

Table des matières

Préface	vii
Avant-propos	ix
1 Les procédés traditionnels	1
1.1 Les substitutions simples	1
1.2 Transpositions	5
1.3 Les substitutions polygrammiques	7
1.4 La genèse du polyalphabétisme	12
1.5 Les machines à chiffrer	16
1.6 La stéganographie	19
2 La cryptographie symétrique moderne	21
2.1 La naissance de la cryptographie moderne	21
2.2 Les systèmes de confidentialité	23
2.3 Diffusion et confusion	24
2.4 Le chiffrement à flot	26
2.5 Le chiffrement par bloc	33
3 La cryptographie à clé publique	45
3.1 Les fonctions à sens unique	46
3.2 Le chiffrement	47
3.3 La signature numérique	57
3.4 L'authentification	62
3.5 Les courbes elliptiques	64
3.6 L'algorithmique de la cryptographie à clé publique	70
4 La cryptanalyse	81
4.1 La force brutale	81
4.2 La loi de Moore	83

4.3	La résolution des substitutions simples	85
4.4	La cryptanalyse du chiffrement polyalphabétique	86
4.5	Les cryptanalyses des chiffrements modernes	96
4.6	La factorisation des entiers	99
4.7	Les attaques physiques	102
5	La cryptographie au quotidien	109
5.1	Les infrastructures de gestion des clés publiques	109
5.2	La carte bancaire	110
5.3	La sécurité de l'internet	115
5.4	La cryptologie dans la téléphonie mobile	118
5.5	La télévision à péage	120
6	La théorie cryptologique	127
6.1	Motivation	127
6.2	La sécurité inconditionnelle	129
6.3	La sécurité calculatoire	134
7	Apport de la physique quantique	151
7.1	Information et calcul quantique	152
7.2	L'algorithme de Shor pour la factorisation	159
7.3	La cryptographie quantique	164
7.4	En conclusion	168
	La nature de la cryptologie	169
	Solutions	173
	Bibliographie	177
	Index	179