

TABLE DES MATIÈRES

Chapitre 1 : éloge de l'intimité	7
La cryptographie, pourquoi ?	12
Chapitre 2 : premiers principes	25
1. Distribution des rôles	26
2. Un peu de vocabulaire	27
3. Les clés	32
4. Algorithmes secrets	34
5. Algorithmes publics à clé secrète	35
6. Les principaux objectifs de la cryptographie	37
7. Autres objectifs	39
8. Messages subliminaux	44
Chapitre 3 : aperçu historique	47
1. Transposition, substitution	48
2. Le chiffre de César	50
3. Les chiffres « monoalphabétiques »	53
4. Le chiffre de Vigenère	58
5. Enigma	66
6. Le carnet de codage	79
Annexe : fréquences des lettres dans la langue française	91
Chapitre 4 : forces et faiblesses	93
1. Fabriquons un système parfait	94
2. Un message équivoque	98
3. Unicité	102
4. La redondance, un ennemi redoutable	103
5. Les clés	108
6. Numérisation	111
7. Les atouts d'un bon cryptosystème	115

Chapitre 5 : clé secrète	119
1. Carnets de codage : le retour	120
2. Chiffrements en continu	128
3. Chiffrements par blocs	133
4. Le « DES » : un standard de chiffrement	137
5. L'« AES » : un successeur pour le DES	144
6. Alice au pays des photons	145
Chapitre 6 : clé publique	157
1. Sens unique	159
2. Brèche secrète	160
3. Le protocole public d'échange de clé	163
4. Les systèmes de chiffrement « à clé publique »	166
5. Les empilements	168
6. Le système « RSA »	174
7. Le tournoi « clé secrète » contre « clé publique »	179
8. « PGP »	184
Annexe A. Le protocole de Diffie et Hellman	189
Annexe B. Empilements	191
Annexe C. Le système RSA	194
Chapitre 7 : authentification	197
1. Empreinte	197
2. Signature numérique	204
3. Empreinte signée	215
4. Alice cherche à tromper Bernard	218
5. Certificats	223
Chapitre 8 : la théorie face au réel	229
1. Attaques de l'algorithme	230
2. Attaques de l'environnement	236
3. Un droit, un devoir, une forme de solidarité	245
Glossaire	247
Index	253