

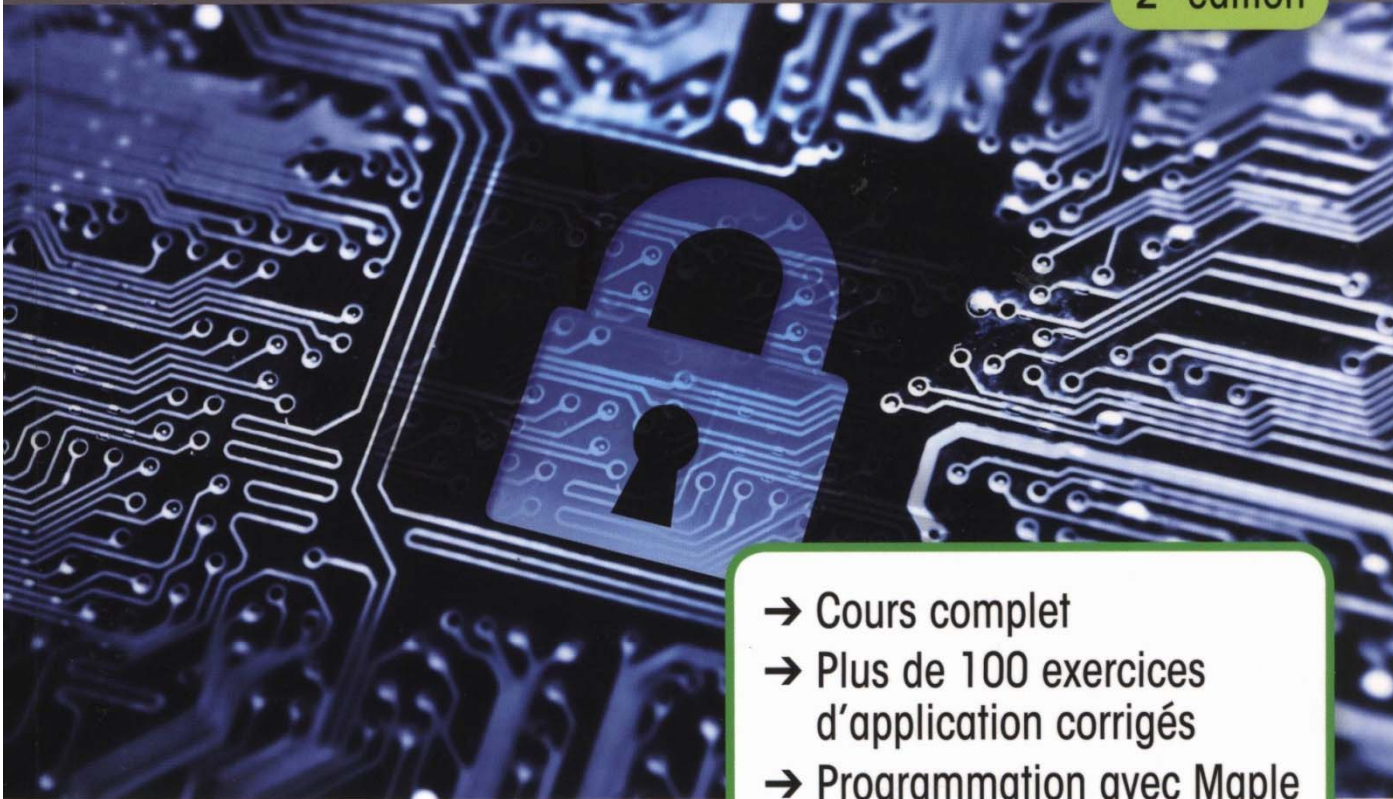
**INFORMATIQUE**

Gilles Dubertret

BTS – DUT – LICENCE  
MATHÉMATIQUES ET INFORMATIQUE

# INITIATION À LA CRYPTOGRAPHIE

2<sup>e</sup> édition

- 
- Cours complet
  - Plus de 100 exercices d'application corrigés
  - Programmation avec Maple

**Vuibert**

# Table des matières

<b>Introduction</b>	<b>xi</b>
<b>1 Les nombres premiers</b>	<b>1</b>
1.1 Nombres premiers . . . . .	1
1.2 Crible d'Ératosthène . . . . .	2
1.3 Facteurs premiers . . . . .	3
1.4 Complexité, liste des nombres premiers, spirale d'Ulam . . . . .	4
1.4.1 Notion de complexité algorithmique . . . . .	4
1.4.2 Liste des nombres premiers . . . . .	7
1.4.3 La spirale d'Ulam . . . . .	7
1.5 Décomposition en facteurs premiers . . . . .	9
1.6 Exercices . . . . .	9
<b>2 Éléments d'arithmétique</b>	<b>13</b>
2.1 Congruences dans $\mathbb{Z}$ . . . . .	13
2.1.1 Introduction . . . . .	13
2.1.2 Congruence . . . . .	15
2.1.3 Ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ . . . . .	17
2.1.4 Structure algébrique de $\mathbb{Z}/n\mathbb{Z}$ . . . . .	17
2.1.5 Groupe, anneau et corps . . . . .	18
2.1.6 Relation d'équivalence . . . . .	19
2.2 Cryptographie : César, Vigenère, permutation (Programmation) . . . . .	20
2.2.1 Système de cryptographie de César . . . . .	20
2.2.2 Système cryptographique de Vigenère . . . . .	22
2.2.3 Permutations alphabétiques . . . . .	23
2.3 Divisibilité dans $\mathbb{Z}$ . . . . .	24
2.3.1 Idéal des multiples de $a : (a)$ . . . . .	24
2.3.2 Divisibilité et idéaux de $\mathbb{Z}$ . . . . .	25
2.3.3 PPCM . . . . .	25
2.3.4 PGCD . . . . .	25
2.3.5 Le Théorème de Gauss . . . . .	27
2.4 PGCD, PPCM et Maple (Programmation) . . . . .	29
2.5 Retour aux nombres premiers . . . . .	30
2.6 Exercices . . . . .	31
2.7 Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ . . . . .	35

2.7.1	Indicateur d'Euler . . . . .	35
2.7.2	Petit Théorème de Fermat . . . . .	37
2.8	Applications et pratique . . . . .	37
2.8.1	Cryptographie et algèbre linéaire . . . . .	37
2.8.2	Calcul de $a^x \bmod n$ et le théorème de Fermat . . . . .	38
2.8.3	Test de non primalité . . . . .	39
2.8.4	Calcul de $a^x$ « à la main ». Notion de cycle . . . . .	39
<b>3</b>	<b>L'algorithme d'Euclide étendu</b> . . . . .	<b>41</b>
3.1	Présentation de l'algorithme . . . . .	41
3.2	Euclide étendu, inverse de $a$ dans $\mathbb{Z}/n\mathbb{Z}$ (Programmation) . . . . .	43
3.2.1	Euclide étendu . . . . .	43
3.2.2	Inverse de $a$ dans $\mathbb{Z}/n\mathbb{Z}$ . . . . .	43
3.3	Exercices . . . . .	44
<b>4</b>	<b>Le logarithme discret</b> . . . . .	<b>47</b>
4.1	Racine primitive . . . . .	47
4.2	Critère de primalité de Lehmer . . . . .	48
4.3	Racine primitive, grands nombres premiers (Programmation) . . . . .	49
4.3.1	Recherche de racine primitive . . . . .	49
4.3.2	Recherche de grands nombres premiers . . . . .	50
<b>5</b>	<b>Cryptosystèmes</b> . . . . .	<b>53</b>
5.1	Exemples de cryptosystèmes classiques . . . . .	54
5.1.1	Trois exemples . . . . .	54
5.1.2	N-gramme substitution . . . . .	54
5.1.3	Permutation d'ordre $d$ . . . . .	54
5.1.4	Playfair Cipher . . . . .	55
5.1.5	Transformation linéaire . . . . .	55
5.1.6	La machine Enigma . . . . .	55
5.2	Casser un cryptosystème . . . . .	61
5.3	Différents niveaux d'attaque . . . . .	62
5.4	Masque jetable, Vernam ( <i>One time pad</i> ) . . . . .	63
5.5	Cryptographie quantique . . . . .	64
5.6	La Cryptographie militaire (1883), Kerckhoffs . . . . .	64
5.7	<i>Communication Theory of Secrecy Systems</i> , Shannon . . . . .	65
5.8	Convertir du texte en nombre (Programmation) . . . . .	66
<b>6</b>	<b>Fonctions à sens unique</b> . . . . .	<b>69</b>
6.1	Fonctions à sens unique . . . . .	69
6.2	Sac à dos, Protocole DH, ..., chiffre de Rabin . . . . .	71
6.2.1	Partage de clés : protocole DH . . . . .	71
6.2.2	Un cryptosystème sans clé . . . . .	72
6.2.3	Algorithme du sac à dos . . . . .	72
6.2.4	Le chiffre de Rabin . . . . .	73
6.3	Implémentation avec Maple (Programmation) . . . . .	73

6.3.1	Le sac à dos . . . . .	73
6.3.2	Partage de clés . . . . .	75
6.3.3	Cryptosystème sans clé . . . . .	76
6.4	Le théorème du reste chinois et le chiffre de Rabin . . . . .	78
6.4.1	Le théorème du reste chinois . . . . .	78
6.4.2	Le chiffre de Rabin . . . . .	79
<b>7</b>	<b>Le RSA et le chiffrement Elgamal</b>	<b>81</b>
7.1	Le système RSA . . . . .	81
7.2	RSA et Maple (Programmation) . . . . .	83
7.3	Chiffrement Elgamal . . . . .	84
<b>8</b>	<b>Le DES</b>	<b>85</b>
8.1	L'algorithme LUCIFER : notion de ronde . . . . .	85
8.2	Le DES . . . . .	87
8.3	IDEA . . . . .	90
8.4	Modes de chiffrement par bloc. Mode ECB, CBC, CFB, OFB . . . . .	91
8.5	Ou exclusif et addition modulo 2 (Programmation) . . . . .	93
8.6	Addition modulo $2^{16}$ . . . . .	94
<b>9</b>	<b>Advanced Encryption Standard (AES)</b>	<b>95</b>
9.1	Introduction . . . . .	95
9.2	Les corps finis (Théorie) . . . . .	95
9.2.1	Construction de $GF(2^8)$ . . . . .	97
9.2.2	L'anneau $GF(2^8)[x]/(x^4 + 1)$ . . . . .	99
9.3	AES . . . . .	100
9.3.1	Les rondes . . . . .	100
9.3.2	La génération des clés de rondes (Key Expansion) . . . . .	101
9.3.3	Déchiffrement . . . . .	102
9.4	Maple et le corps de Galois $GF(2^8)$ (Programmation) . . . . .	102
9.5	Implémentation de l'AES (Programmation) . . . . .	104
9.5.1	Le corps de Galois $GF(2^8)$ . . . . .	104
9.5.2	Les routines . . . . .	104
9.5.3	KeyExpansion . . . . .	109
9.5.4	Le chiffrement . . . . .	111
<b>10</b>	<b>Courbes elliptiques</b>	<b>113</b>
10.1	Introduction . . . . .	113
10.2	Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$ ( $p$ premier) . . . . .	115
10.3	Courbes elliptiques sur $\mathbb{Z}/n\mathbb{Z}$ ( $n$ composé) . . . . .	116
10.4	Application à la cryptographie . . . . .	116
10.5	Application à la décomposition des grands nombres . . . . .	117
10.6	Courbes elliptiques et MAPLE (Programmation) . . . . .	118
10.6.1	Courbes elliptiques sur $\mathbb{R}$ . . . . .	118
10.6.2	Racine carrée dans $\mathbb{Z}/p\mathbb{Z}$ . . . . .	119
10.6.3	Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$ ( $p$ premier) . . . . .	120

10.6.4	Courbe symétrique par rapport à l'axe $Ox$ . . . . .	123
10.6.5	Courbes sur $Z/nZ$ ( $n$ composé) . . . . .	123
<b>11</b>	<b>Fonction de hachage</b> . . . . .	<b>127</b>
11.1	Protocole . . . . .	127
11.2	Empreinte (Hash Code) . . . . .	128
11.3	KECCAK ou SHA-3 . . . . .	129
11.4	Preuve de travail . . . . .	130
11.5	Générateur Pseudo-aléatoire . . . . .	131
<b>12</b>	<b>Protocole ZK : Zero Knowledge</b> . . . . .	<b>133</b>
12.1	Le démon de Quisquater et Guillou . . . . .	133
12.2	Protocole de Fiat-Shamir . . . . .	134
12.3	Graphes et cryptographie . . . . .	135
12.4	Complexité . . . . .	137
<b>13</b>	<b>Identification, Authentification, Signature</b> . . . . .	<b>139</b>
13.1	Authentification . . . . .	139
13.2	Identification . . . . .	141
13.3	Signature . . . . .	142
13.4	Signature Elgamal . . . . .	144
13.5	Conclusion . . . . .	145
<b>14</b>	<b>Horodatage et Blockchain</b> . . . . .	<b>147</b>
14.1	Horodatage . . . . .	147
14.2	Blockchain et le Bitcoin . . . . .	149
<b>15</b>	<b>Exemples d'applications de la cryptographie</b> . . . . .	<b>153</b>
15.1	PKI . . . . .	153
15.2	L'argent n'a pas d'odeur . . . . .	155
15.3	Organiser une partie de poker sur internet . . . . .	155
15.4	HTTPS . . . . .	156
15.5	Carte bancaire . . . . .	157
15.6	PGP . . . . .	158
15.7	Voter <i>via</i> Internet . . . . .	159
15.8	Chiffrement homomorphe . . . . .	160
15.9	Secret partagé, Clé partagée . . . . .	162
15.10	Le WIFI . . . . .	163
15.11	Chiffrement par flot . . . . .	164
15.12	La lettre recommandée avec AR . . . . .	164
15.13	Tatouage numérique . . . . .	165
15.14	Conclusion . . . . .	167
<b>16</b>	<b>Cryptanalyse</b> . . . . .	<b>169</b>

10.6.4	Courbe symétrique par rapport à l'axe $Ox$ . . . . .	123
10.6.5	Courbes sur $\mathbb{Z}/n\mathbb{Z}$ ( $n$ composé) . . . . .	123
<b>11</b>	<b>Fonction de hachage</b> . . . . .	<b>127</b>
11.1	Protocole . . . . .	127
11.2	Empreinte (Hash Code) . . . . .	128
11.3	KECCAK ou SHA-3 . . . . .	129
11.4	Preuve de travail . . . . .	130
11.5	Générateur Pseudo-aléatoire . . . . .	131
<b>12</b>	<b>Protocole ZK : Zero Knowledge</b> . . . . .	<b>133</b>
12.1	Le démon de Quisquater et Guillou . . . . .	133
12.2	Protocole de Fiat-Shamir . . . . .	134
12.3	Graphes et cryptographie . . . . .	135
12.4	Complexité . . . . .	137
<b>13</b>	<b>Identification, Authentification, Signature</b> . . . . .	<b>139</b>
13.1	Authentification . . . . .	139
13.2	Identification . . . . .	141
13.3	Signature . . . . .	142
13.4	Signature Elgamal . . . . .	144
13.5	Conclusion . . . . .	145
<b>14</b>	<b>Horodatage et Blockchain</b> . . . . .	<b>147</b>
14.1	Horodatage . . . . .	147
14.2	Blockchain et le Bitcoin . . . . .	149
<b>15</b>	<b>Exemples d'applications de la cryptographie</b> . . . . .	<b>153</b>
15.1	PKI . . . . .	153
15.2	L'argent n'a pas d'odeur . . . . .	155
15.3	Organiser une partie de poker sur internet . . . . .	155
15.4	HTTPS . . . . .	156
15.5	Carte bancaire . . . . .	157
15.6	PGP . . . . .	158
15.7	Voter <i>via</i> Internet . . . . .	159
15.8	Chiffrement homomorphe . . . . .	160
15.9	Secret partagé, Clé partagée . . . . .	162
15.10	Le WIFI . . . . .	163
15.11	Chiffrement par flot . . . . .	164
15.12	La lettre recommandée avec AR . . . . .	164
15.13	Tatouage numérique . . . . .	165
15.14	Conclusion . . . . .	167
<b>16</b>	<b>Cryptanalyse</b> . . . . .	<b>169</b>

<b>17 La cryptographie à travers l'Histoire</b>	<b>171</b>
17.1 L'Antiquité . . . . .	171
17.2 La mécanisation . . . . .	172
17.3 Systèmes symétriques . . . . .	172
17.4 Systèmes à clé publique (asymétriques) . . . . .	172
17.5 Mars 2000 : la signature numérique a valeur légale en France . . . . .	173
<b>Bibliographie</b>	<b>175</b>
<b>Index</b>	<b>177</b>