

SCIENCES SUP

36283

Cours et exercices corrigés

Licence 3 • Master 1 • Écoles d'ingénieurs

INTRODUCTION À LA CRYPTOGRAPHIE

Johannes Buchmann

DUNOD

M629

36283

①

INTRODUCTION À LA CRYPTOGRAPHIE

Cours et exercices corrigés

Johannes Buchmann

professeur d'informatique et de mathématiques
à l'université de Darmstadt (Allemagne)

Traduit de l'anglais par
JACQUES VÉLU

professeur au CNAM de Paris



Table des matières

AVANT-PROPOS À LA DEUXIÈME ÉDITION	IX
AVANT-PROPOS	XI
CHAPITRE 1 • LES ENTIERS	
1.1 Résultats de base	1
1.2 Divisibilité	2
1.3 Représentation des entiers	3
1.4 Notations O et Ω	5
1.5 Coût de l'addition, la multiplication, la division avec reste	6
1.6 Algorithme polynomial	8
1.7 PGCD	8
1.8 Algorithme d'Euclide	10
1.9 Algorithme d'Euclide étendu	13
1.10 Analyse de l'algorithme d'Euclide étendu	14
1.11 Décomposition en facteurs premiers	18
Exercices	20

CHAPITRE 2 • CONGRUENCES ET CLASSES RÉSIDUELLES

2.1	Congruences	23
2.2	Semigroupe	25
2.3	Groupe	27
2.4	Anneau des classes résiduelles	28
2.5	Corps	28
2.6	Division dans l'anneau des classes résiduelles	29
2.7	Analyse des opérations dans l'anneau des classes résiduelles	30
2.8	Groupe multiplicatif des résidus mod m	31
2.9	Ordre d'un élément d'un groupe	33
2.10	Sous-groupe	34
2.11	Petit théorème de Fermat	36
2.12	Exponentiation rapide	36
2.13	Calcul rapide d'un produit de puissances	38
2.14	Calcul de l'ordre d'un élément	39
2.15	Théorème chinois des restes	40
2.16	Décomposition de l'anneau des classes résiduelles	43
2.17	Formule pour la fonction φ d'Euler	44
2.18	Polynômes	45
2.19	Polynômes sur les corps	47
2.20	Construction de corps finis	49
2.21	Groupe des unités d'un corps fini	51
2.22	Structure du groupe $(\mathbb{Z}/p\mathbb{Z})^*$	52
	Exercices	53

CHAPITRE 3 • CHIFFREMENT

3.1	Système de chiffrement	56
3.2	Cryptosystème symétrique ou asymétrique	58
3.3	Cryptanalyse	58
3.4	Alphabet et mots	61
3.5	Permutations	63
3.6	Chiffrement par bloc	65
3.7	Chiffrement répété	66
3.8	Utilisation du chiffrement par bloc	66
3.9	Algorithme de chiffrement en continu	74
3.10	Chiffrement affine	76
3.11	Matrices et applications linéaires	77
3.12	Chiffrement affine ou linéaire par bloc	82
3.13	Chiffres de Vigenère, de Hill, et chiffrement par permutation	82
3.14	Cryptanalyse des chiffrements affines par bloc	83
3.15	Cryptosystèmes	84
	Exercices	89

CHAPITRE 4 • PROBABILITÉS ET SECRET PARFAIT

4.1	Probabilités	93
4.2	Probabilités conditionnelles	94
4.3	Paradoxe des anniversaires	95
4.4	Secret parfait	96
4.5	Technique du masque jetable	99
4.6	Nombres aléatoires	100
4.7	Nombres pseudo-aléatoires	101
	Exercices	101

CHAPITRE 5 • DES

5.1	Chiffres de Feistel	103
5.2	Algorithme du DES	104
5.3	Un exemple	109
5.4	Sécurité du DES	111
	Exercices	111

CHAPITRE 6 • AES

6.1	Notations	113
6.2	Algorithme Cipher	114
6.3	Algorithme KeyExpansion	118
6.4	Un exemple	119
6.5	Fonction InvCipher	120
	Exercices	121

CHAPITRE 7 • FABRICATION DE NOMBRES PREMIERS

7.1	Essai par division	122
7.2	Test de Fermat	124
7.3	Nombres de Carmichael	125
7.4	Test de Miller-Rabin	126
7.5	Nombres premiers aléatoires	128
	Exercices	129

CHAPITRE 8 • CHIFFREMENT À CLÉS PUBLIQUES

8.1	L'idée	130
8.2	Sécurité	132
8.3	RSA	133
8.4	Chiffrement de Rabin	144
8.5	Échange de clés selon Diffie-Hellman	147
8.6	Chiffrement ElGamal	151
	Exercices	155

CHAPITRE 9 • FACTORISATION

9.1	L'idée	158
9.2	Méthode $p - 1$	159
9.3	Crible quadratique	159
9.4	Analyse du crible quadratique	164
9.5	Efficacité d'autres algorithmes de factorisation	167
	Exercices	168

CHAPITRE 10 • LOGARITHMES DISCRETS

10.1	Problème DL	169
10.2	Énumération	170
10.3	Algorithme pas de bébé/pas de géant de Shanks	170
10.4	Algorithme ρ de Pollard	172
10.5	Algorithme de Pohlig-Hellman	176
10.6	Calcul d'indice	179
10.7	Autre algorithmes	183
10.8	Généralisation de l'algorithme de calcul d'indice	183
	Exercices	184

CHAPITRE 11 • FONCTIONS CRYPTOGRAPHIQUES DE HACHAGE

11.1	Fonctions de hachage et de compression	185
11.2	Attaque des anniversaires	187
11.3	Fonctions de compression à partir des fonctions de chiffrement	188
11.4	Fonctions de hachage à partir des fonctions de compression	189
11.5	SHA-1	191
11.6	Autres fonctions de hachage	193
11.7	Une fonction de compression arithmétique	193
11.8	Codes d'authentification de message	195
	Exercices	195

CHAPITRE 12 • SIGNATURE DIGITALE

12.1	Idée	197
12.2	Sécurité	198
12.3	Signatures RSA	199
12.4	Signer au moyen d'un système à clés publiques	203
12.5	Signature ElGamal	203
12.6	DSA	207
12.7	Signature indéniable	209
12.8	Signature en aveugle	213
	Exercices	215

CHAPITRE 13 • AUTRES SYSTÈMES

13.1 Corps finis	217
13.2 Courbes elliptiques	218
13.3 Formes quadratiques	221
Exercices	221

CHAPITRE 14 • IDENTIFICATION

14.1 Mot de passe	223
14.2 Mot de passe à usage unique	223
14.3 Identification par défi-réponse	224
Exercices	227

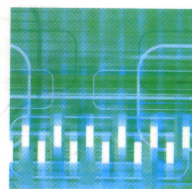
CHAPITRE 15 • PARTAGE DE SECRET

15.1 Le principe	229
15.2 Protocole de partage de secret de Shamir	230
Exercices	232

CHAPITRE 16 • INFRASTRUCTURE DE CLÉS PUBLIQUES

16.1 Environnement de sécurité personnelle	233
16.2 Autorité de certification	235
16.3 Certification en chaîne	238

SOLUTION DES EXERCICES 240**RÉFÉRENCES BIBLIOGRAPHIQUES** 256**INDEX** 257



Johannes Buchmann

Traduit de l'anglais par Jacques Vélu

INTRODUCTION À LA CRYPTOGRAPHIE

Les techniques de cryptographie présentent de nombreux usages. De la signature des documents électroniques à la protection du copyright, elles permettent d'assurer la confidentialité, l'accès et l'identification des documents.

Ce livre présente, sans formalisme mathématique excessif, les outils mathématiques et algorithmiques utiles à la compréhension de la cryptographie. Le cours est complété par des exercices simples dont la moitié trouvent leurs corrigés en fin d'ouvrage.

Ce manuel s'adresse aux étudiants en Licence 3 ou Master 1 de mathématiques appliquées ou d'informatique ainsi qu'aux élèves ingénieurs.

JOHANNES BUCHMANN est professeur d'informatique et de mathématiques à l'université de Darmstadt (Allemagne).

JACQUES VÉLU est professeur au CNAM de Paris.

