

# TABLE DES MATIÈRES

<b>Avant-propos</b>	<b>3</b>
<b>1. De la cryptographie classique à la cyber-sécurité moderne</b>	<b>13</b>
1.1. Intérêt historique de la cryptographie classique.....	13
1.2. Exposé du plan .....	14
1.2.1. Méthodes de substitution .....	14
1.2.2. Dictionnaires chiffrés.....	14
1.2.3. Chiffrement par transposition .....	15
1.2.4. Machines cryptographiques.....	15
1.2.5. Chiffrements modernes : symétriques par bloc et RSA, extraction de racines carrées .....	15
1.2.6. Autres chapitres .....	15
1.3. Ne pas rêver avec la cryptographie quantique.....	16
1.4. Python pour le développement de systèmes cryptographiques par les élèves du secondaire 17	
<b>2. Cryptographie classique par substitution, ou transposition</b>	<b>23</b>
2.1. Frontière entre la cryptographie classique et la cryptographie moderne.....	23
2.2. Méthodes par substitution simple.....	23
2.2.1. Carré de Polybe (150 av. J.-C.).....	24
2.2.2. Chiffre de César, monoalphabétique (50 av. J.-C.).....	25
2.2.3. Chiffre des templiers (env. 1314), le plus trivial .....	25
2.2.4. Chiffrement affine ; mono-alphabétique [1.21] .....	25
2.2.5. Chiffre poly-alphabétique de Vigenère (1586) .....	26
2.2.6. Chiffre polyalphabétique de Lester Hill (1929) [2.3].....	27
2.2.7. Exercice : dénombrement du nombre de clés du chiffre de Hill.....	28
2.2.8. Chiffre de Delastelle (1902) [1.4].....	30
<b>3. Chiffrement par dictionnaires</b>	<b>33</b>
3.1. Cryptographie par dictionnaire ou par répertoires [1.37] .....	33
3.1.1. Grand chiffre de Paris (1750) .....	34
3.1.2. Petits chiffres .....	35
3.1.3. Grand chiffre de Napoléon (fin 1811) [3.8].....	35
3.1.4. Dictionnaire chiffré (Brachet, 1851) [3.4] .....	35
3.1.5. Dictionnaire télégraphique (H. Mamert-Gallian, 1874) [3.5].....	35
3.1.6. Dictionnaire (F. Airenti, 1893) [3.1].....	36
3.1.7. Dictionnaire (Étienne Bazeries, 1893) [1.2] [3.3] .....	36
3.1.8. Dictionnaire F.J. Sittler [3.6].....	37
3.1.9. Code Nilac [3.14].....	37
3.2. Ambiguïté du chiffrement et déchiffrement .....	37
3.3. Cryptanalyse du dictionnaire armée de 1877 qui est introuvable .....	37
<b>4. Méthodes de chiffrement par transposition</b>	<b>43</b>
4.1. Principe des méthodes par transposition.....	43
4.2. ScyTale ou bâton de Plutarque (en usage chez les spartiates).....	43

<b>4.3. Chiffre de Saknussem (<i>Voyage au centre de la terre</i> de Jules Verne).....</b>	<b>44</b>
<b>4.4. Chiffrement de transposition par grille .....</b>	<b>44</b>
4.4.1. Grille de Cardan [4.5] .....	44
4.4.2. Grille de Fleissner [4.4] .....	44
4.4.2.1. Chiffrement .....	45
4.4.2.2. Déchiffrement.....	46
<b>4.5. Chiffrement par carré latin (transposition et substitution) .....</b>	<b>46</b>
<b>4.6. Chiffrement par carré magique (transposition et substitution) .....</b>	<b>46</b>
<b>4.7. Chiffrement par transposition de colonne, le « chiffrement sans dictionnaire (S.D.) »</b>	
<b>de l'armée française en 1912 [4.2] .....</b>	<b>47</b>
4.7.1. Avantage militaire des méthodes par transposition de colonnes par rapport aux dictionnaires .....	47
4.7.2. Chiffrement .....	49
4.7.3. Déchiffrement .....	49
4.7.4. Cryptanalyse .....	50
<b>4.8. Substitution (Polybe) + transposition de colonnes : chiffre allemand ADFGVX</b>	
<b>de juin 1918.....</b>	<b>51</b>
4.8.1. Radiogramme de la victoire.....	51
4.8.2. Solution connaissant la clé de transposition et la clé du chiffrement de Polybe .....	53
<b>5. Machines cryptographiques .....</b>	<b>55</b>
<b>5.1. Cadrons chiffrants : disque Kronberg copié par l'armée mexicaine.....</b>	<b>55</b>
<b>5.2. Cylindres chiffrants (Jefferson, Bazeries) .....</b>	<b>56</b>
<b>5.3. Combinaison substitutions poly-alphabétiques (les rotors)</b>	
<b>et transpositions (le tableau de connexion) : machine ENIGMA.....</b>	<b>56</b>
5.3.1. Inventée pour les civils .....	56
5.3.2. Le fonctionnement d'Enigma .....	57
5.3.3. Nombre de clés possibles.....	60
5.3.4. Point forts et faiblesses .....	61
<b>6. Chiffrements modernes .....</b>	<b>63</b>
<b>6.1. Le RSA : chiffrement asymétrique clé publique-clé privée.....</b>	<b>63</b>
6.1.1. Principe des chiffrements asymétriques (clé publique-clé privée) .....	63
6.1.2. Création des clés, la publique et la clé privée.....	64
6.1.3. Chiffrement et déchiffrement RSA .....	66
6.1.3.1. Chiffrement des messages .....	66
6.1.3.2. Déchiffrement des messages .....	66
6.1.3.3. Exemple.....	66
6.1.4. Justification de la cryptographie RSA.....	67
6.1.4.1. Justification du déchiffrement par la clé privée de base.....	67
6.1.4.2. Justification du déchiffrement par les autres clés privées .....	68
6.1.5. Multiplicité des clés privées $d_i$ en RSA, cas de clés publiques « faibles ».....	69
6.1.6. Problème de la cryptanalyse du déchiffrement RSA, factorisation d'un grand entier .....	69
6.1.7. Exercices RSA pour la Terminale scientifique.....	70
6.1.7.1. Exercice avec la calculatrice Python autorisée .....	70
6.1.7.2. Exercice RSA avec calculs détaillés à la main .....	72
6.1.7.3. Exercice simple RSA de calcul de $p, q$ secrets.....	73
6.1.7.4. Premier exercice RSA utilisant le théorème des restes chinois.....	74
6.1.7.5. Deuxième exercice RSA utilisant le théorème des restes chinois.....	77
6.1.7.6. Exercice sur les corps finis pour le RSA sur les courbes elliptiques .....	78

<b>6.2. Chiffrements basés sur l'extraction d'une racine carrée dans <math>Z/pZ</math>.....</b>	<b>79</b>
6.2.1. Cryptographie et extraction de racines carrées .....	79
6.2.1.1. Crypto-système de Rabin [6.9].....	79
6.2.1.2. Chiffrement de Goldwasser-Micali [6.10] basé sur le symbole de Legendre .....	80
6.2.2. Le symbole de Legendre, outil de cryptographie .....	82
6.2.2.1. Le symbole de Legendre : propriétés pour la cryptographie.....	83
<b>6.3. Chiffrement symétrique par bloc (DES).....</b>	<b>84</b>
6.3.1. Le chiffrement par bloc.....	84
6.3.1.1. Ancienneté du chiffrement par bloc .....	84
6.3.1.2. Description du DES.....	85
6.3.1.3. Le Triple DES pour améliorer la sécurité.....	85
6.3.2. Utilisation du schéma de Feistel pour faire la permutation .....	86
6.3.2.1. Exercice (niveau Terminale) de cryptanalyse Feistel par paire clair-chiffré .....	86
6.3.2.2. Exercice dérivé de l'épreuve de sélection Alkindi 2018-2019.....	88
<b>7. Boîte à outils cryptographique classique en Python .....</b>	<b>93</b>
<b>7.1. Mode d'emploi de la boîte à outils.....</b>	<b>93</b>
<b>7.2. Algorithme d'Euclide étendu.....</b>	<b>95</b>
7.2.1. Code Python 3.....	95
7.2.2. Programme de test et contrôle .....	97
<b>7.3. Résolution de systèmes modulaires par le théorème chinois (Bac scientifique) .....</b>	<b>98</b>
7.3.1. Code Python 3.....	98
7.3.2. Programme de test et contrôle .....	99
<b>7.4. Chiffrement, déchiffrement et cryptanalyse de Vigenère (Bac scientifique) .....</b>	<b>99</b>
7.4.1. Code Python 3.....	99
7.4.2. Programme de test et contrôle .....	106
<b>7.5. Inverse d'une matrice M modulo 26 .....</b>	<b>107</b>
7.5.1. Code Python 3.....	107
7.5.2. Programme de test et utilisation pour des exercices Alkindi et le Bac .....	108
<b>7.6. Chiffrement-déchiffrement de Hill (Bac scientifique) .....</b>	<b>109</b>
7.6.1. Code Python 3.....	109
7.6.2. Programme de test et contrôle .....	112
<b>7.7. Programme de RSA, clés, chiffrement, déchiffrement (Bac scientifique).....</b>	<b>112</b>
7.7.1. Code Python 3.....	112
7.7.2. Test et contrôle.....	117
<b>7.8. RSA : calcul de la clé privée par le logarithme discret (rho de Pollard).....</b>	<b>118</b>
7.8.1. Code Python 3.....	119
7.8.2. Test du logarithme discret.....	120
<b>7.9. Cryptosystème de Rabin et algorithme de Tonelli-Shanks .....</b>	<b>120</b>
7.9.1. Code Python 3.....	121
7.9.2. Test de l'algorithme Tonelli-Shanks d'extraction des racines carrées dans $Z/pZ$ .....	125
<b>7.10. Corrigés inforMatiques de certaines épreuves Alkindi .....</b>	<b>126</b>
<b>8. Annales et corrigés du concours Alkindi 2020-2016 .....</b>	<b>127</b>
<b>8.1. Épreuve finale Paris, 13 mai 2020, exercice n° 1 .....</b>	<b>128</b>
8.1.1. Énoncé.....	128
8.1.2. Corrigé.....	128

<b>8.2. Épreuve finale Paris, 13 mai 2020, exercice n° 2</b> .....	<b>129</b>
8.2.1. Énoncé.....	129
8.2.2. Corrigé.....	130
8.2.3. Commentaires : solution générale comme chiffrement algébrique.....	131
<b>8.3. Épreuve finale Paris, 13 mai 2020, exercice n° 3</b> .....	<b>132</b>
8.3.1. Énoncé.....	132
8.3.2. Corrigé.....	133
8.3.3. Commentaires.....	135
<b>8.4. Épreuve finale Paris, 13 mai 2020, exercice n° 4</b> .....	<b>135</b>
8.4.1. Énoncé.....	135
8.4.2. Corrigé.....	136
8.4.3. Commentaires.....	138
<b>8.5. Épreuve finale Paris, 13 mai 2020, exercice n° 5</b> .....	<b>139</b>
8.5.1. Énoncé.....	139
8.5.2. Corrigé.....	140
<b>8.6. Épreuve finale Paris, 13 mai 2020, exercice n° 6</b> .....	<b>142</b>
8.6.1. Énoncé.....	142
8.6.2. Corrigé.....	144
8.6.3. Commentaire.....	145
<b>8.7. Épreuve finale Paris, 13 mai 2020, exercice n° 7</b> .....	<b>145</b>
8.7.1. Énoncé.....	145
8.7.2. Corrigé.....	146
8.7.3. Commentaires.....	147
<b>8.8. Épreuve finale Paris, 13 mai 2020, exercice n° 8</b> .....	<b>148</b>
8.8.1. Énoncé.....	148
8.8.2. Corrigé.....	148
<b>8.9. Épreuve finale Paris, 28 mai 2019, exercice n° 1</b> .....	<b>150</b>
8.9.1. Énoncé.....	150
8.9.2. Corrigé.....	151
8.9.3. Commentaires.....	151
<b>8.10. Épreuve finale Paris, 28 mai 2019, exercice n° 2</b> .....	<b>152</b>
8.10.1. Énoncé.....	152
8.10.2. Annexe de l'énoncé : dictionnaire chiffré de l'exercice.....	152
8.10.3. Corrigé.....	154
8.10.4. Commentaires.....	155
<b>8.11. Épreuve finale Paris, 28 mai 2019, exercice n° 3</b> .....	<b>155</b>
8.11.1. Énoncé.....	155
8.11.2. Corrigé.....	156
8.11.3. Commentaires et généralisation.....	158
<b>8.12. Épreuve finale Paris, 28 mai 2019, exercice n° 4</b> .....	<b>158</b>
8.12.1. Énoncé.....	158
8.12.2. Corrigé.....	159
8.12.3. Commentaires.....	163
<b>8.13. Épreuve finale Paris, 28 mai 2019, exercice n° 5</b> .....	<b>163</b>
8.13.1. Énoncé.....	163
8.13.3. Corrigé.....	164
8.13.4. Commentaires et généralisations.....	171
<b>8.14. Épreuve finale Paris, 28 mai 2019, exercice n° 6</b> .....	<b>171</b>
8.14.1. Énoncé.....	171

8.14.2. Corrigé.....	172
8.14.3. Commentaires.....	173
<b>8.15. Épreuve finale Paris, 28 mai 2019, exercice n° 7.....</b>	<b>174</b>
8.15.1. Énoncé.....	174
8.15.2. Corrigé.....	174
<b>8.16. Épreuve finale Paris, 16 mai 2018, exercice n° 1.....</b>	<b>175</b>
8.16.1. Énoncé.....	175
8.16.2. Corrigé.....	175
8.16.3. Commentaires sur l'exercice.....	176
<b>8.17. Épreuve finale Paris, 16 mai 2018, exercice n° 2.....</b>	<b>176</b>
8.17.1. Énoncé.....	176
8.17.2. Corrigé.....	177
8.17.3. Commentaires.....	178
<b>8.18. Épreuve finale Paris, 16 mai 2018, exercice n° 3.....</b>	<b>179</b>
8.18.1. Énoncé.....	179
8.18.2. Corrigé.....	180
8.18.3. Commentaires.....	182
<b>8.19. Épreuve finale Paris, 16 mai 2018, exercice n° 4.....</b>	<b>183</b>
8.19.1. Énoncé.....	183
8.19.2. Corrigé.....	184
8.19.3. Commentaires.....	188
<b>8.20. Épreuve finale Paris, 16 mai 2018, exercice n° 5.....</b>	<b>189</b>
8.20.1. Énoncé.....	189
8.20.2. Corrigé.....	190
8.20.3. Commentaires.....	191
<b>8.21. Épreuve finale Paris, 16 mai 2018, exercice n° 6.....</b>	<b>192</b>
8.21.1. Énoncé.....	192
8.21.2. Corrigé.....	193
8.21.3. Commentaires.....	197
<b>8.22. Épreuve finale Paris, 17 mai 2017, exercice n° 1.....</b>	<b>198</b>
8.22.1. Énoncé.....	198
8.22.2. Corrigé.....	199
8.22.3. Commentaires.....	199
<b>8.23. Épreuve finale Paris, 17 mai 2017, exercice n° 2.....</b>	<b>200</b>
8.23.1. Énoncé.....	200
8.23.2. Corrigé.....	200
8.23.3. Commentaires.....	202
<b>8.24. Épreuve finale Paris, 17 mai 2017, exercice n° 3.....</b>	<b>202</b>
8.24.1. Énoncé.....	202
8.24.2. Corrigé.....	203
8.24.3. Commentaires.....	203
<b>8.25. Épreuve finale Paris, 17 mai 2017, exercice n° 4.....</b>	<b>204</b>
8.25.1. Énoncé.....	204
8.25.2. Corrigé.....	205
8.25.3. Commentaires.....	205
<b>8.26. Épreuve finale Paris, 18 mai 2016, exercice n° 1.....</b>	<b>206</b>
8.26.1. Énoncé.....	206
8.26.2. Corrigé.....	207
8.26.3. Commentaires.....	207

<b>8.27. Épreuve finale Paris, 18 mai 2016, exercice n° 2</b> .....	<b>208</b>
8.27.1. Énoncé .....	208
8.27.2. Corrigé .....	208
8.27.3. Commentaires .....	210
<b>8.28. Épreuve finale Paris, 18 mai 2016, exercice n° 3</b> .....	<b>211</b>
8.28.1. Énoncé .....	211
8.28.2. Corrigé .....	212
8.28.3. Commentaires .....	212
<b>8.29. Épreuve finale Paris, 18 mai 2016, exercice n° 4</b> .....	<b>214</b>
8.29.1. Énoncé .....	214
8.29.2. Corrigé de R. Giuge .....	214
8.29.3. Commentaires .....	216
<b>9. Interception des communications sécurisées par RSA (HTTPS /TLS) avec un <i>Man-in-the-middle</i></b> .....	<b>221</b>
<hr/>	
<b>9.1. Interception des télécommunications</b> .....	<b>221</b>
<b>9.2. Attaques par reroutage vers un <i>Man-In-The-Middle</i>, mobiles et terminaux fixes [9.8]</b> .....	<b>223</b>
9.2.1. « Empoisonnement » ( <i>Poisoning</i> ) des DNS .....	223
9.2.2. Adresse IP des serveurs interceptés changée dynamiquement dans le réseau Internet mondial .....	225
9.2.3. Reroutage vers Man-In-The-Middle par IMSI et WiFi catchers des communications mobiles .....	226
<b>9.3. Principe et protection contre le reroutage par IMSI catchers des communications mobiles</b> .....	<b>227</b>
9.3.1. Protection contre les écoutes en 2G par des stations pirates .....	227
<b>9.4. Authentification des serveurs pour protection contre les MITM avec les certificats x509 délivrés par les Autorités de certification (AC)</b> .....	<b>228</b>
9.4.1. Authentification des serveurs basée sur les certificats X509 délivrés par les Autorités de certification .....	228
9.4.2. Installation des certificats dans le serveur (rôle du paramètre <i>Common Name</i> ) et chaîne de certificats dans les navigateurs .....	229
9.4.3. Fonctionnement de la vérification par le client des certificats d'un serveur .....	230
<b>9.5. Protection des communications par HTTPS/TLS/RSA</b> .....	<b>230</b>
9.5.1. Principe des systèmes de transmission sécurisée par clé publique-clé privée utilisés dans HTTP/TLS/RSA .....	231
9.5.2. Vérification du certificat SSL pour l'authenticité du serveur .....	233
9.5.3. Génération d'une clé de session " <i>Master Key</i> " (2 048 bits) pour le chiffrement RSA des données applicatives .....	234
9.5.4. Extension : certificat dans le client servant de signature à celui-ci .....	234
9.5.5. Pour les Travaux Pratiques informatiques : tracer les échanges sécurisés RSA avec un reverse-proxy .....	235
<b>9.6. Travaux pratiques : création d'un faux certificat serveur X509 pour un MITM</b> .....	<b>235</b>
9.6.1. Énoncé du sujet .....	235
9.6.2. Corrigé .....	237
<b>Abréviations et acronymes</b> .....	<b>245</b>
<hr/>	
<b>Index des abréviations et acronymes</b> .....	<b>249</b>
<hr/>	
<b>Index des noms propres</b> .....	<b>250</b>
<hr/>	