

Douglas Stinson

Cryptographie

Théorie et pratique

*Traduction de Serge Vaudenay,
Gildas Avoine et Pascal Junod*



Vuibert Informatique

Cryptographie

BIBLIOTHEQUE DU CERIST

L'édition originale de ce livre a été publiée aux États-Unis par CRC Press, Inc., 2000 Corporate Blvd., N.W. Boca Raton, Florida 33431, sous le titre :

Cryptography – Theory and Practice

© CRC Press, Inc., 2002

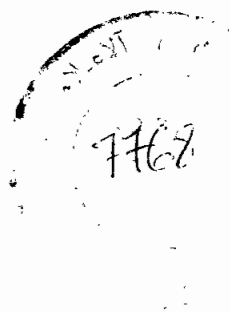
© Vuibert, Paris, 2003

ISBN 2-7117-4800-6

Contact : informatique@vuibert.fr

Web : www.vuibert.fr

Conception de la couverture : Jean Widmer



Les programmes et exemples figurant dans ce livre ont pour but d'illustrer les sujets traités. Il n'est donné aucune garantie quant à leur utilisation dans le cadre d'une activité professionnelle ou commerciale.

Toute représentation ou reproduction intégrale ou partielle, faite sans le consentement de l'auteur, ou de ses ayants droit, ou ayants cause, est illicite (loi du 11 mars 1957, alinéa 1^{er} de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée par les articles 425 et suivants du Code pénal. La loi du 11 mars 1957 n'autorise, aux termes des alinéas 2 et 3 de l'article 41, que les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective d'une part et d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration.

À mes enfants, Michela et Aiden

BIBLIOTHEQUE DU CERIST

Table des matières

1	Cryptographie classique	1
1.1	Introduction : quelques systèmes simples	1
1.1.1	Chiffrement par décalage	3
1.1.2	Chiffrement par substitution	6
1.1.3	Chiffrement affine	8
1.1.4	Chiffrement de Vigenère	12
1.1.5	Chiffrement de Hill	13
1.1.6	Chiffrement par permutation	18
1.1.7	Chiffrement en chaîne	20
1.2	Cryptanalyse	24
1.2.1	Cryptanalyse du chiffrement affine	25
1.2.2	Cryptanalyse du chiffrement par substitution	27
1.2.3	Cryptanalyse du chiffrement de Vigenère	30
1.2.4	Cryptanalyse du chiffrement de Hill	34
1.2.5	Cryptanalyse d'un chiffrement en chaîne	35
1.3	Notes et références	37
	Exercices	37
2	Théorie de Shannon	44
2.1	Introduction	44
2.2	Notions élémentaires de théorie des probabilités	45
2.3	Secret parfait	47
2.4	Entropie	52
2.4.1	Codage de Huffman et entropie	54
2.5	Propriétés de l'entropie	57
2.6	Clefs parasites et distance d'unicité	60
2.7	Système cryptographique produit	65
2.8	Notes et références	68
	Exercices	68

3	Chiffrement par bloc et AES	71
3.1	Introduction	71
3.2	Réseaux de substitution-permutation	72
3.3	Cryptanalyse linéaire	77
3.3.1	Lemme d'empilement	78
3.3.2	Approximations linéaires de S-boîtes	80
3.3.3	Cryptanalyse linéaire d'un SPN	82
3.4	Cryptanalyse différentielle	87
3.5	<i>Data Encryption Standard</i> (DES)	93
3.5.1	Description de DES	93
3.5.2	Analyse de DES	98
3.6	<i>Advanced Encryption Standard</i> (AES)	100
3.6.1	Description d'AES	101
3.6.2	Analyse d'AES	106
3.7	Modes opératoires	107
3.8	Notes et références	110
	Exercices	111
4	Fonctions de hachage cryptographiques	115
4.1	Fonctions de hachage et intégrité des données	115
4.2	Sécurité des fonctions de hachage	117
4.2.1	Modèle de l'oracle aléatoire	118
4.2.2	Algorithmes dans le modèle de l'oracle aléatoire	119
4.2.3	Comparaison de critères de sécurité	123
4.3	Fonctions de hachage itérées	126
4.3.1	Construction de Merkle-Damgård	127
4.3.2	SHA-1	132
4.4	Codes d'authentification de messages	135
4.4.1	MAC emboîtés et HMAC	137
4.4.2	CBC-MAC	139
4.5	MAC inconditionnellement sûrs	141
4.5.1	Fonctions de hachage fortement universelles	144
4.5.2	Optimalité de probabilités de tromperie	146
4.6	Notes et références	148
	Exercices	149
5	Chiffrement RSA et factorisation d'entiers	155
5.1	Introduction à la cryptographie à clef publique	155
5.2	Compléments de théorie des nombres	157
5.2.1	Algorithme d'Euclide	157
5.2.2	Théorème des restes chinois	162
5.2.3	Autres résultats utiles	164
5.3	Chiffrement RSA	166
5.3.1	Implémentation de RSA	168

5.4	Tests de primalité	171
5.5	Racines carrées modulo n	180
5.6	Algorithmes de factorisation	181
5.6.1	Méthode $p - 1$ de Pollard	182
5.6.2	Méthode rho de Pollard	183
5.6.3	Algorithme de Dixon	186
5.6.4	Algorithmes de factorisation en pratique	191
5.7	Autres attaques de RSA	193
5.7.1	Calculer $\phi(n)$	193
5.7.2	Exposant de déchiffrement	193
5.7.3	Attaque de Wiener	198
5.8	Chiffrement de Rabin	202
5.8.1	Sécurité du chiffrement de Rabin	204
5.9	Sécurité sémantique de RSA	206
5.9.1	Information partielle sur le texte clair	207
5.9.2	OAEP	209
5.10	Notes et références	216
	Exercices	217
6	Systèmes à clef publique fondés sur le logarithme discret	224
6.1	Chiffrement d'ElGamal	224
6.2	Algorithmes pour le calcul du logarithme discret	226
6.2.1	Algorithme de Shanks	227
6.2.2	Méthode rho de Pollard pour le logarithme discret	229
6.2.3	Algorithme de Pohlig-Hellman	231
6.2.4	Méthode du calcul d'indice	235
6.3	Complexité des algorithmes génériques	237
6.4	Corps finis	241
6.5	Courbes elliptiques	245
6.5.1	Courbes elliptiques sur le corps des réels	245
6.5.2	Courbes elliptiques modulo un nombre premier	248
6.5.3	Propriétés des courbes elliptiques	251
6.5.4	ECIES	252
6.5.5	Calcul de multiples de point	255
6.6	Algorithmes pour le logarithme discret en pratique	257
6.7	Sécurité des systèmes du type ElGamal	258
6.7.1	Sécurité des bits du logarithme discret	258
6.7.2	Sécurité sémantique	262
6.7.3	Problèmes de Diffie-Hellman	263
6.8	Notes et références	265
	Exercices	265

7 Schémas de signature	271
7.1 Introduction	271
7.2 Sécurité des schémas de signature	274
7.2.1 Signatures et fonctions de hachage	276
7.3 Schéma de signature d'ElGamal	277
7.3.1 Sécurité du schéma de signature d'ElGamal	279
7.4 Variantes du schéma de signature d'ElGamal	283
7.4.1 Signature de Schnorr	283
7.4.2 DSA (<i>Digital Signature Algorithm</i>)	285
7.4.3 ECDSA	287
7.5 Schéma de signature prouvé sûr	289
7.5.1 Signatures jetables	289
7.5.2 FDH	294
7.6 Signatures incontestables	297
7.7 Signatures sans échec	302
7.8 Notes et références	307
Exercices	307
Lectures complémentaires	312
Bibliographie	314
Index des systèmes cryptographiques	328
Index des algorithmes	329
Index des problèmes	330
Index	331