

# CRYPTOGRAPHIE

Théorie et pratique

2<sup>e</sup> édition

Douglas Stinson

Traduction de Serge Vaudenay, Gildas Avoine et Pascal Junod



F2010/4BD  
N° 04

~~BHAB.~~

Douglas Stinson

M 495

047944

(3)

# Cryptographie

Théorie et pratique



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



Vuibert Informatique

# Table des matières

<b>1</b>	<b>Cryptographie classique</b>	<b>1</b>
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
<b>2</b>	<b>Théorie de Shannon</b>	<b>44</b>
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

<b>3</b>	<b>Chiffrement par bloc et AES</b>	<b>71</b>
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
<b>4</b>	<b>Fonctions de hachage cryptographiques</b>	<b>115</b>
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
<b>5</b>	<b>Chiffrement RSA et factorisation d'entiers</b>	<b>155</b>
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
<b>6</b>	<b>Systèmes à clef publique fondés sur le logarithme discret</b>	<b>224</b>
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 de 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

<b>7 Schémas de signature</b>	<b>271</b>
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
<b>Lectures complémentaires</b>	<b>312</b>
<b>Bibliographie</b>	<b>314</b>
<b>Index des systèmes cryptographiques</b>	<b>328</b>
<b>Index des algorithmes</b>	<b>329</b>
<b>Index des problèmes</b>	<b>330</b>
<b>Index</b>	<b>331</b>

*Cryptographie – Théorie et pratique* est un ouvrage de référence, universellement traduit et apprécié. Il offre une présentation lisible, et sous forme mathématique précise, des thèmes majeurs de la cryptographie. Il aborde tous les sujets de recherche contemporains, donnant au lecteur introduction et étude des résultats fondamentaux.

La plupart des algorithmes sont présentés sous forme de pseudo-programmes avec des exemples et une présentation informelle des idées sous-jacentes. Cet ouvrage donne une étude méthodique et compréhensible de tous les sujets essentiels en cryptologie : cryptographie à clef secrète, standard de chiffrement, systèmes à clef publique.

Cette deuxième édition prend en compte les avancées techniques de ces cinq dernières années. De nombreux nouveaux sujets ont ainsi été introduits et une mise à jour

approfondie de ceux traités dans la première édition a été menée. La nouvelle édition aborde les sujets suivants :

- les plus récents standards FIPS (*Federal Information Processing Standards*) : AES (*Advanced Encryption Standard*), SHA-1 (*Secure Hash Algorithm*), ECDSA (*Elliptic Curve Digital Signature Algorithm*) ;
- l'utilisation de réseaux de substitution-permutation pour le chiffrement par blocs et les concepts d'analyse ;
- les cryptanalyses linéaire et différentielle ; le modèle de l'oracle aléatoire pour les fonctions de hachage ;
- la sécurité sémantique de RSA et OAEP (*Optional Asymmetric Encryption Padding*) ;
- l'attaque de Wiener sur les exposants RSA.

Toutes ses qualités demeurent : explications claires et précises, rigueur mathématique, description en pseudo-code des algorithmes, nombreux exemples.

#### L'auteur

**Douglas Stinson**, docteur en informatique, est professeur à la faculté de mathématiques de l'université de Waterloo (Ontario). Il a été directeur de la publication du *Journal of Cryptology* et est également membre du comité éditorial de quatre autres journaux. Il a publié de nombreux articles dans les domaines de la cryptographie, de la combinatoire et de l'informatique théorique. Il a obtenu en 1994 la médaille Hall de l'Institute of Combinatorics and Its Applications.

#### Les traducteurs

**Serge Vaudenay**, ancien élève de l'École normale supérieure de la rue d'Ulm, est titulaire d'un doctorat en informatique obtenu à l'université de Paris VII. Chercheur au CNRS puis professeur à l'EPFL de Lausanne où il dirige le Laboratoire en sécurité et cryptographie (LASEC), ses recherches concernent principalement la sécurité des algorithmes cryptographiques.

**Gildas Avoine** est titulaire d'un DEA en informatique (intelligence artificielle et algorithmes) et diplômé de l'EPFL (systèmes de communication). **Pascal Junod** est diplômé du Swiss Institute of Technology de Zurich. Ils sont tous deux assistants au LASEC.

