

Sommaire

Introduction	9
 Chapitre 1 – Jusqu’où va la sécurité de l’information ?	11
Les codes, les chiffres et les clés	12
Clés privées et clés publiques	15
Le « télégramme Zimmermann »	16
Le Bureau 40 se met au travail	18
 Chapitre 2 – La cryptographie de l’Antiquité au XIX^e siècle	23
La stéganographie	23
La cryptographie par transposition	24
Rendre à César ce qui appartient à César	26
$16 = 4$: l’arithmétique modulaire et les mathématiques du chiffre de César	29
En jouant aux espions	35
Au-delà du chiffre affine	37
L’analyse de fréquences	40
Un exemple en détail	41
Le chiffre polyalphabétique	43
La contribution d’Alberti	44
Le carré de Vigenère	45
Classer des alphabets	49
Le cryptanalyste anonyme	51
 Chapitre 3 – Des machines qui encodent	55
Le code Morse	55
À 80 kilomètres de Paris	59
La machine Enigma	62
Décrypter le code Enigma	69
Les Britanniques prennent le relais	71
Autres codes de la Seconde Guerre mondiale	73
Les « radiocodeurs » navajos	75
Les voies de l’innovation : le chiffre de Hill	76

Chapitre 4 – Dialoguer avec des zéros et des un	79
Le code ASCII	79
Le système hexadécimal	81
Systèmes de numération et changements de base	84
Codes contre la perte d'informations	85
Les « autres » codes : les normes de l'industrie et du commerce	90
Les cartes de crédit	90
Les codes-barres	94
Le code EAN-13	95
 Chapitre 5 – Un secret de polichinelle : la cryptographie à clé publique	99
Le problème de la distribution de clé	99
L'algorithme de Diffie-Hellman	100
Les nombres premiers au secours : l'algorithme RSA	104
L'algorithme RSA en détail	105
Pourquoi devrions-nous avoir confiance en l'algorithme RSA ?	106
Une assez bonne confidentialité	107
Authentification des messages et des clés	108
Les fonctions de hachage	109
Les certificats de clé publique	110
Mais alors, peut-on acheter sur Internet en toute sécurité ?	112
 Chapitre 6 – Un futur quantique	113
Le traitement quantique	113
Le chat qui n'était ni vivant ni mort	114
Du bit au <i>qubit</i>	116
La fin de la cryptographie ?	117
Ce qu'enlève la mécanique quantique, la mécanique quantique le donne	118
Le chiffre indéchiffrable	119
32 centimètres de secret absolu	124
 Annexe	127
 Bibliographie	139
 Index analytique	141