Introduction

La cryptologie est étymologiquement la science du secret. Cette science regroupe plusieurs disciplines. La cryptographie, qui est l'art de masquer des messages afin que seuls les destinataires légitimes puissent les déchiffrer, en est une. Mais ce n'est pas la seule. Citons par exemple la cryptanalyse, qui est l'étude des méthodes de chiffrements dans le but de les rendre inutiles.
Si certaines méthodes de cryptologie sont utilisées depuis l'Antiquité, la recherche scientifique dans ce domaine est assez récente. L'essentiel des découvertes a eu lieu au cours du XX^{e} siècle. Par exemple, la cryptographie à clé publique est un immense domaine de recherche qui a été initié au début des années 70.
Depuis quelques décennies, la cryptologie s'est étendue à d'autres sujets tels la signature électronique, l'identification ou l'authentification. Ces nouvelles possibilités sont probablement plus utiles que de chiffrer des messages. Tout un chacun en use quotidiennement sans même s'en rendre compte. Par exemple, lorsque l'on utilise une carte bancaire pour effectuer une transaction, plusieurs algorithmes d'authentification sont effectués entre le terminal et la puce de la carte pour que celle-ci « prouve » son authenticité.
Le but de ce livre est d'expliquer les méthodes les plus couramment utilisées actuellement pour effectuer les principales tâches cryptologiques. Le point important est qu'il s'agit bien d'expliquer et non pas seulement de décrire ces méthodes.
Par exemple, un groupe international de chercheurs ont décidé d'une méthode standard de chiffrement (de cryptage) en novembre 2001, celle-ci s'appelle **AES** (initiales de « Advanced Encryption Standard »). Il existe de multiples sources où l'on peut trouver une description détaillée de cet algorithme, notre but ici est de tenter de comprendre la logique ayant présidé à sa construction. Grâce à des considérations historiques, informatiques et mathématiques, nous allons percer à jour les raisons des différentes étapes. En fin de compte, cette succession de calculs *a priori* très mystérieuse va devenir très logique.
La cryptologie moderne s'appuie sur des notions mathématiques avancées (telle les courbes elliptiques que l'on décrira succintement) portant sur plusieurs domaines. On va se limiter ici à l'étude des notions d'arithmétique nécessaires en cryptologie. L'arithmétique ayant le double avantage d'être accessible aux étudiants dès la première année universitaire et d'être à la base des principales méthodes de cryptologie actuelles.

La première partie de cet ouvrage présente une brève histoire de la cryptologie. Les étapes les plus marquantes sont présentées afin de comprendre l'évolution

des idées dans ce domaine. Nous verrons qu'il existe des principes intemporels et que certains concepts anciens sont encore utilisés dans les méthodes les plus modernes.

La deuxième partie est une longue parenthèse mathématiques où sont développées les notions et propriétés utiles pour comprendre la cryptologie moderne. Cette partie peut être lue comme un cours d'algèbre de base et d'arithmétique.

La dernière partie poursuit la description des principales méthodes de cryptologie, en se concentrant sur celles développées à l'ère informatique. Les grandes découvertes de la fin du XX^{e} siècle y sont décrites en détail. Les différentes tâches de la cryptologie actuelles et les moyens de les accomplir sont également présentés.
Cette seconde édition permet de corriger quelques erreurs présentes dans la première édition, de mettre à jour les données et compléter diverses informations mais également de parler des nouveautés de la dernière décennie notamment des ordinateurs quantiques et de la blockchain.

Je tiens à remercier particulièrement Jacques Patarin, de l'université de Versailles, dont l'enthousiasme communicatif a largement contribué à mon goût pour la cryptologie.
Un grand merci à tous ceux qui ont contribué à l'amélioration de ce livre, par sa relecture et des suggestions pertinentes : Geneviève Moebs, Jérome Trosset dit « Adrameleck », Louis Rivoallan, Frédéric Manconi, Noël Fraissex, Jean-Philippe Furter, Étienne Matheron, Xavier Roart dit « Goto », sans oublier papy Jean-Paul et ma moman chérie.
Je tiens tout particulièrement remercier Axel Cypel pour sa lecture minutieuse de la première édition qui m'a grandement aidé pour rédiger le présent volume ! Merci aux relecteurs de la seconde édition : Texas Granger, ProfRogue, Key, FreshPineapple, Valoukanga, Matuidi Chariot et bien sûr un énorme merci à Blanche Heisler pour ses commentaires judicieux et son enthousiasme.
Il va sans dire que ma reconnaissance est immense envers mon épouse qui m'a supporté et soutenu pendant la préparation de cet ouvrage.

Table des matières

I Cryptologie à l'ancienne **1**

1 Historique **3**
I De l'Antiquité au Moyen Âge . . . 3
II Le chiffrement de Vigenère . . . 8
II.1 Description . . . 8
II.2 Cryptanalyse . . . 10
III Le one-time pad ou masque jetable . . . 12
IV La machine Enigma . . . 14
V Et après... . . . 18
VI Exercices . . . 19

II Les nombres de la cryptologie **21**

2 Divisibilité et congruence **23**
I Divisibilité . . . 23
I.1 Définitions et critères de divisibilité . . . 23
I.2 Division euclidienne . . . 25
II Congruence . . . 27
II.1 Relation d'équivalence . . . 27
II.2 Relation de congruence . . . 29
II.3 Preuve des critères de divisibilité . . . 30
II.4 Opérations et congruences . . . 32
II.5 Classes d'équivalence . . . 33
III Réponses aux questions . . . 35
IV Exercices . . . 36

3 Groupes - Anneaux - Corps **39**
I Groupes . . . 39
I.1 Définitions, premières propriétés . . . 39
I.2 Morphismes de groupes . . . 44
I.3 Sous-groupes . . . 46
I.4 Sous-groupes de $(\mathbb{Z}, +)$ . . . 47
II Anneaux et Idéaux . . . 48
II.1 Généralités . . . 49
II.2 Règles de calcul . . . 50

II.3 Éléments inversibles - Corps . . . 52
II.4 Morphismes d'anneaux . . . 53
II.5 Sous-anneaux et idéaux . . . 54
II.6 Intersection et somme d'idéaux . . . 55
II.7 Anneaux principaux . . . 57
II.8 Anneaux quotients . . . 60
III Réponses aux questions . . . 62
IV Exercices . . . 63

4 Arithmétique dans un anneau principal 65
I Plus grand diviseur commun . . . 66
I.1 Définition - Exemples . . . 66
I.2 Relation de Bézout . . . 69
I.3 Méthode de calcul : Algorithme d'Euclide . . . 70
II Éléments premiers entre eux . . . 73
III Plus petit multiple commun . . . 76
IV PGCD et PPCM de n éléments . . . 78
V Éléments irréductibles - Éléments premiers . . . 79
V.1 Définitions . . . 79
V.2 Comment trouver les nombres premiers ? . . . 80
V.3 Éléments premiers . . . 82
V.4 Décomposition en facteurs premiers . . . 84
V.5 Polynômes irréductibles . . . 86
V.6 Anneaux euclidiens et factoriels . . . 88
VI Réponses aux questions . . . 92
VII Exercices . . . 94

5 Anneau $\mathbb{Z}/n\mathbb{Z}$ 99
I Éléments inversibles et diviseurs de zéros . . . 100
II Et si n est un nombre premier ? . . . 104
III Équations et systèmes d'équations . . . 108
III.1 Équation $\dot{a}\dot{x} = \dot{b}$ dans $\mathbb{Z}/n\mathbb{Z}$ . . . 108
III.2 Théorème des restes chinois . . . 110
IV Décomposition de $\mathbb{Z}/n\mathbb{Z}$ . . . 112
V Réponses aux questions . . . 116
VI Exercices . . . 117

6 Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ 121
I Groupes cycliques . . . 122
I.1 Sous-groupe monogène . . . 122
I.2 Ordre d'un élément d'un groupe . . . 123
I.3 Éléments primitifs . . . 126
II Structure de $(\mathbb{Z}/p\mathbb{Z})^\times$ . . . 129
III Structure de $(\mathbb{Z}/p^r\mathbb{Z})^\times$ . . . 130
IV Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$ . . . 131
V L'indicateur de Carmichaël . . . 133
VI Réponses aux questions . . . 139
VII Exercices . . . 140

7 Résidus quadratiques 143
I Définition - Exemples . . . 143
II Résidus quadratiques dans $\mathbb{Z}/p\mathbb{Z}$ . . . 144
III Symbole de Legendre . . . 146
IV Calcul des racines carrées dans $\mathbb{Z}/p\mathbb{Z}$ . . . 156
IV.1 Cas où p est congru à 3 modulo 4 . . . 157
IV.2 Cas où p est congru à 1 modulo 4 . . . 159
V Carrés modulo un entier quelconque . . . 161
VI Nombre de racines carrées modulo n . . . 165
VII Entiers de Blum . . . 171
VIII Résidualité quadratique . . . 173
IX Réponses aux questions . . . 174
X Exercices . . . 176

III Cryptologie contemporaine 179

8 Schémas de Feistel - Standards de chiffrement par blocs 181
I Schémas de Feistel . . . 184
I.1 La construction . . . 185
I.2 Le résultat essentiel . . . 187
I.3 Avec une ou deux rondes seulement . . . 188
I.4 La preuve . . . 189
II Data Encryption Standard (DES) . . . 193
II.1 Construction . . . 193
II.2 La polémique . . . 197
III Advanced Encryption Standard (AES) . . . 199
III.1 AddRoundKey . . . 200

III.2 SubBytes . . . 200
III.3 ShiftRows . . . 203
III.4 MixColumns . . . 204
III.5 Fonctionnement . . . 204
IV Modes opératoires du chiffrement par bloc. . . . 205
IV.1 Le mode ECB (Electronic Codebook Mode) . . . 205
IV.2 Le mode CBC (Cipher Block Chaining Mode) . . . 206
IV.3 Le mode OFB (Output Feedback Mode) . . . 206
IV.4 Le mode CFM (Cypher Feedback Mode) . . . 207
V Réponses aux questions . . . 208

9 Cryptographie à clé publique 209
I Définitions et principes généraux . . . 211
I.1 Quelques notions de complexité . . . 211
I.2 Fonctions à sens unique . . . 214
I.3 Application . . . 216
II RSA . . . 216
II.1 Cryptage . . . 217
II.2 Décryptage . . . 218
II.3 Sécurité . . . 219
III Chiffrement de Rabin . . . 220
III.1 Cryptage . . . 220
III.2 Décryptage . . . 221
III.3 Sécurité . . . 222
IV Ordinateurs quantiques . . . 223
IV.1 Qubits . . . 223
IV.2 Cryptographie post-quantique . . . 224
V Le cryptosystème ElGamal . . . 225
V.1 Cryptage . . . 226
V.2 Décryptage . . . 226
V.3 Sécurité . . . 227
VI ElGamal généralisé . . . 228
VII Protocole d'échange de Clé de Diffie-Hellman . . . 229
VII.1 Description . . . 229
VII.2 Attaque . . . 230
VIII Cryptographie multivariable . . . 231
IX Tests de primalité . . . 232
IX.1 Test de pseudo-primalité . . . 233
IX.2 Test de Rabin-Miller . . . 234
X Exercices . . . 236

10 Signature - Identification - Blockchain **241**
I Procédés de signature . . . 241
II La signature RSA . . . 243
III Généralisation . . . 244
IV La signature ElGamal . . . 245
IV.1 Description . . . 245
IV.2 Sécurité . . . 246
V DSS . . . 247
VI Courbes elliptiques . . . 248
VI.1 Coefficients réels . . . 249
VI.2 Coefficients dans un corps fini . . . 252
VII ECDSA . . . 254
VIII Fonctions de hachage . . . 255
VIII.1 Principes généraux . . . 256
VIII.2 Le paradoxe des anniversaires . . . 258
VIII.3 Une fonction résistante aux collisions . . . 260
VIII.4 Petit historique . . . 261
IX Procédés d'identification « à clé privée » . . . 262
X Procédés d'identification « à clé publique » . . . 263
XI Procédé d'identification de Guillou-Quisquater . . . 264
XII Applications : sécurité des cartes bancaires . . . 265
XII.1 Structure d'une carte bancaire . . . 266
XII.2 Le rôle de la puce . . . 267
XII.3 Paiement en ligne . . . 268
XIII Blockchain . . . 269
XIII.1 Structure d'un bloc . . . 270
XIII.2 Sécurité décentralisée . . . 271
XIII.3 Perspectives . . . 273
XIV Réponses aux questions . . . 273
XV Exercices . . . 274

IV Solution des exercices **277**

Bibliographie . . . 319

Index . . . 321