conditionnelles et formule de Bayes 19

1.2.3 Entropie 20

Source d'information 20

Entropie d'une source 21

Entropies conjointe et conditionnelle 22

Extension d'une source 23

1.2.4 Stéganographie et tatouage numérique 25

1.2.5 Chiffrement parfait 26
1.2.6 Chiffrement parfait en pratique et principes de Kerckhoffs 27
1.3 Codage par blocs, algèbre et arithmétique 28
1.3.1 Blocs et modes de chaînage, du CBC au CTR 29
1.3.2 Structures algébriques des mots de codes 32
Groupes 33
Anneaux 34
Corps 36
Espaces vectoriels et algèbre linéaire 36
1.3.3 Codage bijectif d'un bloc 38
Inverse modulaire : algorithme d'Euclide 38
L'indicatrice d'Euler et le théorème de Fermat 41
L'exponentiation modulaire et le logarithme discret . . . 43
Fonctions à sens unique 45
1.3.4 Construction des corps premiers et corps finis 46
Tests de primalité et génération de nombres premiers . . 47
Arithmétique des polynômes 49
L'anneau $V[X]/P$ et les corps finis 51
Polynômes irréductibles 52
Constructions des corps finis 54
1.3.5 Implémentations des corps finis 56
Opérations sur les polynômes 56
Utilisation des générateurs 57
Racines primitives 59
1.3.6 Courbes sur des corps finis 61
Modèle de Weierstraß 61
Le groupe des points d'une courbe elliptique 63
1.3.7 Générateurs pseudo-aléatoires 65
Les générateurs congruentiels 67
Les registres à décalage linéaire 67
Générateurs cryptographiquement sûrs 69
Quelques tests statistiques 70
1.4 Décoder, déchiffrer, attaquer 72
1.4.1 Décoder sans ambiguïté 72
Propriété du préfixe 74
L'arbre de Huffman 76
Représentation des codes instantanés 76
Théorème de McMillan 77
1.4.2 Les codes non injectifs 78
L'empreinte de vérification 78
Les fonctions de hachage 78

Transformations avec perte 83
Transformée de Fourier et transformée discrète 84
Algorithme de la Transformée de Fourier discrète (DFT) 85
DFT et racines $n^{\text{ièmes}}$ de l'unité dans un corps fini 87
Produit rapide de polynômes par la DFT 89
Partage de secret 90
1.4.3 Cryptanalyse 90
Attaque des générateurs congruentiels linéaires 91
Algorithme de Berlekamp-Massey pour la synthèse de registres à décalage linéaire 91
Le paradoxe des anniversaires 94
Attaque de Yuval sur les fonctions de hachage 95
Factorisation des nombres composés 96
Nombres premiers robustes 101
Résolution du logarithme discret 102

2 Théorie de l'information et compression 107
2.1 Théorie de l'information 108
2.1.1 Longueur moyenne d'un code 108
2.1.2 L'entropie comme mesure de la quantité d'information . 109
2.1.3 Théorème de Shannon 110
2.2 Codage statistique 111
2.2.1 Algorithme de Huffman 112
L'algorithme de Huffman est optimal 115
2.2.2 Codage arithmétique 117
Arithmétique flottante 117
Arithmétique entière 120
En pratique 120
2.2.3 Codes adaptatifs 122
Algorithme de Huffman dynamique – `pack` 123
Compression dynamique 123
Décompression dynamique 124
Codage arithmétique adaptatif 125
2.3 Heuristiques de réduction d'entropie 126
2.3.1 Run-Length Encoding (RLE) 126
Le code du fax (suite et fin) 128
2.3.2 Move-to-Front 128
2.3.3 Transformation de Burrows-Wheeler (BWT) 129
2.4 Codes compresseurs usuels 132
2.4.1 Algorithme de Lempel-Ziv et variantes `gzip` 132
2.4.2 Comparaison des algorithmes de compression 136

2.4.3 Formats GIF et PNG pour la compression d'images . . . 137
2.5 La compression avec perte . . . 138
2.5.1 Dégradation de l'information . . . 138
2.5.2 Transformation des informations audiovisuelles . . . 139
2.5.3 Le format JPEG . . . 139
DCT-JPEG . . . 139
Tatouage numérique d'images JPEG . . . 142
JPSEC . . . 143
2.5.4 Le format MPEG . . . 144

3 Cryptologie **147**
3.1 Principes généraux et terminologie . . . 147
3.1.1 Terminologie . . . 147
3.1.2 À quoi sert la cryptographie ? . . . 148
3.1.3 Les grands types de menaces . . . 150
Cryptanalyse et attaques sur un chiffrement . . . 150
3.2 Système cryptographique à clef secrète . . . 152
3.2.1 Principe du chiffrement à clef secrète . . . 152
3.2.2 Classes de chiffrements symétriques . . . 154
Les chiffrements symétriques par flot . . . 154
Les chiffrements symétriques par blocs . . . 156
Chiffrement inconditionnellement sûr . . . 157
3.2.3 Le système Data Encryption Standard (DES) . . . 157
Présentation exhaustive du système DES . . . 157
Diversification de la clef dans DES . . . 158
Avantages et applications de DES . . . 159
Cryptanalyse de DES . . . 161
3.2.4 Le standard AES (Rijndael) . . . 163
Principe de l'algorithme . . . 165
La diversification de la clef dans AES . . . 170
Sécurité de AES . . . 172
3.3 Système cryptographique à clef publique . . . 173
3.3.1 Motivations et principes généraux . . . 173
3.3.2 Chiffrement Rivest-Shamir-Adleman (RSA) . . . 175
Efficacité et robustesse de RSA. . . . 176
Attaques sur RSA . . . 178
3.3.3 Chiffrement non-déterministe et OAEP . . . 179
3.3.4 Chiffrement El Gamal . . . 181
3.3.5 Codes homomorphes . . . 182
3.4 Authentification, intégrité, non-répudiation . . . 184
3.4.1 Fonctions de hachage cryptographiques . . . 185

MD5 187
SHA-1 et SHA-256. 188
Whirlpool 190
Keccak (SHA-3) 191
État des lieux sur la résistance aux collisions 192
Performance des principales fonctions de hachage 193
3.4.2 La signature électronique 194
Contrôle d'intégrité par les fonctions de hachage 194
Codes d'authentification ou MAC 195
Les signatures numériques 197
La signature RSA 198
Le Standard de Signature Digitale (DSS) 199
3.4.3 Preuve à divulgation nulle de connaissance 201
3.5 Protocoles usuels de gestion de clefs 202
3.5.1 Génération de bits cryptographiquement sûre 202
3.5.2 Protocole d'échange de clef secrète de Diffie-Hellman et attaque *Man-in-the-middle* 203
3.5.3 Kerberos : un distributeur de clefs secrètes 205
Présentation générale du protocole Kerberos 205
Détail des messages Kerberos 207
Les faiblesses de Kerberos 208
3.5.4 Authentification à clef publique 210
3.5.5 Infrastructures hiérarchiques à clefs publiques : PKIX . . 211
Principe général 211
Les éléments de l'infrastructure 212
Les certificats électroniques 214
Le modèle PKIX 217
Défauts des Public Key Infrastructure (PKI) 221
3.5.6 Architecture pair à pair par toile de confiance : le modèle hybride PGP 222
3.5.7 Un utilitaire de sécurisation de canal, SSH 230
Authentification du serveur 232
Établissement d'une connexion sécurisée 232
Authentification du client *i.e.* de l'utilisateur 233
Sécurité, intégrité et compression 233
3.5.8 Utilisation de la cryptographie dans les applications mobiles et les réseaux sociaux. 234
3.5.9 Projets de standardisation et recommandations 236

4 Détection et correction d'erreurs **239**
4.1 Principe de la détection et de la correction d'erreurs 240
4.1.1 Codage par blocs 240
4.1.2 Un exemple simple de détection par parité 241
4.1.3 Correction par parité longitudinale et transversale . . . 242
4.1.4 Schéma de codage et probabilité d'erreur 243
4.1.5 Deuxième théorème de Shannon 244
Rendement d'un code et efficacité 244
Capacité de canal 244
Transmission sans erreur sur un canal de capacité fixée . 246
4.2 Détection d'erreurs par parité - codes CRC 247
4.2.1 Contrôle de parité sur les entiers : ISBN, EAN, LUHN . 248
Code-barres EAN 248
Code ISBN 250
Clef RIB 250
Carte bancaire : LUHN-10 250
4.2.2 Codes de Redondance Cyclique (CRC) 251
Codage CRC 251
Décodage CRC 251
Nombre d'erreurs de bit détectées 252
Exemples de codes CRC 253
4.3 Distance d'un code 253
4.3.1 Code correcteur et distance de Hamming 253
4.3.2 Codes équivalents, étendus et raccourcis 257
Codes équivalents 257
Code étendu 257
Code poinçonné 258
Code raccourci 258
4.3.3 Code parfait 259
4.3.4 Codes de Hamming binaires 260
4.4 Codes linéaires et codes cycliques 262
4.4.1 Codes linéaires et redondance minimale 262
4.4.2 Codage et décodage des codes linéaires 265
Codage par multiplication matrice-vecteur 265
Décodage par multiplication matrice-vecteur 266
4.4.3 Codes LDPC 269
Matrice de contrôle creuse 269
Encodage Low Density Parity Check (LDPC) 269
Représentation par graphes de Tanner 270
Décodage itératif 272
Applications pratiques des codes LDPC 278

4.4.4 Codes cycliques 279
Caractérisation : polynôme générateur 280
Opération de codage 282
Détection d'erreurs et opération de décodage 283
4.4.5 Codes BCH 284
Codes d'interpolation et décodage de Berlekamp-Welch 284
Distance garantie 286
Construction des polynômes générateurs BCH 286
Codes BCH optimaux : codes de Reed-Solomon 288
Décodage rapide des codes de Reed-Solomon 289
Le protocole PAR-2 292
Code-barres bidimensionnel QR 293
4.5 Paquets d'erreurs et entrelacement 295
4.5.1 Paquets d'erreurs 295
4.5.2 Entrelacement 296
4.5.3 Entrelacement avec retard et table d'entrelacement . . . 296
4.5.4 Code entrelacé croisé et code CIRC 298
Application : code CIRC 299
4.6 Codes convolutifs et turbo-codes 302
4.6.1 Le codage par convolution 302
4.6.2 Le décodage par plus court chemin 303
Le diagramme d'état 304
Le treillis de codage 304
L'algorithme de Viterbi 305
Codes systématiques, rendement et poinçonnage 307
Codes convolutifs récursifs 307
4.6.3 Les turbo-codes 307
Composition parallèle 308
Décodage turbo 309
Turbo-codes en blocs et turbo-codes hybrides 311
Performances et applications des turbo-codes 311

Compression, cryptage, correction : en guise de conclusion 313

Solutions des exercices 317
Solutions des exercices proposés au chapitre 1 317
Solutions des exercices proposés au chapitre 2 331
Solutions des exercices proposés au chapitre 3 339
Solutions des exercices proposés au chapitre 4 359
Solution de l'exercice du casino 376

Liste des figures, tables, algorithmes et acronymes utilisés **379**
Liste des figures 379
Liste des tables 381
Liste des algorithmes 382
Liste des acronymes 383

Bibliographie **387**

Index **391**

Liste des figures, tables, algorithmes et acronymes utilisés

Liste des figures

1 Schéma fondamental du codage 1
2 Schéma des notions introduites dans le premier chapitre, avec leurs dépendances 4

1.1 Chiffrement bit à bit (par flot). 27
1.2 Mode de chiffrement par blocs ECB. 30
1.3 Mode de chiffrement par blocs CBC. 30
1.4 Mode de chiffrement par blocs CFB. 31
1.5 Mode de chiffrement par blocs OFB. 31
1.6 Mode de chiffrement par blocs CTR. 32
1.7 Principe d'une fonction à sens unique. 46
1.8 Addition d'une courbe elliptique (gauche) et doublement (droite) sur la courbe réelle $y^2 = x^3 - x\sqrt[3]{2}$ 63
1.9 Schéma de fonctionnement d'un LFSR. 68
1.10 Chiffrement *Bluetooth*. 69
1.11 Exemple d'arbre de Huffman. 76
1.12 Principe d'une fonction de hachage. 79
1.13 Fonction de compression d'une fonction de hachage. 81
1.14 Construction de Merkle-Damgård. 81
1.15 Constructions de Davies-Meyer (à g.) et Miyaguchi-Preneel (à d.). . . 82
1.16 Transformée de Fourier 84
1.17 Transformée de Fourier discrète (DFT) 84
1.18 Transformée en cosinus discrète (DCT) 85
1.19 Détection de cycle de Floyd, sous forme de Rho. 97

2.1 Algorithme de Huffman : départ 112
2.2 Algorithme de Huffman : première étape ($q = 2$) 112
2.3 Exemple de construction d'un code de Huffman. 114

2.4 Code du fax. 128
2.5 bzip2. 132
2.6 Image 8×8 en RGB sur fond blanc (ici en niveaux de gris). 140
2.7 Balayage en zigzag de JPEG. 141
2.8 Compression JPEG. 141
2.9 Compression MPEG-1. 144
2.10 Compression du son MP3. 145

3.1 Relation fondamentale de la cryptographie. 148
3.2 Principe d'un algorithme de contrôle d'intégrité. 149
3.3 Principe du chiffrement à clef secrète. 152
3.4 Chiffrement symétrique par flot (*Stream cipher*). 154
3.5 Chiffrement symétrique par blocs (*Bloc cipher*). 156
3.6 Un tour de DES. 158
3.7 La fonction f de DES. 159
3.8 La diversification de clef dans DES. 160
3.9 Représentation matricielle (par colonnes) d'un bloc de 16 octets. . . . 165
3.10 Étape `SubBytes` dans AES. 166
3.11 Opération `ShiftRows` dans AES. 168
3.12 Opération `MixColumns` dans AES. 169
3.13 Opération `AddRoundKey` dans AES. 170
3.14 Opération `KeyExpansion` dans AES. 170
3.15 Vision de la clef étendue `W` comme une succession de colonnes. 171
3.16 Principe du chiffrement à clef publique. 174
3.17 Optimal Asymmetric Encryption Padding (OAEP) 181
3.18 Retrait privé d'information par algèbre linéaire homomorphe. 183
3.19 Historique des principales fonctions de hachage. 185
3.20 Le i-ème tour dans MD5 ($0 \leqslant i \leqslant 63$). 188
3.21 Le i-ème tour dans SHA-1 ($0 \leqslant i \leqslant 79$). 189
3.22 Construction en éponge de Keccak (SHA-3). 191
3.23 Vérification d'intégrité par des fonctions de hachage en disposant d'un canal sécurisé. 194
3.24 Vérification d'intégrité par des fonctions de hachage à partir d'une fonction de chiffrement. 195
3.25 Principe d'utilisation d'un MAC. 196
3.26 Code d'authentification par chiffrement à clef secrète. 196
3.27 Principe de la signature à clef publique et de sa vérification. 199
3.28 Les étapes d'authentification Kerberos. 206
3.29 Principe de la création des certificats. 212
3.30 Émission d'un certificat. 213
3.31 Génération et contenu d'un certificat X.509. 215
3.32 Vérification de certificat et extraction de clef publique. 216
3.33 Le modèle PKI pour les certificats X-509. 217
3.34 Enregistrement authentifié. 218
3.35 Authentification par cryptographie à clef publique. 219
3.36 Un exemple du modèle de confiance de PGP. 223

3.37 Illustration du prototole d'établissement d'un tunnel SSH lors d'une authentification par clefs publiques. 230

4.1 Code EAN-128 de la théorie des codes. 249
4.2 Exemple d'un code LDPC régulier (10,5) et de sa représentation par un graphe de Tanner. Les six arêtes en gras illustrent un cycle de longueur 6. 271
4.3 Exemple de renversement de bit sur le code de Hamming $(7,4)$ et le mot reçu $y = 0011101$ pour un mot de code transmis $c = 0011001$. . . 274
4.4 Informations extrinsèques pour les messages $r_{j,i}^{(r)}$ (a) et $q_{i,j}^{(r)}$ (b) 275
4.5 Matrice QR 25×25 et localisation des motifs 294
4.6 Code QR de niveau 3-L pour `https://theoriedescodes.imag.fr` . . 294
4.7 Diagramme d'état du code convolutif de polynômes générateurs $P_1 = X$ et $P_2 = X + 1$. 304
4.8 Treillis du code convolutif généré par $P_1 = X$ et $P_2 = X + 1$. 305
4.9 Transformation d'un code convolutif systématique de longueur de contrainte 3 en code systématique récursif RSC. 308
4.10 Codeur turbo par composition parallèle et entrelacement de deux codeurs RSC. 309
4.11 Décodage itératif d'un turbo-code. 310

80 Codage $CORR(CRYPT(COMP(M)))$ d'un message M. 314
81 Décodage d'un message $M' = CORR(CRYPT(COMP(M)))$. 314

82 Arbre de Huffman et Théorème de McMillan 325
83 Algorithme de Viterbi sur le message 10010010011101111010. 374

Liste des tables

1.1 Répartition des lettres dans ce manuscrit LaTeX. 14
1.2 Complexités classiques obtenues par l'analyse d'algorithmes. 16
1.3 Un extrait du code ASCII. 29
1.4 Opérations sur les inversibles avec générateur en caractéristique impaire. 58
1.5 Lograrithme discret et exponentiation dans différents groupes 61
1.6 Lois de groupes en caractéristiques 2 et 3 avec $P = (x_1, y_1) \neq -P$ et $Q = (x_2, y_2) \neq \pm P$ 64
1.7 Extrait de table du χ^2. 71
1.8 Distribution des multiples de p modulo m. 97
1.9 Crible quadratique pour 7429. 101

2.1 Codage arithmétique de "bebecafdead". 118
2.2 Décodage arithmétique de "0.15633504500". 119
2.3 Codage arithmétique entier de "bebecafdead". 121
2.4 Décodage arithmétique entier de "156335043840". 122
2.5 BWT sur COMPRESSE. 130

2.6 Taux de compression de différents algorithmes. 136

3.1 Fréquence d'apparition des lettres en français. 153
3.2 Fréquences du texte chiffré comparées aux références. 154
3.3 Évolution de l'état interne et extraction des bits dans Rabbit 156
3.4 Complexité des cryptanalyses sur DES. 161
3.5 Coût et performance des attaques sur DES en 1996. 162
3.6 Vitesses comparées de quelques méthodes de chiffrements par blocs. . 164
3.7 `ShiftRows` : décalage des lignes en fonction de N_b dans l'algorithme Rijndael. 168
3.8 Conjectures sur les sécurités comparées de chiffrements par blocs . . . 182
3.9 Principales différences entre W et Rijndael. 190
3.10 Résistance aux collisions pour les principales fonctions de hachage. . . 192
3.11 Performances typiques des principales fonctions de hachage à travers la suite eBASH [5] pour des messages d'entrées M de différentes tailles. 193
3.12 Attaque Man-in-the-middle dans le protocole d'échange de clef de Diffie-Hellman. 204
3.13 Envoi de message intercepté par le Man-in-the-middle. 204

4.1 Ordre de grandeur du taux d'erreurs. 240
4.2 Codage avec bit de parité. 242
4.3 Correction d'erreurs par bits de parité. 243
4.4 Exemples de codes CRC. 254
4.5 Comparaison des principaux algorithmes de propagation 278
4.6 Table d'entrelacement initiale de retard 2 pour des mots de longueur 5. 297
4.7 Table d'entrelacement de retard 2 après un tour. 297
4.8 Quelques polynômes primitifs de $\mathbb{F}_2$. 315

Liste des algorithmes

1.1 Codage fax simplifié. 9
1.2 Décodage fax. 12
1.3 PGCD : algorithme d'Euclide. 38
1.4 PGCD : algorithme d'Euclide étendu. 40
1.5 Puissance modulaire. 44
1.6 Test de primalité de Miller-Rabin. 48
1.7 Évaluation de polynôme par le schéma de Horner 50
1.8 Test d'irréductibilité de Ben-Or. 54
1.9 Recherche d'un polynôme irréductible creux. 55
1.10 Test Racine Primitive. 59
1.11 Test Polynôme Générateur. 60
1.12 Transformée de Fourier Discrète Rapide, DFT_ω. 87
1.13 Produit rapide de deux polynômes. 89
1.14 Algorithme de Berlekamp-Massey. 93
1.15 Attaque des anniversaires de Yuval. 95
1.16 Factorisation de Pollard. 98

1.17 Factorisation par courbes elliptiques de Lenstra 99
1.18 Algorithme de Gordon. 102

2.1 Description de l'algorithme de Huffman. 112
2.2 Codage arithmétique. 118
2.3 Décodage arithmétique. 119
2.4 Algorithme de Huffman dynamique : compression. 124
2.5 Algorithme de Huffman dynamique : décompression. 125
2.6 Réciproque de la BWT. 131
2.7 LZW : compression. 134
2.8 LZW : décompression. 135

3.1 Chiffrement AES. 166
3.2 Diversification des clefs dans AES. 172
3.3 Galois Counter Mode 197
3.4 Astuce de Shamir pour double-et-ajoute simultané 201

4.1 Algorithme de renversement de bits à décision ferme 273
4.2 Décodage LDPC par propagation 276
4.3 Décodage des Reed-Solomon. 291
4.4 Algorithme de Viterbi (décodage des codes convolutifs). 306
4.5 Déchiffrement AES. 344
4.6 Factorisation de n à partir de (n,e,d) dans RSA (cas e petit). 347
4.7 Factorisation de n à partir de (n, e, d) dans RSA. 348
4.8 Générateur pseudo-aléatoire cryptographique RSA. 353
4.9 Décodage du code de répétition avec détection maximale. 362
4.10 Décodage du code de répétition avec correction maximale. 362
4.11 Décodage du code de répétition (détection et correction). 363
4.12 Distance d'un code ($|V| = 2$). 363

Liste des acronymes

ADSL Asymmetric Digital Subscriber Line 311
AES Advanced Encryption Standard 156
AKS Agrawal-Kayal-Saxena 48
ARQ Automatic Repeat reQuest 241
BCH Bose-Chaudhuri-Hocquenghem 287
BSC Binary Symmetric Channel 246
BWT Transformation de Burrows-Wheeler IX
CA Autorité de Certification 211
CBC Cipher Block Chaining 30
CFB Cipher FeedBack 31
CIRC Cross-Interleaved Reed-Solomon Code 299
CRC Codes de Redondance Cyclique XII
CRL Listes de Révocation de Certificats 214
CTR CounTeR mode encryption 32
CVV Cryptogramme Visuel de Vérification 251

DCT Transformée en cosinus discrète 85
DES Data Encryption Standard X
DFT Transformée de Fourier discrète IX
DLP Problème du Logarithme Discret 45
DRM Digital Right Management 26
DSS Standard de Signature Digitale XI
eBACS ECRYPT Benchmarking of Cryptographic Systems
ECB Electronic Code Book 29
ECC Cryptographie sur Courbes Elliptiques 182
ECDSA Elliptic Curve Digital Signature Algorithm 200
eIDAS Electronic IDentification Authentication and trust Services 236
FDD Facteurs de Degrés Distincts 282
GCM Galois Counter Mode 197
GIF Graphics Interchange Format 137
GPG Gnu Privacy Guard 223
GSM Global System for Mobile Communications 155
HDD Hard Disk Drives 240
JPEG Joint Photographic Experts Group 26
JPSEC Secure JPEG-2000 143
KDC Key Distribution Center 205
LDPC Low Density Parity Check XII
LFSR Registre à décalage à rétroaction linéaire 67
LZ77 Lempel-Ziv 1977 132
LZ78 Lempel-Ziv 1978 132
LZAP Lempel-Ziv All Prefixes 135
LZMA Lempel-Ziv Markov chain-Algorithm 133
LZMW Lempel-Ziv Miller-Wegman 135
LZO Lempel-Ziv Oberhumer 137
LZW Lempel-Ziv Welch 133
MAC Message Authentication Code 80
MD5 Message-Digest algorithm 5 186
MDC Manipulation Detection Code 80
MDS Maximum Distance Separable 264
MGF fonction génératrice de masque 191
MPEG Motion Picture Experts Group 144
NESSIE New European Schemes for Signatures, Integrity, and Encryption 182
NIST National Institute of Standards and Technology 65
NSC Non-Systematic Convolutional code 307
OAEP Optimal Asymmetric Encryption Padding 179
OFB Output FeedBack 31
OTR Off-the-Record Messaging 235
PAR PARity archive volume set 293
PGCD Plus Grand Commun Diviseur 35
PPCM Plus Petit Commun Diviseur 35
PGP Pretty Good Privacy 150
PKI Public Key Infrastructure XI
PKIX PKI for X.509 certificates 217
PNG Portable Network Graphics 138
QR Quick Response code 294
RA Autorité d'enregistrement 214
RAID Redundant Array of Independent Disks 293

RLE Run-Length Encoding IX
RSA Rivest-Shamir-Adleman X
RSC Recursive Systematic Convolutional codes 307
RGB Rouge/Vert/Bleu 139
SHA Secure Hash Algorithm 186
SSD Solid State Drives 240
SSH Secure SHell 230
SSL Secure Sockets Layer 220
TGS Ticket Granting Service 206
TLS Transport Layer Security 220
UHF Ultra Hautes Fréquences 254
UMTS Universal Mobile Telecommunications System 311
UPC-A Universal Product Code 248
YUV Espace colorimétrique luminance chrominance 139
ZOI Zone d'influence 143

Bibliographie

[1] Thierry Autret, Laurent Bellefin, et Marie-Laure Oble-Laffaire. *Sécuriser ses échanges électroniques avec une PKI : Solutions techniques et aspects juridiques.* Eyrolles, 2002.

[2] Gildas Avoine, Pascal Junod, et Philippe Oechslin. *Sécurité informatique : Exercices corrigés.* Vuibert, 2004.

[3] Michel Barlaud et Claude Labit, éditeurs. *Compression et codage des images et des vidéos.* Hermes, 2002.

[4] Daniel J. Barrett, Richard E. Silverman, et Robert G. Byrnes. *SSH, The Secure Shell : The Definitive Guide.* O'Reilly, 2^e édition, 2005.

[5] Daniel J. Bernstein et Tanja Lange. eBACS : ECRYPT benchmarking of cryptographic systems. `http://bench.cr.yp.to` (accédé le 23/04/2018).

[6] Johannes A. Buchmann. *Introduction à la cryptographie.* Dunod, 2006.

[7] Christophe Cachat et David Carella. *PKI Open source : déploiement et administration.* O'Reilly, 2003.

[8] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, et R. Thayer. Openpgp message format (rfc 4880), novembre 2007. `http://www.ietf.org/rfc/rfc4880.txt`.

[9] Alexandre Casamayou, Guillaume Connan, Thierry Dumont, Laurent Fousse, François Maltey, Matthias Meulien, Marc Mezzarobba, Clément Pernet, Nicolas M. Thiéry, et Paul Zimmermann. *Calcul mathématique avec Sage.* 2010. `http://sagebook.gforge.inria.fr/`.

[10] Gérard Cohen, Jean-Louis Dornstetter, et Philippe Godlewski. *Codes correcteurs d'erreurs.* Masson, 1992.

[11] Michel Demazure. *Cours d'algèbre. Primalité, Divisibilité, Codes.* volume XIII de *Nouvelle bibliothèque mathématique.* Cassini, Paris, 1997.

[12] Jean-Guillaume Dumas, Pascal Lafourcade, et Patrick Redon. *Architectures PKI et communications sécurisées.* Dunod, 2015.

[13] Jean-Guillaume Dumas, Pascal Lafourcade, et Sébastien Varrette. *Les blockchains en 50 questions.* Dunod, 2018.

[14] Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier, et Sébastien Varrette. *Foundations of Coding : Compression, Encryption, Error-Correction.* Wiley, USA, 2015. `http://foundationsofcoding.imag.fr`.

[15] Touradj Ebrahimi, Franck Leprévost, et Bertrand Warusfel, éditeurs. *Cryptographie et sécurité des systèmes et réseaux.* Hermes, 2006.

[16] Touradj Ebrahimi, Franck Leprévost, et Bertrand Warusfel, éditeurs. *Enjeux de la sécurité multimédia.* Hermes, 2006.

[17] Federal Information Processing Standards. Publication 180-1 : Secure hash standard, avril 1997. `http://www.itl.nist.gov/fipspubs/fip180-1.htm`.

[18] Federal Information Processing Standards. Publication 180-2 : Secure hash standard, août 2002. `https://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf`.

[19] Federal Information Processing Standards. Publication 180-4 : Secure hash standard, août 2015. `http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf`.

[20] Federal Information Processing Standards. Publication 202 : SHA-3 standard : Permutation-based hash and extendable-output functions, août 2015. `http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf`.

[21] Joachim von zur Gathen et Jürgen Gerhard. *Modern Computer Algebra.* Cambridge University Press, 1999.

[22] Alain Glavieux, éditeur. *Codage de canal.* Hermes, 2005.

[23] Aurélien Géron. *WiFi déploiement et sécurité : La QoS et le WPA.* Dunod/01 Informatique, 2^e édition, 2006.

[24] Godfrey Harold Hardy et Edward Maitland Wright. *An introduction to the theory of numbers.* Oxford science publications. Clarendon Press, 5^e édition, 1998.

[25] Eric Incerti. *Compression d'image : Algorithmes et standards.* Vuibert, 2003.

[26] J.Kelsey, S. Chang, et R. Perlner. Special publication 800-185 : SHA-3 derived functions : cSHAKE, KMAC, tuplehash and parallelhash, décembre 2016.

[27] Donald E. Knuth. *Seminumerical Algorithms*, volume 2 de *The Art of Computer Programming.* Addison-Wesley, Reading, MA, USA, 3^e édition, 1997.

[28] Neal Koblitz. *A Course in Number Theory and Cryptography.* Springer-Verlag, 1987.

[29] Rudolf Lidl et Harald Niederreiter. *Introduction to Finite Fields and their Applications.* Cambridge University Press, 1994. `http://www.loc.gov/catdir/toc/cam029/93049020.html`.

[30] Bruno Martin. *Codage, cryptologie et applications.* Presses Polytechniques et Universitaires Romandes, 2004.

[31] James Massey. *Applied digital information theory.* ETH Zurich, 1998. `http://www.isiweb.ee.ethz.ch/archive/massey_scr`.

[32] Stéphane Natkin. *Les protocoles de sécurité d'Internet.* Sciences Sup. Dunod, 2002.

[33] Pascal Plumé. *Compression de données.* Eyrolles, 1993.

[34] Alain Reboux. *Devenez un magicien du numérique : Effets graphiques, sonores et cryptographie.* Dunod, 2003.

[35] David Salomon. *Data Compression.* Springer, 1997.

[36] Bruce Schneier. *Secrets et mensonges : sécurité numérique dans un monde en réseau.* Vuibert informatique, 2000.

[37] Bruce Schneier. *Cryptographie appliquée, algorithmes, protocoles et codes source en C.* Vuibert, Paris, 2^{e} édition, 2001.

[38] Victor Shoup. *A computational introduction to number theory and algebra.* Cambridge University Press, 2005.

[39] Simon Singh. *Histoire des codes secrets.* LGF - Le livre de poche, 2001.

[40] Jacques Vélu. *Méthodes mathématiques pour l'informatique : Cours et exercices corrigés.* Dunod, 4^{e} édition, 2005.

[41] Damien Vergnaud. *Exercices et problèmes de cryptographie.* Dunod, 2012.