

TABLE DES MATIÈRES

| | |
|---|------------|
| Chapitre 1 : éloge de l'intimité | 7 |
| La cryptographie, pourquoi ? | 10 |
| Mise en appétit : grilles mêlées | 19 |
| Le saviez-vous ? | 20 |
| Chapitre 2 : premiers principes | 23 |
| 1. Distribution des rôles | 24 |
| 2. Un peu de vocabulaire | 24 |
| 3. Les clés | 28 |
| 4. Algorithmes secrets | 29 |
| 5. Algorithmes publics à clé secrète | 30 |
| 6. Les principaux objectifs de la cryptographie | 32 |
| 7. Autres objectifs | 33 |
| 8. Messages subliminaux | 37 |
| Mise en appétit : petit Champollion deviendra grand | 39 |
| Travaux dirigés : partage de secrets | 40 |
| Chapitre 3 : aperçu historique | 47 |
| 1. Transposition, substitution | 47 |
| 2. Le chiffre de César | 49 |
| 3. Les chiffres « monoalphabétiques » | 51 |
| 4. Le chiffre de Vigenère | 55 |
| 5. Enigma | 61 |
| 6. Le carnet de codage | 71 |
| Mise en appétit : message subliminal | 81 |
| Travaux dirigés : l'attaque du texte chiffré | 83 |
| Travaux dirigés : information | 91 |
| Chapitre 4 : forces et faiblesses | 101 |
| 1. Fabriquons un système parfait | 102 |
| 2. Un message équivoque | 105 |
| 3. Unicité | 108 |
| 4. La redondance, un ennemi redoutable | 108 |
| 5. Les clés | 112 |
| 6. Numérisation | 114 |
| 7. Les atouts d'un bon cryptosystème | 117 |
| Mise en appétit : jeux avec les mots | 120 |
| Travaux dirigés : redondance | 121 |
| Travaux dirigés : équivoque | 130 |

| | |
|---|------------|
| Chapitre 5 : clé secrète | 139 |
| 1. Carnets de codage : le retour | 139 |
| 2. Chiffrements en continu | 146 |
| 3. Chiffrements par blocs | 150 |
| 4. Le « DES » : un standard de chiffrement | 152 |
| 5. L' « AES » : un successeur pour le DES | 157 |
| 6. Alice au pays des photons | 158 |
| Mise en appétit : listes à prolonger | 167 |
| Travaux dirigés : surchiffrement | 169 |
| Travaux dirigés : chaînage | 173 |
| Chapitre 6 : clé publique | 179 |
| 1. Sens unique | 180 |
| 2. Brèche secrète | 181 |
| 3. Le protocole public d'échange de clé | 183 |
| 4. Les systèmes de chiffrement « à clé publique » | 185 |
| 5. Les empilements | 187 |
| 6. Le système « RSA » | 192 |
| 7. Le tournoi « clé secrète » contre « clé publique » | 195 |
| 8. « PGP » | 199 |
| Annexe : le système RSA | 203 |
| Mise en appétit : les diodes | 205 |
| Travaux dirigés : sens unique | 206 |
| Chapitre 7 : authentification | 213 |
| 1. Empreinte | 213 |
| 2. Signature numérique | 218 |
| 3. Empreinte signée | 226 |
| 4. Alice cherche à tromper Bernard | 229 |
| 5. Certificats | 232 |
| Mise en appétit : S + 1 | 237 |
| Travaux dirigés : empreintes | 238 |
| Chapitre 8 : la théorie face au réel | 243 |
| 1. Attaques de l'algorithme | 244 |
| 2. Attaques de l'environnement | 248 |
| 3. Un droit, un devoir, une forme de solidarité | 254 |
| Mise en appétit : fuite d'information | 256 |
| Travaux dirigés : complexité | 258 |
| Indications et corrigés | 263 |
| Glossaire | 293 |
| Bibliographie | 298 |
| Index | 299 |