

AVANT-PROPOS

La cryptographie est une discipline très ancienne. Elle regagne en popularité avec les concours internationaux comme Alkindi [1.27] organisé par l'association Animath pour les classes de collège et lycée de la 4^e à la 2^{de} (70 000 candidats en 2020). Le concours comprend des épreuves qui sont inspirées pour certaines de la cryptanalyse de méthodes de chiffrements classiques datant de plus de 2000 ans : on trouvait ainsi le chiffrement de Polybe (150 av. J.-C.) comme un des sujets de l'épreuve finale 2016. Comme les Olympiades de mathématiques plus générales (classes de 4^e à 1^{re}), ce beau concours qui s'internationalise aide à révéler des talents, imaginations, cultures et vitesses qui pourront s'exprimer plus généralement dans les mathématiques appliquées. D'autres concours du niveau écoles d'ingénieur sont organisés depuis peu [1.46] comme TRACS.

Il y a abondance d'excellents ouvrages et de monographies consacrés à l'histoire de la cryptographie ou contenant un chapitre sur le sujet. On en trouvera à la fin de cette introduction, beaucoup plus complets que ce livre dont la partie historique est très brève et n'a aucune ambition de s'y comparer.

Le *premier objectif* du livre est de préparer les élèves du secondaire (4^e à Seconde) à la cryptographie et aux *épreuves de cryptographie du Bac scientifique* (quelques sujets depuis 2016). Pour la préparation du concours Alkindi par les enseignants et les candidats, le livre donne donc la presque intégralité des corrigés des épreuves finales 2016-2020 avec des commentaires sur les différentes autres approches ou pour restituer l'exercice dans le contexte historique des méthodes de chiffrement si cela est pertinent. C'est le chapitre 8. Les énoncés des exercices 2016 ont été revus sinon personne ne pouvait raisonnablement trouver la solution de l'exercice n° 4. Ce qui est nouveau, c'est de donner l'intégralité de ces corrigés commentés. *Pour le Bac* il y a des exercices basés sur ceux des années où la cryptographie est sortie (2016).

En classe de terminale scientifique les problèmes de codage (code-barres, code ISBN, code Insee) *sont au programme du Bac* ainsi que la cryptographie : chiffrement affine, Vigenère, Hill, chiffrement RSA). Il a semblé utile de donner des exercices adaptés à ce niveau [1.49], [1.50] donc supérieur à celui de Alkindi en rajoutant des exercices sur RSA qui fait partie des chiffrements modernes exclus en principe du plan (les autres chiffrements figuraient pour le concours Alkindi). Le programme 2020 comporte un cours d'arithmétique donnant les bases suffisantes (algorithme d'Euclide, petit théorème de Fermat, Lemme et Théorème chinois) pour le RSA et le chiffrement de Hill. Il y a aussi une introduction à la théorie des graphes et aux chaînes de Markov qu'on utilise en modélisation des langages dans le chapitre sur le chiffrement par dictionnaire ou dans Alkindi 2018 n° 3. Rester à un niveau de mathématiques assez élémentaire n'implique cependant pas que les exercices soient tous faciles, aussi bien ceux de Alkindi que ceux donnés pour les terminales scientifiques dans la nouvelle

option « maths expertes ». Les concours de crypto sont plus libres que les programmes du Bac et pourront porter sur d'autres chiffres classiques que ceux qui ont été précédemment évoqués, comme le montre la typologie des sujets :

Typologie des exercices de l'épreuve finale Alkindi 2016-2020

Chiffrement par substitution alphabétique mono ou polyalphabétique (Playfair, etc.)	9
Stéganographie (ou art de la dissimulation : ajouter des lettres de bourrage à un texte qui est en clair par ailleurs (2019 n° 3)	1
Machines cryptographiques diverses	5
Chiffrement simple par grille (pas de rotation)	5
Chiffrement affine, chiffrement algébrique (dont Hill)	3
Exploration de graphe (Séparation et Évaluation Progressive)	2
Farfelu (rien à voir avec une méthode classique, 2016 n° 4, 2019 n° 7, 2020 n° 8)	3
Partage de secret (2020 n° 6)	1

29

On peut ainsi s'étonner que certaines méthodes historiquement importantes comme celle de transposition de colonnes n'aient pas encore été clairement le sujet d'épreuves Alkindi (voir 2020 n° 8), malgré leur utilisation dans toutes les armées en 1914-1918, mais il y en a eu dans les épreuves de sélection. Le livre s'est donc aussi efforcé d'expliquer l'ensemble des méthodes historiques, commençant avec le carré de Polybe jusqu'aux méthodes modernes en cryptographie symétrique (le DES de 1970, la cryptographie asymétrique (RSA)) puisqu'elles pourraient être des sujets. On n'a pas traité les nombreux autres sujets de la période plus récente, signatures de messages, fonctions de hachage, preuves à divulgation nulles de connaissance, bien que rien ne garantisse que les auteurs des épreuves, redoutablement inventifs, ne cherchent pas dans ces sujets.

En France, heureusement, on estime qu'il n'y a pas de connaissance sans culture, et celle-ci commence par l'histoire (et la pratique de la géographie redécouverte du XIX^e siècle grâce à Vidal-Lablache et ses magnifiques cartes grand public, retard par rapport à l'Allemagne qui est probablement un autre facteur de la défaite de 1870 que la faiblesse du système de correspondance chiffrée de l'époque). Donner une histoire pratique de la cryptologie destinée aux personnes découvrant le sujet, enseignants ou candidats, en se limitant aux méthodes susceptibles de servir de thème à des épreuves de concours s'inscrit dans le premier objectif. On cherche à ce que le nom des grands cryptologues et leurs travaux soient ainsi connus. Soit dit en passant Al-Kindi [1.28] présenté comme le premier cryptologue n'a été découvert que récemment. Son nom ne figure dans aucun ouvrage de cryptologie classique, comme un du milieu du XIX^e siècle, celui du général italien Luigi Sacco [1.17], édition 1951, ou celui récent de Bauer [1.1] ; la notoriété assez soudaine d'Al-Kindi est venue avec l'influence croissante du courant de réattribution de découvertes européennes aux scientifiques d'Asie ou d'Afrique.

Le *deuxième objectif* du livre est de donner des exemples en langage Python pour la cryptographie, méthode utilisée par d'autres ouvrages thématiques pour apprendre Python comme [1.3], [1.15] en profitant de la motivation des lecteurs. On donne donc (Chapitre 7) une boîte à outils pratique de certains algorithmes en Python et des méthodes classiques de chiffrement-déchiffrement-cryptanalyse toutes faites. On y voit l'utilisation des listes et la façon de contourner l'impossibilité de modifier une *string* de caractères Python.

Dans le premier objectif, très large, on disait qu'on voulait « préparer à la cryptographie » et notamment selon le sens primitif, à déchiffrer les communications secrètes. Il faut donc aux futurs cryptologues un esprit pluridisciplinaire, pas seulement orienté vers les mathématiques. Cela fait appel à la compréhension des langues, et au déchiffrement spécifique des couches de *protocoles de télécommunications*.

Le *troisième objectif* est donc d'illustrer concrètement un aspect de la transversalité des disciplines utilisées en cryptographie, le déchiffrement du RSA est ainsi réalisable sans progrès sur la factorisation des entiers et la résolution du log discret. Des travaux sur ce thème trouvent donc place dans ce livre, en dernier chapitre il est vrai car le public est différent, ce sont des télécommunications et pour des spécialistes, mais bien expliqué à destination des professeurs de mathématiques, avec l'aide des schémas qui y sont inclus, il passionnera les élèves et les motivera pour continuer y compris dans le domaine professionnel des réseaux et de la cyber-sécurité passive ou active. Les transactions et messages étant presque essentiellement à travers un moyen de télécommunication, ce domaine doit obligatoirement être inclus. J'ai donc expliqué dans le dernier chapitre 9 des réalisations pratiques du fameux « *Man-in-the-middle* » pour l'interception des chiffrements asymétriques (RSA), le but étant de démystifier son impossibilité. En l'occurrence, on ne fait pas une attaque cryptanalytique, mais on utilise de faux certificats X509 [9.2] pour le protocole sécurisé HTTPS [9.1] d'accès à des serveurs ; ceci est évoqué comme possibilité par Stern [1.19] mais sans les détails de réalisation qui sont par contre fournis ici. Comme exemple pratique pour ce chapitre, on a traité dans la section 9.6 comme sujet de TP en classe de terminale scientifique le calcul comme le ferait une « Autorité de Certification », d'un vrai-faux certificat de serveur en utilisant les bibliothèques Python de crypto.

Cela montre que la sécurité du RSA repose sur la confiance dans ces « Autorités de Certification » qui délivrent les certificats de serveurs. Et que cela permettrait donc des attaques *protocolaires* et non pas *cryptologiques* réussies avec de « faux certificats à vrai nom de domaine », faites éventuellement par des autorités étatiques maîtres d'Internet, des PKI (*Public Key Infrastructure*) ou de l'émission de vrais-faux certificats. C'est un sujet qui n'est pas spécifiquement cryptologique, mais cela fait réfléchir sur le fait que certaines autorités étatiques, sans savoir résoudre le logarithme discret ou la factorisation des entiers, pourraient intercepter le RSA ou d'autres chiffrements à clé publique. Un futur cryptologue doit savoir que certains peuvent s'affranchir du respect des normes et même des lois au nom d'intérêts régaliens supérieurs.

Du même auteur

Mathématiques appliquées

[0.1] *Méthodes et Modèles de la Recherche Opérationnelle*, vol. 3 (avec Arnold Kaufmann), Dunod 1973, traductions anglaise *Integer and Mixed Programming*, Addison Wesley (1976), russe (MIR, 1975), espagnole (CCSA, 1975), roumaine (1976).

[0.2] *Exercices et Problèmes de Recherche Opérationnelle*, Masson, 1976.

[0.3] *Analyse de données*, Masson, 1976.

[0.4] *Recherche Opérationnelle*, Presses des Ponts et Chaussées, 1981.

[0.5] *Cours de Recherche Opérationnelle*, Presses des Ponts et Chaussées, 1995, vol. 1, « Programmation linéaire et non linéaire, théorie des graphes ».

[0.6] *Cours de Recherche Opérationnelle*, Presses des Ponts et Chaussées, 1995, vol. 2, « Contrôle optimal et optimisation en dimensions infinies, Théorie des jeux ».

Histoire navale

[0.7] *Les 4 couleurs du Surcouf*, AFHEMA, 2017.

Télécommunications

[0.8] *SMS and MMS interworking in Mobile Networks*, (avec Vincent Jonack), Artech Publishing House, 2004.

[0.9] *Virtual Roaming Systems for GSM, GPRS and UMTS*, Wiley, 2009.

[0.10] *Virtual Roaming Data Services and Seamless Technology Change*, River Publishers, 2014.

[0.11] *Cours d'interception et de protection des communications de mobiles*, PFPL, 2017.

[0.12] *Practical LTE Based Security Forces PMR Networks*, River Publishers, 2018.

TABLE DES MATIÈRES

Avant-propos	3
1. De la cryptographie classique à la cyber-sécurité moderne	13
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
2. Cryptographie classique par substitution, ou transposition	23
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
3. Chiffrement par dictionnaires	33
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
4. Méthodes de chiffrement par transposition	43
4.1. Principe des méthodes par transposition	43
4.2. ScyTale ou bâton de Plutarque (en usage chez les spartiates)	43

4.3. Chiffre de Saknussem (<i>Voyage au centre de la terre</i> de Jules Verne).....	44
4.4. Chiffrement de transposition par grille	44
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
4.5. Chiffrement par carré latin (transposition et substitution)	46
4.6. Chiffrement par carré magique (transposition et substitution)	46
4.7. Chiffrement par transposition de colonne, le « chiffrement sans dictionnaire (S.D.) »	
de l'armée française en 1912 [4.2]	47
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
4.8. Substitution (Polybe) + transposition de colonnes : chiffre allemand ADFGVX	
de juin 1918.....	51
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
5. Machines cryptographiques	55
5.1. Cadrons chiffrants : disque Kronberg copié par l'armée mexicaine.....	55
5.2. Cylindres chiffrants (Jefferson, Bazeries)	56
5.3. Combinaison substitutions poly-alphabétiques (les rotors)	
et transpositions (le tableau de connexion) : machine ENIGMA.....	56
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
6. Chiffrements modernes	63
6.1. Le RSA : chiffrement asymétrique clé publique-clé privée.....	63
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

6.2. Chiffrements basés sur l'extraction d'une racine carrée dans Z/pZ.....	79
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
6.3. Chiffrement symétrique par bloc (DES).....	84
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
7. Boîte à outils cryptographique classique en Python.....	93
7.1. Mode d'emploi de la boîte à outils.....	93
7.2. Algorithme d'Euclide étendu.....	95
7.2.1. Code Python 3.....	95
7.2.2. Programme de test et contrôle.....	97
7.3. Résolution de systèmes modulaires par le théorème chinois (Bac scientifique).....	98
7.3.1. Code Python 3.....	98
7.3.2. Programme de test et contrôle.....	99
7.4. Chiffrement, déchiffrement et cryptanalyse de Vigenère (Bac scientifique).....	99
7.4.1. Code Python 3.....	99
7.4.2. Programme de test et contrôle.....	106
7.5. Inverse d'une matrice M modulo 26.....	107
7.5.1. Code Python 3.....	107
7.5.2. Programme de test et utilisation pour des exercices Alkindi et le Bac.....	108
7.6. Chiffrement-déchiffrement de Hill (Bac scientifique).....	109
7.6.1. Code Python 3.....	109
7.6.2. Programme de test et contrôle.....	112
7.7. Programme de RSA, clés, chiffrement, déchiffrement (Bac scientifique).....	112
7.7.1. Code Python 3.....	112
7.7.2. Test et contrôle.....	117
7.8. RSA : calcul de la clé privée par le logarithme discret (rho de Pollard).....	118
7.8.1. Code Python 3.....	119
7.8.2. Test du logarithme discret.....	120
7.9. Cryptosystème de Rabin et algorithme de Tonelli-Shanks.....	120
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
7.10. Corrigés informatiques de certaines épreuves Alkindi.....	126
8. Annales et corrigés du concours Alkindi 2020-2016.....	127
8.1. Épreuve finale Paris, 13 mai 2020, exercice n° 1.....	128
8.1.1. Énoncé.....	128
8.1.2. Corrigé.....	128

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

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

8.27. Épreuve finale Paris, 18 mai 2016, exercice n° 2	208
8.27.1. Énoncé	208
8.27.2. Corrigé	208
8.27.3. Commentaires	210
8.28. Épreuve finale Paris, 18 mai 2016, exercice n° 3	211
8.28.1. Énoncé	211
8.28.2. Corrigé	212
8.28.3. Commentaires	212
8.29. Épreuve finale Paris, 18 mai 2016, exercice n° 4	214
8.29.1. Énoncé	214
8.29.2. Corrigé de R. Giuge	214
8.29.3. Commentaires	216
9. Interception des communications sécurisées par RSA (HTTPS /TLS) avec un <i>Man-in-the-middle</i>	221
<hr/>	
9.1. Interception des télécommunications	221
9.2. Attaques par reroutage vers un <i>Man-In-The-Middle</i>, mobiles et terminaux fixes [9.8]	223
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
9.3. Principe et protection contre le reroutage par IMSI catchers des communications mobiles	227
9.3.1. Protection contre les écoutes en 2G par des stations pirates	227
9.4. Authentification des serveurs pour protection contre les MITM avec les certificats x509 délivrés par les Autorités de certification (AC)	228
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
9.5. Protection des communications par HTTPS/TLS/RSA	230
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
9.6. Travaux pratiques : création d'un faux certificat serveur X509 pour un MITM	235
9.6.1. Énoncé du sujet	235
9.6.2. Corrigé	237
Abréviations et acronymes	245
<hr/>	
Index des abréviations et acronymes	249
<hr/>	
Index des noms propres	250
<hr/>	