

Les codes secrets décryptés

Table des matières détaillée

1.	Introduction	7
1.1.	Définition de termes courants	9
1.2.	Repères historiques	13
	Les 3000 premières années (de 2000 av. J.-C. à 1000 ap. J.-C.)	13
	L'éveil de l'Occident (de 1000 à 1800)	14
	L'essor des communications (de 1800 à 1970)	17
	La cryptologie moderne (de 1970 à nos jours)	19
1.3.	Conventions	21
2.	Stéganographie	23
2.1.	Encres invisibles	27
	Les plus simples	27
	Autres encres apparaissant avec le feu	28
	Encres apparaissant avec de la poudre	28
	Encres utilisant des produits chimiques	28
	Pantagruel, chapitre XXIV	29
2.2.	Les Ave Maria de Trithème	31
	Chiffrement	31
	Déchiffrement	32
	Décryptement	32
2.3.	Grille de Cardan	33
	Chiffrement	33
	Déchiffrement	33
	Variantes	34
2.4.	L'alphabet bilitère de Francis Bacon	35
	Chiffrement	36
	Déchiffrement	37
	Variantes : les chiffres trilitères	37
2.5.	Sémagrammes	39
2.6.	Micropoint	41
2.7.	Acrostiches	43
2.8.	Code de Trevanion	45
2.9.	Lettres à double entente	46
	Lettre de Richelieu à l'ambassadeur de France à Rome	46
	Correspondance entre George Sand et Alfred de Musset	47
	Déchiffrement	47
2.10.	La méthode de Grandpré	48
2.11.	Cacher une image numérique dans une autre	50
	Parenthèse mathématique : deux règles de calculs avec les matrices	50
	Camouflage	51
	Décamouflage	51
	Exemple numérique	51
	Exemple visuel	51
2.12.	Cacher un texte dans une image numérique	53
	Parenthèse informatique : représentation d'une image couleur	53
	Parenthèse mathématique : conversion décimal - binaire	54
	Parenthèse informatique : le code ASCII	55
	Représentation binaire du texte	56
	Intégration du texte dans l'image	56
	Récupération du texte	56
3.	Codes et répertoires	57
	Types de répertoires	58
	Répertoires ordonnés	59

	Répertoires incohérents	59
	Décryptement	59
3.1.	Code de Popham	61
3.2.	Code télégraphique chiffré de Sittler	63
	Décryptement	66
3.3.	Code Navajo	68
4.	Chiffres de transposition	71
	Parenthèse mathématique : nombre de permutations	71
4.1.	La scytale spartiate	72
	Chiffrement	73
	Exemple	73
	Déchiffrement	73
	Décryptement	73
4.2.	Le chiffre Rail Fence	75
	Chiffrement	75
	Déchiffrement	75
	Variante	75
	Déchiffrement d'un rail fence à trois niveaux	76
4.3.	La grille tournante	77
	Construction d'un cache	77
	Chiffrement	77
	Décryptement	78
	<i>Mathias Sandorf</i> , de Jules Verne	80
	Variante	88
4.4.	Transpositions rectangulaires	89
	Chiffrement	89
	Déchiffrement	90
	Décryptement d'un tableau à colonnes complètes	90
	Décryptement d'un tableau à colonnes incomplètes	94
4.5.	Double transposition	96
	Chiffrement	96
	Déchiffrement	97
4.6.	Le chiffre UBCHI	98
	Chiffrement	98
	Déchiffrement	98
4.7.	Transpositions triangulaires et trapézoïdales	100
	Chiffrement	100
	Déchiffrement	100
	Variantes	100
4.8.	Transpositions à figures	102
4.9.	Une lettre chiffrée de Balzac	103
5.	Substitutions simples	105
5.1.	Le Pig pen	106
	L'alphabet des templiers	107
	L'alphabet de « La Buse »	107
	Le code tic-tac-toe	109
5.2.	Le carré de Polybe	110
	Chiffrement	111
	Déchiffrement	112
	Décryptement	112
	Variante d'Uesugi Kenshin	113
	Variante d'Elizabeth Van Lew	113
	Carré du bastion Troubetskoï	114
	Remplissage de la grille avec un mot de passe	114
	Le chiffre des nihilistes	115
	Système de Mirabeau	115
5.3.	Le chiffre de César	117
	Chiffrement	119

	Déchiffrement	120
	Décryptement	120
	ROT13	121
5.4.	Alphabets désordonnés	122
	Chiffrement	122
	Décryptement	124
	Attaque par mot probable	124
	Analyse des fréquences	126
	Analyse des fréquences en français	126
	<i>Le scarabée d'or</i> , d'Edgar Allan Poe	132
	<i>Les compagnons du silence</i> , de Paul Féval	152
	<i>Les hommes dansants</i> , d'Arthur Conan Doyle	153
	<i>Chain of Death</i> , de Maxwell Grant	153
5.5.	Alphabet Morse	155
5.6.	Alphabets réversibles	156
	Chiffrement et déchiffrement	156
	Le chiffre Atbash	156
	Le chiffre Albam	157
	Le chiffre Atbah	157
	Le chiffre de Wolseley	157
5.7.	Le chiffre du calendrier	159
	Décryptement	159
5.8.	Le système monôme-binôme	160
	Chiffrement	160
	Décryptement	160
	Variantes	161
5.9.	Le chiffre VIC	162
	Chiffrement	162
	Déchiffrement	168
5.10.	Le chiffre affine	169
	Parentèse mathématique : addition modulo n	169
	Chiffrement	169
	Exemple de chiffrement	170
	Déchiffrement	170
	Parentèse mathématique : l'inverse modulo n	170
	Parentèse mathématique : l'algorithme d'Euclide étendu	171
	Formule de déchiffrement	171
	Exemple de déchiffrement	172
	Décryptement	172
5.11.	Chiffrement monoalphabétique par polyphones	173
	Chiffre de l'Inquisiteur de Malte (1585)	173
	Exemple de chiffrement	173
	Exemple de déchiffrement	173
	Variantes	174
	<i>The Man from Scotland Yard</i> , de Maxwell Grant	174
	Chiffrement	175
5.12.	Le chiffre de Bazeris	176
	Première version	176
	Chiffrement	176
	Exemple de chiffrement	177
	Déchiffrement	177
	Version améliorée	177
	Chiffrement	178
	Déchiffrement	179
6.	Chiffres homophoniques	181
6.1.	Représentation multiple du E	183
6.2.	Le carré de 25 à représentations multiples	184
	Carré de 25 à quatre représentations	184
	Décryptement	184

	Carré de 25 à deux représentations	185
	Carré de 25 à huit représentations	185
	Carré de 25 à seize représentations	186
	Décryptement	187
6.3.	Le disque de l'armée mexicaine	193
	Décryptement de deux cryptogrammes semblables	194
	Cryptanalyse d'un long cryptogramme	195
	Variante : les appareils à bande	198
6.4.	Renversement des fréquences	199
	Variantes	200
6.5.	Le système du dictionnaire	202
	<i>Le code Rebecca</i> , de Ken Follett	203
6.6.	Les papiers de Beale	204
6.7.	Le cryptogramme du tueur du Zodiaque	209
7.	Chiffres polyalphabétiques	213
7.1.	Tableau de Trithème	216
7.2.	Le chiffre de Belaso	218
	Chiffrement	218
	Déchiffrement	218
7.3.	Le chiffre de Porta	219
	Décryptement	220
7.4.	Le carré de Vigenère	222
	Comment utiliser le carré de Vigenère ?	223
	Vigenère (chiffré = clair + clef)	223
	Beaufort (chiffré = clef - clair)	223
	Variante à l'allemande du chiffre de Beaufort (chiffré = clair - clef)	223
	Variante de Rozier	224
7.5.	La réglette de Saint-Cyr	225
7.6.	Le chiffre de Vigenère	227
	Chiffrement	227
	Décryptement	228
	Première méthode (Babbage-Kasiski)	228
	Deuxième méthode (Bazeries)	232
	Troisième méthode (Friedman)	233
	Décryptement automatique d'un chiffre de Vigenère	235
	Allongement de la clef	237
	Procédé autoclave	237
	Exemple	238
	Décryptement	238
	Variante	239
	Décryptement	239
7.7.	Le chiffre de Beaufort	240
	Chiffrement	240
	Exemple	240
	Variante à l'allemande	240
	Exemple	240
7.8.	Le chiffre de Gronsfeld	241
	La Jangada	241
7.9.	Le masque jetable	248
	Exemple	249
	Il ne faut jamais utiliser deux fois la même clef !	249
	Méthode	250
	Génération de clefs	252
7.10.	Tableau à alphabets désordonnés	254
	Tableau à alphabets désordonnés et parallèles	254
	Décryptement	255
	Tableau à alphabets désordonnés et non parallèles	255
7.11.	Le cylindre de Jefferson	256

8.	Chiffres tomogrammiques	259
8.1.	Le chiffre de Chase	259
	Chiffrement	259
	Déchiffrement	260
8.2.	Le code Morse fractionné	261
	Chiffrement	261
	Déchiffrement	262
	Variante (Morbit)	262
	Chiffrement	263
	Déchiffrement	263
8.3.	Le chiffre Pollux	264
	Chiffrement	264
	Déchiffrement	265
	Décryptement	265
8.4.	Le chiffre de Collon	267
	Chiffrement	267
	Déchiffrement	268
	Décryptement	268
	Exemple de décryptement	268
8.5.	Le chiffre bifide de Delastelle	274
	Méthode de chiffrement	274
	Exemple	274
	Déchiffrement	274
	Variante trifide	275
8.6.	Le chiffre ADFGVX	276
	Chiffrement	277
	Déchiffrement	278
9.	Chiffres polygrammiques	291
9.1.	Tableau de bigrammes	293
9.2.	Le chiffre de Playfair	294
	Chiffrement	294
	Déchiffrement	295
	Caractéristiques du système Playfair	295
	Décryptement « à l'ancienne »	297
	Décryptement informatisé	302
9.3.	Le chiffre Slidefair	303
	Chiffrement	303
	Exemple	303
9.4.	Chiffrement à deux carrés	304
	Chiffrement	304
	Déchiffrement	304
9.5.	Chiffrement à trois carrés	305
	Chiffrement	305
	Déchiffrement	305
9.6.	Chiffrement à quatre carrés	307
	Chiffrement	307
	Déchiffrement	307
	Décryptement	308
	Variante	308
9.7.	Chiffre de Hill	309
	Chiffrement	309
	Déchiffrement	310
	Exemple de déchiffrement	311
	Petite parenthèse mathématique	311
	Variante	312
	Décryptement	312
	Parenthèse mathématique	313
10.	Cryptographie moderne	315

	Utilisateurs légitimes	315
	Adversaires	315
10.1.	Le chiffrement par blocs	317
10.2.	Les systèmes à clefs publiques	318
10.3.	Le chiffre de Merkle-Hellman	320
	Parenthèse mathématique : suite supercroissante	320
	1. Choix de la clef	321
	2. Chiffrement	322
	3. Déchiffrement	322
	Exemple complet de chiffrement/déchiffrement	322
10.4.	RSA	324
	1. Choix de la clef	324
	2. Chiffrement	325
	3. Déchiffrement	325
10.5.	Courbes elliptiques	326
	Parenthèse mathématique : logarithme discret	326
	Utilisation des courbes elliptiques en cryptographie	326
10.6.	Cryptographie quantique	328
11.	ABC de cryptanalyse	329
11.1.	Principes de Kerkhoffs	330
	Desiderata de la cryptographie militaire	330
	Commentaires	331
11.2.	Comment reconnaître un chiffre ?	332
11.3.	Devenez casseur de codes !	346
12.	Divertissements cryptographiques	353
12.1.	Devenez télépathe !	353
	Le truc	354
12.2.	Devenez devin !	355
	Présentation du tour	355
	Explication du tour	356
	Codage de la couleur	356
	Codage de la distance	356
	Carte de Jules	357
12.3.	Cryptographie oulipienne	358
	La belle absente	358
13.	Bibliographie	359
	Livres en français	359
	Livres en anglais	365
	Internet	367