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 4e à la 2de (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 4e à 1re), 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 (4e 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