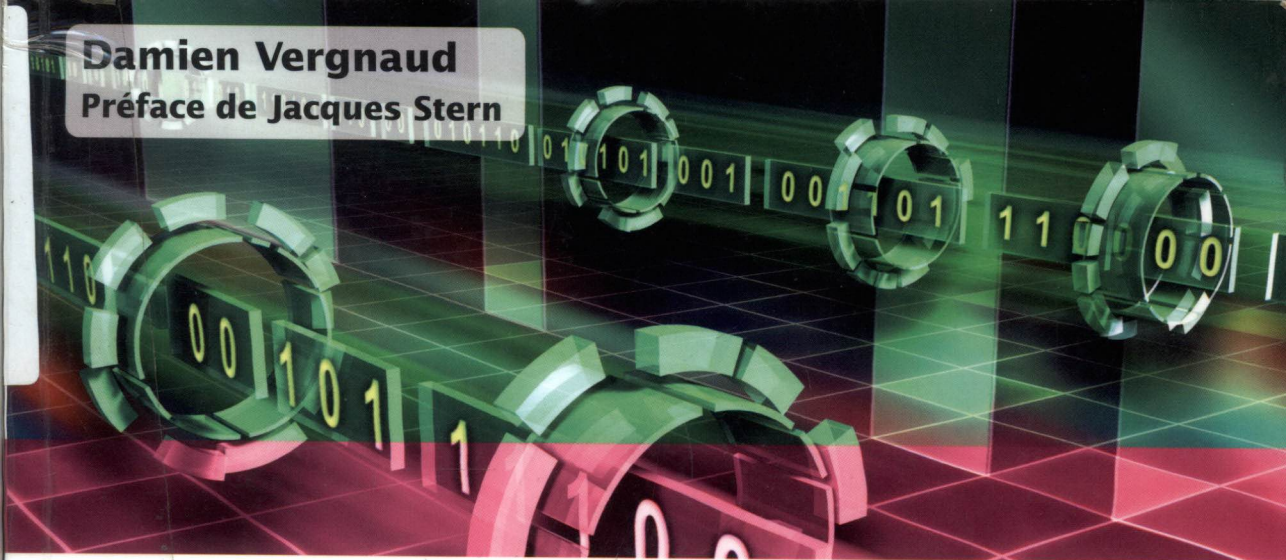


Damien Vergnaud
Préface de Jacques Stern



Exercices et problèmes de cryptographie

Licence
Master
Écoles d'ingénieurs



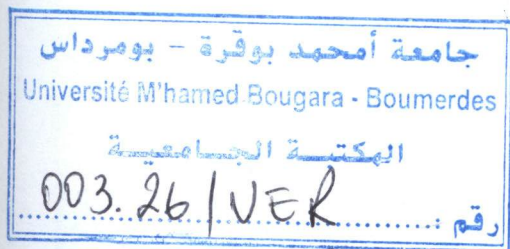
DUNOD

Damien Vergnaud

Préface de Jacques Stern



Exercices et problèmes de cryptographie



leaf.



DUNOD

TABLE DES MATIÈRES

Chapitre 1. Cryptographie classique	1
1.1 Chiffrement par substitution mono-alphabétique	1
Exercice 1.1 (avec programmation). Chiffrement de César	3
Exercice 1.2 (avec programmation). Chiffrement affine	4
Exercice 1.3 (avec programmation). Chiffrement par substitution mono-alphabétique	5
1.2 Chiffrement par substitution poly-alphabétique	11
Exercice 1.4 (avec programmation). Chiffrement de Vigenère – test de Kasiski	12
Exercice 1.5 (avec programmation). Chiffrement de Vigenère – indice de coïncidence	13
Exercice 1.6. Chiffrement de Hill – nombre de clés	15
Exercice 1.7. Chiffrement de Hill – attaque à clair connu	16
1.3 Chiffrement par transposition	17
Exercice 1.8 (avec programmation). Scytale	17
Exercice 1.9 (avec programmation). Chiffrement par transposition par colonnes	19
1.4 Chiffrement parfait	20
Exercice 1.10. Carré latin	20
Exercice 1.11 (avec programmation). Mauvaise utilisation du chiffrement jetable	22
Problème 1.12. Algorithme de Viterbi	23
1.5 La machine Enigma	25
Exercice 1.13. Enigma – Nombre de clés	27
Exercice 1.14 (avec programmation). Enigma – Tableau de connexions	28
Problème 1.15. Enigma – Indice de coïncidence	29
Chapitre 2. Chiffrement par bloc – Modes opératoires, DES et AES	33
2.1 Modes opératoires	34
Exercice 2.1. Modes opératoires et propriétés de sécurité	36
Exercice 2.2. Mode opératoire CBC *	38
Exercice 2.3. Attaque sur le mode CBC avec le processus de bourrage RFC2040	40
2.2 Schémas de Feistel	41
Exercice 2.4. Schéma de FEISTEL à un ou deux tours	42
Exercice 2.5. Sécurité du schéma de FEISTEL à trois tours	43
Exercice 2.6. Distingueur pour le schéma de FEISTEL à trois tours *	45
2.3 Chiffrement DES	46
Exercice 2.7. Clés faibles et semi-faibles du chiffrement DES	47
Exercice 2.8. Propriété de complémentation du chiffrement DES	49
Exercice 2.9. Chiffrement DES avec blanchiment	50
Exercice 2.10. Construction de Even-Mansour	51
Exercice 2.11. Double chiffrement	52
Exercice 2.12. Chiffrement Triple-DES avec deux clés indépendantes	53
Exercice 2.13. Mode opératoire CBC-CBC-ECB	54
2.4 Chiffrement AES	56
Exercice 2.14 (avec programmation). S-Boîte de l'AES	58
Exercice 2.15 (avec programmation). Opération MixColumns	60
Exercice 2.16. Propriétés de l'opération MixColumns	62
Exercice 2.17 (avec programmation). Diversification de clé de l'AES	63
2.5 Fonctions de hachage cryptographiques	65
Exercice 2.18. Chiffrement par bloc et fonction de compression	67
Exercice 2.19. Sécurité de la construction de Matyas-Meyer-Oseas avec le DES	68
Exercice 2.20. Attaque en pré-image pour une fonction de hachage itérée *	69

Exercices et problèmes de cryptographie

Chapitre 3. Chiffrement par bloc – Techniques avancées de cryptanalyse	71
3.1 Cryptanalyse différentielle	72
Exercice 3.1 (avec programmation). Table des différences du DES	73
Problème 3.2. Cryptanalyse différentielle de FEAL-4 *	75
3.2 Cryptanalyse différentielle impossible	79
Exercice 3.3. Attaque par différentielle impossible contre DEAL	80
Problème 3.4. Attaque par différentielle impossible contre l'AES *	82
3.3 Cryptanalyse linéaire	86
Exercice 3.5 (avec programmation). Table d'approximation linéaire du DES	86
Exercice 3.6. Approximation linéaire de l'addition	88
Problème 3.7. Cryptanalyse linéaire de SAFER *	91
Exercice 3.8. Biais de la parité d'une permutation	93
3.4 Attaques par décalage	94
Problème 3.9. Attaque par décalage sur TREYFER	95
Exercice 3.10. Attaque par décalage sur 2K-DES	97
3.5 Attaques par saturation	98
Problème 3.11. Attaque par saturation contre l'AES *	98
3.6 Attaques par distingueurs <i>ad hoc</i>	101
Exercice 3.12. Attaque par distiguteur sur Magenta	101
Exercice 3.13. Attaque par distiguteur sur Ladder-DES	103
Exercice 3.14. Distingueur pour le chiffrement M6	104
3.7 Attaques génériques sur les fonctions de hachage itérées	106
Exercice 3.15. Multi-collisions pour les fonctions de hachage itérées	106
Exercice 3.16. Attaque en collision contre fonctions de hachage concaténées	108
Problème 3.17. Attaque de Kelsey-Schneier	109
Chapitre 4. Chiffrement par flot	113
4.1 Registres à décalage à rétroaction linéaire	113
Exercice 4.1. LFSR et polynômes de rétroaction	115
Exercice 4.2. Propriétés statistiques d'une suite produite par un LFSR	116
Exercice 4.3. Reconstruction du polynôme de rétroaction minimal	117
4.2 Chiffrement par flot par registres à décalage irrégulier	118
Exercice 4.4 (avec programmation). Distingueur sur le générateur à signal d'arrêt	119
Problème 4.5. Propriétés du générateur par auto-rétrécissement	121
4.3 Chiffrement par flot par registre filtré	122
Exercice 4.6. Attaque « deviner et déterminer » sur Toyocrypt	123
Exercice 4.7. Attaque algébrique sur Toyocrypt *	124
4.4 Chiffrement par flot par registres combinés	126
Exercice 4.8. Attaque par corrélation sur le générateur de Geffe	127
Exercice 4.9. Attaque « deviner et déterminer » sur le générateur de Geffe	128
Exercice 4.10. Attaque algébrique sur le générateur de Geffe	129
4.5 Le chiffrement par flot A5/1	130
Exercice 4.11. États internes de A5/1	131
Exercice 4.12. Attaque par compromis temps-mémoire sur A5/1	133
Problème 4.13. Attaque « deviner et déterminer » sur A5/1	134
4.6 Le chiffrement par flot RC4	136
Exercice 4.14. Cryptanalyse de RC4 sans opération d'échange *	137
Exercice 4.15. Biais de la suite chiffrante produite par RC4	139
Problème 4.16. Attaque par recouvrement de clé sur RC4	141

Chapitre 5. Problème du logarithme discret	145
5.1 Logarithme discret dans un groupe générique	145
Exercice 5.1. Multi-exponentiation	147
Exercice 5.2. Algorithme de Shanks	148
Exercice 5.3. Algorithme ρ de Pollard	150
Exercice 5.4. Algorithme de Pohlig-Hellman	153
Exercice 5.5 (avec programmation). Application de l'algorithme de Pohlig-Hellman	155
5.2 Problème du logarithme discret dans $\mathbb{Z}_p^*$	156
Exercice 5.6. Entiers friables	157
Problème 5.7. Méthode de Kraitchik – Calcul d'indice *	159
5.3 Problèmes algorithmiques liés au logarithme discret	163
Exercice 5.8. Auto-réductibilité du problème du logarithme discret	163
Exercice 5.9. Algorithme λ de Pollard	165
Problème 5.10. Logarithme discret de petit poids de Hamming	168
Exercice 5.11. Logarithme discret avec information partielle	171
5.4 Interpolation polynomiale de logarithme discret	172
Exercice 5.12. Polynôme d'interpolation du logarithme discret	173
Exercice 5.13. Interpolation polynomiale de logarithme discret – Borne inférieure	174
Exercice 5.14. Interpolation polynomiale de logarithme discret en moyenne *	176
Chapitre 6. Factorisation des entiers et primalité	179
6.1 Tests de primalité	179
Exercice 6.1. Certificats de primalité de Pratt	180
Exercice 6.2. Nombre pseudo-premier de Fermat en base a	181
Problème 6.3. Nombres de Carmichael – Critère de Korselt	182
Exercice 6.4 (avec programmation). Recherche de nombres de Carmichael	183
Problème 6.5. Test de primalité de Solovay-Strassen	186
Problème 6.6. Test de primalité de Miller-Rabin	189
Exercice 6.7. Identité de Agrawal-Kayal-Saxena	191
Exercice 6.8. Nombres de Fermat et test de primalité de Pépin	193
Problème 6.9. Nombres de Mersenne et test de Lucas-Lehmer *	194
6.2 Méthodes exponentielles de factorisation	197
Exercice 6.10 (avec programmation). Factorisation par divisions successives	197
Exercice 6.11 (avec programmation). Factorisation par la méthode Fermat	198
Exercice 6.12. Algorithme de Lehman *	199
Exercice 6.13. Méthode $p-1$ de Pollard	201
Exercice 6.14 (avec programmation). Factorisation par la méthode $p-1$ de Pollard	203
Exercice 6.15. Algorithme ρ de Pollard	204
6.3 Multi-évaluation de polynômes et algorithme de Pollard-Strassen	205
Exercice 6.16. Division euclidienne rapide par la méthode de Newton	205
Exercice 6.17. Multi-évaluation d'un polynôme univarié	208
Exercice 6.18. Algorithme de Pollard-Strassen	210
6.4 Racine carrée modulaire et factorisation	211
Exercice 6.19. Extraction de racine carrée modulo p	211
Exercice 6.20. Extraction de racine carrée modulo p^f	213
Exercice 6.21. Extraction de racine carrée modulo N	214
Problème 6.22. Carrés modulaires friables	216
Exercice 6.23. Factorisation et logarithme discret	220

Exercices et problèmes de cryptographie

Chapitre 7. Chiffrement à clé publique	223
7.1 Fonction RSA	223
Exercice 7.1. Fonction RSA et factorisation	224
Exercice 7.2. Auto-réductibilité du problème RSA	225
Problème 7.3. Sécurité des bits de la fonction RSA	227
7.2 Chiffrement RSA	228
Exercice 7.4. Sécurité du protocole de chiffrement RSA naïf	230
Exercice 7.5. RSA avec module commun	230
Exercice 7.6 (avec programmation). Diffusion de données chiffrées avec RSA	231
Exercice 7.7. Attaque de Wiener	233
Exercice 7.8 (avec programmation). Attaque de Wiener	234
Exercice 7.9 (avec programmation). RSA et clairs liés	236
Exercice 7.10. RSA et petits textes clairs	237
Problème 7.11. Implantation du chiffrement RSA et théorème des restes chinois	238
7.3 Mise en accord de clé de Diffie-Hellman	239
Exercice 7.12. Attaque par le milieu	240
Problème 7.13. Logarithme discret et Diffie-Hellman *	241
7.4 Chiffrement d'ElGamal et variantes	244
Exercice 7.14. Sécurité du chiffrement d'ElGamal naïf	244
Exercice 7.15. Sécurité des bits du logarithme discret	246
Exercice 7.16. Attaque ElGamal par petit sous-groupe	248
Chapitre 8. Signatures numériques	251
8.1 Signatures basées sur la primitive RSA	251
Exercice 8.1. Sécurité du protocole de signature RSA naïf	252
Exercice 8.2. Sécurité des protocoles de signature de De Jonge et Chaum	253
Exercice 8.3. Sécurité de $\mathcal{F}$ -RSA et propriétés de $\mathcal{F}$	255
Exercice 8.4. Sécurité de $\mathcal{F}$ -RSA pour la recommandation CCITT	257
Exercice 8.5. Sécurité de $\mathcal{F}$ -RSA avec encodage PKCS #1 v1.5	259
Exercice 8.6. Contrefaçon existentielle de $\mathcal{F}$ -RSA avec redondance linéaire	262
Exercice 8.7. Contrefaçon universelle de $\mathcal{F}$ -RSA avec redondance linéaire *	263
Problème 8.8. Sécurité du protocole de signature de Boyd	264
8.2 Signatures d'ElGamal et variantes	268
Exercice 8.9. Contrefaçon existentielle du schéma de signature d'ElGamal naïf	268
Exercice 8.10. Contrefaçon universelle du schéma de signature d'ElGamal naïf	269
Exercice 8.11. Vérification des signatures d'ElGamal	270
Exercice 8.12. Fonction de hachage et sécurité des signatures de Schnorr	271
Exercice 8.13 (avec programmation). Paramètres publics dans le protocole DSA	272
Exercice 8.14. Clé temporaire et sécurité des signatures d'ElGamal	273
8.3 Signatures de Lamport et variantes	275
Exercice 8.15. Sécurité et efficacité des signatures de Lamport	275
Exercice 8.16. Espace de message de la signature de Lamport	276
Exercice 8.17. Extension de l'espace des messages des signatures de Lamport *	277
Exercice 8.18. Arbres de Merkle	279
Problème 8.19. Sécurité du protocole de signature de Groth	281
Bibliographie	285
Index	291

Damien Vergnaud
Préface de Jacques Stern

Exercices et problèmes de cryptographie

Cet ouvrage s'adresse aux étudiants de second cycle d'informatique ou de mathématiques ainsi qu'aux élèves en écoles d'ingénieurs.

La **cryptographie** 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**.

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 3^e année.

Cet ouvrage présente les **outils mathématiques et algorithmiques** utiles en cryptographie et les **fonctionnalités cryptographiques de base** (le chiffrement, la signature et l'authentification) dans le cadre de la cryptographie symétrique et asymétrique. Il propose plus d'une **centaine d'exercices et problèmes** qui sont entièrement corrigés et précédés de rappels de cours.

Damien Vergnaud

est maître de conférences en informatique à l'École normale supérieure. Depuis 2008, il intervient également dans le cours d'initiation à la cryptologie au MPRI (Master parisien de recherche en informatique).



L'ouvrage propose de nombreux **exercices de programmation**. Les données numériques ainsi que des exercices supplémentaires et des références complémentaires sont disponibles en ligne sur www.dunod.com, sur la page dédiée à l'ouvrage.



6950760
ISBN 978-2-10-057340-0

