

Jean-Michel Masereel
Valérie Nacheff
Emmanuel Volte

Évolution de la cryptographie à travers les âges

Cours, exercices corrigés,
algorithmes en Scratch et Python



Table des matières

Introduction	13
0.1. La cryptographie	13
0.2. Cryptographie symétrique / asymétrique	15
0.2.1. La cryptographie symétrique	15
0.2.2. La cryptographie asymétrique	15
0.3. Systèmes de chiffrement et clef	15
0.3.1. Coder et chiffrer	15
0.3.2. Quelques propriétés indispensables pour bien chiffrer .	16
0.4. Les apports de la cryptographie	16
0.5. Présentation de l'ouvrage	18
0.6. Exercices	18
I. De l'Antiquité à la fin de la Seconde Guerre mondiale	25
1. La cryptographie dans l'Antiquité	29
1.1. Le plus ancien document chiffré de l'Antiquité	29
1.2. Petite histoire de l'alphabet	30
1.2.1. L'évolution de l'alphabet	30
1.2.2. L'alphabet et la mythologie	31
1.3. Le procédé « Atbash », 500 av. J.-C.	31
1.4. La scytale spartiate, 400 av. J.-C.	33
1.5. Le carré de Polybe, 200 à 125 av. J.-C.	34
1.6. Le code de Jules César, 60 av. J.-C.	35
1.7. Exercices	35
2. La cryptographie au Moyen Âge et à la Renaissance	39
2.1. Le Moyen Âge	39
2.1.1. Les méthodes de chiffrement	39
2.1.2. Les premières cryptanalyses	40

2.1.3.	Les premiers nomenclateurs	43
2.2.	La Renaissance	44
2.2.1.	Le XV ^e siècle	44
2.2.2.	Le XVI ^e siècle	46
2.3.	Quelques exemples de nomenclateurs	52
2.3.1.	Marie de Guise	52
2.3.2.	Marie Stuart	55
2.4.	Exercices	58
3.	La cryptographie de l’Ancien Régime	63
3.1.	Le chiffre de Louis XIV	63
3.2.	Le chiffre de Marie-Antoinette	64
3.3.	Exercices	68
4.	Les chiffrements affine, de Playfair et de Hill	71
4.1.	Le chiffrement affine	71
4.2.	Le chiffrement de Playfair	72
4.2.1.	Les chiffrements polygraphiques	72
4.2.2.	Description du chiffre de Playfair	72
4.2.3.	Cryptanalyse	74
4.2.4.	Utilisation du chiffrement de Playfair	76
4.3.	Le chiffrement de Hill	76
4.3.1.	Historique	76
4.3.2.	Description	76
4.3.3.	Cryptanalyse	77
4.3.4.	L’influence du chiffrement de Hill sur la cryptographie	78
4.4.	Exercices	78
5.	La cryptographie des guerres mondiales	81
5.1.	La Première Guerre mondiale	81
5.1.1.	Le télégramme de Zimmermann	82
5.1.2.	Le chiffre ADFGVX	84
5.2.	La Seconde Guerre mondiale	86
5.2.1.	La machine Enigma et les cryptanalystes de Bletchley Park	86
5.2.2.	Le code Navajo	92
5.3.	Exercices	93

II. La cryptographie symétrique à clef secrète	95
6. La génération de nombres aléatoires	99
6.1. Définitions	100
6.2. Sécurité des générateurs pseudo-aléatoires	101
6.3. Générateurs de bits purement aléatoires	102
6.3.1. Les générateurs matériels	102
6.3.2. Les générateurs logiciels	103
6.3.3. La correction du désalignement	104
6.4. Générateurs pseudo-aléatoires non cryptographiquement sûrs	105
6.4.1. Les générateurs congruentiels linéaires - LCG	105
6.4.2. Mersenne Twister	108
6.4.3. Les générateurs basés sur les fonctions à sens unique	109
6.5. Générateurs cryptographiquement sûrs	109
6.6. Tests statistiques	111
6.6.1. Test du monobit et application	111
6.6.2. Tests du poker	112
6.6.3. Run test	113
6.6.4. Tests graphiques	121
6.7. Exercices	126
6.7.1. Autour des vitraux de Richter	126
6.7.2. Autour de la racine de 2	131
6.7.3. Autre exercice	133
7. Le chiffrement à flot	135
7.1. Le masque jetable ou One-Time Pad	135
7.1.1. Description	135
7.1.2. Historique	136
7.1.3. Utilisations	136
7.1.4. Le masque jetable et la cryptographie quantique	137
7.2. LFSR	139
7.2.1. Introduction	139
7.2.2. Définition - Exemples - Propriétés	139
7.2.3. Algorithme de Berlekamp-Massey	141
7.2.4. Améliorations des LFSR	142
7.3. Exemples de chiffrements à flot	144
7.3.1. RC4	144
7.3.2. A5/1	146

7.3.3.	E0	147
7.3.4.	SNOW 2.0	147
7.4.	Exercices	149
8.	Chiffrement par blocs	151
8.1.	Introduction	151
8.2.	Modes opératoires	152
8.2.1.	Le mode ECB (Electronic Code Book)	152
8.2.2.	Le mode CBC (Cipher Block Chaining)	154
8.2.3.	Le mode OFB (Output FeedBack)	155
8.2.4.	Le mode CFB (Cipher FeedBack)	157
8.2.5.	Le mode CTS (CipherText Stealing)	159
8.3.	DES	161
8.3.1.	Introduction	161
8.3.2.	Fonctionnement	162
8.3.3.	Avenir	163
8.4.	AES	163
8.4.1.	Principe	164
8.4.2.	Description	164
8.5.	Exercices	169
8.5.1.	DES	169
8.5.2.	AES	176
9.	Les schémas de Feistel	179
9.1.	Les différents types de schémas	179
9.1.1.	Définitions et notations	179
9.1.2.	Les schémas de Feistel classiques	180
9.1.3.	Les schémas de Feistel contractants	181
9.1.4.	Les schémas de Feistel expansifs	182
9.2.	Les attaques	183
9.2.1.	Présentation	183
9.2.2.	Sur les schémas classiques	185
9.2.3.	Sur les schémas de Feistel contractants	188
9.2.4.	Sur les schémas de Feistel expansifs	190
9.3.	Exercices	195

10. Les fonctions de hachage	199
10.1. Utilisation des fonctions de hachage	200
10.1.1. L'intégrité des données	200
10.1.2. L'engagement	200
10.1.3. Les mots de passe	200
10.1.4. La signature	201
10.1.5. Les structures de données	201
10.2. Définitions	201
10.3. Collisions sur les fonctions de hachage	202
10.3.1. Paradoxe des anniversaires	202
10.3.2. Application aux fonctions de hachage	204
10.4. Construction pratique d'une fonction de hachage en Python	204
10.4.1. Quelques fonctions utiles	204
10.4.2. Construction d'une fonction de compression	205
10.5. Construction de fonctions de hachage par le procédé de Merkle-Damgård	205
10.5.1. Complétion du message (padding)	206
10.5.2. Algorithme de Merkle-Damgård	206
10.5.3. Attaque par « length extension »	207
10.6. Conclusion	208
10.7. Exercices	208
11. La stéganographie	211
11.1. Stéganographie dans l'histoire	211
11.1.1. Dans l'Antiquité, 500 av. J.-C.	211
11.1.2. La grille de Cardan, 1550	212
11.1.3. Stéganographie dans la littérature	213
11.1.4. Stéganographie dans les journaux	213
11.1.5. Stéganographie moderne	214
11.2. Cacher un texte dans un arbre de choix	214
11.3. Exercices	218
III. La cryptographie asymétrique à clef publique	223
12. Les origines de la cryptographie à clef publique	227
12.1. La complexité des algorithmes	227

12.2. Le problème du sac à dos (1972)	228
12.2.1. Introduction	228
12.2.2. Formulation mathématique	229
12.2.3. Les méthodes de résolution	229
12.2.4. Le problème du sac à dos en cryptographie : le cryptosystème de Merkle-Hellman (1978) [17]	231
12.3. Le protocole d'échange de clefs de Diffie-Hellman (1976)	232
12.3.1. Le protocole	232
12.3.2. L'attaque de l'homme du milieu	233
12.3.3. Le problème calculatoire de Diffie-Hellman	233
12.4. Le chiffrement de Rabin (1979)	234
12.4.1. Présentation du chiffrement	234
12.4.2. Déchiffrement	234
12.4.3. Sécurité du chiffrement	235
12.5. Le chiffrement d'El Gamal (1984)	235
12.5.1. Chiffrement	235
12.5.2. Déchiffrement	236
12.5.3. Sécurité	236
12.6. Exercices	236
13. Le RSA (1977)	243
13.1. Présentation du RSA	243
13.1.1. Le RSA en confidentialité	243
13.1.2. Démonstration de la propriété de base du RSA	245
13.1.3. Le RSA en authentification	246
13.1.4. Le RSA en signature	246
13.1.5. Le RSA en confidentialité/signature	246
13.1.6. Le RSA pour tirer à Pile ou Face sur Internet	247
13.1.7. La factorisation et l'indicatrice d'Euler	248
13.2. Quelques erreurs à ne pas faire avec le RSA	248
13.2.1. Attaques par messages prévisibles	248
13.2.2. Plusieurs envois du même message	248
13.2.3. Deux personnes distinctes doivent avoir deux modules distinctes	248
13.2.4. Les attaques en signature	249
13.3. Le RSA et les cartes bancaires	249
13.3.1. Code confidentiel	249
13.3.2. Authentification hors ligne	250

13.3.3. Authentification en ligne	250
13.4. Exercices	251
14. Les preuves à divulgation nulle de connaissance	255
14.1. Deux exemples simples	255
14.1.1. La caverne d'Ali Baba	255
14.1.2. Les bonbons d'Halloween	257
14.2. Définitions	258
14.2.1. Les propriétés des protocoles	258
14.2.2. Les schémas de mise en gage	258
14.3. Les schémas à divulgation nulle de connaissance avec mise en gage	259
14.3.1. Le problème des 3 couleurs	259
14.3.2. PKP : Permuted Kernel Problem	262
14.4. Exercices	267
15. Les courbes elliptiques	273
15.1. Courbes elliptiques sur \mathbb{R}	273
15.1.1. Définition	273
15.1.2. La loi de groupe	273
15.2. Courbes elliptiques modulo un nombre premier	276
15.2.1. Définition	276
15.2.2. Addition sur les courbes elliptiques modulo un nombre premier	276
15.2.3. Exemple	277
15.3. Application à la cryptographie	278
15.3.1. Fonction exponentielle sur les courbes elliptiques . . .	278
15.3.2. Le système de Menezes-Vanstone	279
15.4. Exercices	279
IV. Notions mathématiques et informatiques	281
16. Pré-requis : rappels	283
16.1. Relations binaires	283
16.2. Propriétés sur les entiers naturels	284
16.3. Raisonnement par récurrence	285
16.4. Division euclidienne dans \mathbb{Z}	285

17. Structures algébriques	287
17.1. Loi interne sur un ensemble	287
17.2. Groupes	287
17.2.1. Sous-groupes	289
17.3. Anneaux	290
17.4. Corps	291
17.5. Espaces vectoriels	292
17.6. Algèbres	292
17.7. Les groupes finis et le théorème de Lagrange	293
18. Arithmétique	295
18.1. Algèbre dans \mathbb{Z}	295
18.1.1. Sous-groupes de \mathbb{Z}	295
18.1.2. PGCD	295
18.1.3. Nombres premiers entre eux	298
18.1.4. PPCM	299
18.1.5. Nombres premiers	301
18.2. Algèbre dans $\mathbb{Z}/n\mathbb{Z}$	302
18.2.1. Définitions - Propriétés	302
18.2.2. Théorème des restes chinois	307
18.2.3. Indicatrice d'Euler	308
18.2.4. Les théorèmes de Fermat et d'Euler-Fermat	309
19. Le logarithme discret	311
19.1. L'algorithme Baby-step giant-step	311
19.2. Méthode rho de Pollard pour le logarithme discret	312
20. Arithmétique des polynômes	315
20.1. Définitions - Propriétés	315
20.2. Division euclidienne	316
20.3. Racines d'un polynôme	316
20.4. PGCD, PPCM, polynômes premiers entre eux	317
20.4.1. Plus grand commun diviseur	317
20.4.2. Polynômes premiers entre eux	319
20.4.3. Plus petit commun multiple	320
20.5. Polynômes irréductibles	321
20.5.1. Définition - Propriétés	321
20.5.2. Décomposition en facteurs irréductibles	321

20.6. Algèbre $\mathbb{K}[X]/\langle P \rangle$	322
20.6.1. Les idéaux de $\mathbb{K}[X]$	322
20.6.2. Algèbre $\mathbb{K}[X]/\langle P \rangle$	322
20.6.3. Représentation de l'algèbre $\mathbb{K}[X]/\langle P \rangle$	323
20.6.4. Calculs dans $\mathbb{K}[X]/\langle P \rangle$	324
21. Corps finis	325
21.1. Introduction - Exemple	325
21.2. Construction des corps finis	325
21.3. Caractéristique d'un corps fini	326
21.4. Arithmétique dans $\mathbb{F}_2[X]/\langle P \rangle$	326
21.5. Application à l'AES	327
21.5.1. L'addition	328
21.5.2. La multiplication	328
21.5.3. L'inverse	328
22. Primalité	331
22.1. Introduction - Premiers tests	331
22.1.1. Un algorithme élémentaire	331
22.1.2. Le crible d'Eratosthène	331
22.1.3. Test de primalité de Fermat	332
22.2. Le test de Solovay-Strassen	332
22.2.1. Les résidus quadratiques	332
22.2.2. Les symboles de Legendre et Jacobi	333
22.2.3. Le test de primalité d'Euler	335
22.2.4. Le test de Solovay-Strassen	335
22.3. Le test de Miller-Rabin	337
22.4. Deux algorithmes de factorisation	338
22.4.1. La méthode $p - 1$ de Pollard	338
22.4.2. La méthode rho de Pollard	339
23. Informatique appliquée	341
23.1. Introduction rapide à Scratch et Python	341
23.2. Scratch	341
23.2.1. Installation de Scratch, documentation	341
23.2.2. Les types de variables	341
23.2.3. Opérations sur les nombres et les chaînes de caractères	342
23.2.4. Les listes	343

23.2.5. Les blocs	343
23.3. Python	343
23.3.1. Installation de Python, documentation	343
23.3.2. Vue d'ensemble de Python	344
23.3.3. Principaux types d'objets	346
23.3.4. Tranchage	350
23.3.5. La programmation	351
23.3.6. Les fonctions	352
23.3.7. Les dictionnaires	354
23.4. Exemple de problème	356
23.4.1. Énoncé	356
23.4.2. Correction	356

V. Solutions des exercices **359**

Bibliographie **417**

Index **419**