**FICHES DU CLUB ALKINDI** **juillet 2021**
**FICHE n° 10**

# LIVRES, SITES INTERNET, FILMS ET SÉRIES

Si vous avez lu un livre de cryptographie ou découvert un site Internet intéressant, n'hésitez pas à partager votre opinion sur ce site afin que cela profite à tous.

## 1. LIVRES

***Histoires des codes secrets,* Simon Singh, Le Livre de Poche**

Ce livre est sans doute l'un des meilleurs, sinon le meilleur livre sur le sujet. Si vous n'achetez qu'un seul livre, achetez celui-là. Il présente une approche très historique et permet de bien comprendre les techniques de chiffrement et de déchiffrement de l'Antiquité jusqu'à notre époque moderne (le système RSA). L'auteur, Simon Singh, est docteur en physique nucléaire et journaliste scientifique en Grande-Bretagne. L'ouvrage est extrêmement clair, bien documenté, facile à lire, avec une approche très pédagogique. Autre avantage, c'est un Livre de Poche et il n'est pas cher .
Ce livre est un peu ancien (paru en 1999), mais reste une valeur très sûre.

***La Bible des codes secrets*, Hervé Lehning, Flammarion**

Un excellent livre également. L'auteur est professeur agrégé de mathématiques et il a une excellente pédagogie. Le récit est historique, comme il se doit, tout est très clair, bien expliqué, avec humour et avec des petits exercices (corrigés) qui permettent de bien comprendre et de s'entraîner à pratiquer. Ce livre est très complet et comme il est récent (novembre 2019), il aborde également dans ses derniers chapitres des sujets plus modernes : la protection du Wi-Fi, la sécurité des téléphones portables, les fonctions de hachage, la confidentialité des objets connectés etc.
Ce livre est un peu plus cher que le précédent puisque récent, mais il vaut largement le détour.

***Cryptographie classique, de la préparation du concours Alkindi aux épreuves du bac.***
**Arnaud Henry-Labordère, Éditions Ellipses**

Un livre intéressant dont le titre annonce clairement l'objet. L'auteur explique bien la nécessité de connaître les méthodes de cryptographie classiques et en donne de très nombreux exemples de l'Antiquité à la Première Guerre mondiale. Il traite également des machines cryptographiques et des chiffrements modernes : le RSA, le chiffrement symétrique par bloc (DES) ou d'autres modes de

chiffrements modernes assez complexes [j'ai pas tout compris :-) ]. Le livre est très dense, certains sujets sont traités de façon un peu résumée, mais ils peuvent être approfondis par ailleurs sur Internet. Un bon livre.

**À noter** : ce livre fournit également une « boîte à outils » de *petits programmes classiques en Python,* pour chiffrer et déchiffrer, niveau Bac scientifique, ainsi que *les Annales et corrigés de tous les exercices des épreuves finale du concours Alkindi de 2016 à 2020.*

***Codage et cryptographie,*** dans la collection « Le monde est MATHÉMATIQUE », écrit par Joan GOMEZ, éditions RBA.

Livre très intéressant qui traite également de façon complète l'aspect historique de la cryptographie. Il est publié dans une collection de livres consacrés aux mathématiques et de ce fait il est plutôt pour les « matheux », avec des éléments qui dépassent parfois un peu le programme de Seconde (calcul matriciel par exemple que l'on étudie en 1ère ES). L'accent est mis sur les méthodes modernes de chiffrement, le chapitre sur la machine Enigma et celui sur le système RSA sont très clairs. Un petit livre intéressant mais assez technique.

On ne peut évidemment pas citer une multitude de livres. Si il y a un livre qui vous a particulièrement intéressé, n'hésitez pas à en parler dans les commentaires.

## 2. SITES INTERNET

### - dcode.fr

Ce site vous permet de gagner énormément de temps, puisqu'il décrypte un message secret chiffré par un tableau de Vigenère ou par le code ADFGX en quelques dixièmes de seconde. Encore faut-il savoir, face à un message, de quel type de chiffrement il s'agit ?
D'où la nécessité de connaître un peu les principaux types de chiffrement. Le sujet a été évoqué dans la fiche de présentation (fiche n° 1).

Par aileurs, **dcode.fr** présente des articles forts intéressants qui traitent de nombreux sujets de cryptographie, de l'Antiquité à nos jours.

### - cryptoprograms.com

Site à peu près semblable à dcode.fr qui permet de chiffrer et de déchiffrer en anglais, en français et dans de nombreuses autres langues.

Il existe de nombreux sites Internet consacrés à a cryptographie, il suffit de taper « code secret » ou « cryptographie » sur Google. Laissez-vous le plaisir de les découvrir et n'hésitez pas à nous en parler.

## 3. APPLICATION Android pour téléphone mobile

### Cryptography – Collection of cyphers and hashes

Cette application est assez impressionnante. Elle propose un très grand nombre de modes de chiffrements et de déchiffrements, ainsi que des cours théoriques ! Elle a été créée à l'origine en anglais, mais s'adapte à la langue du téléphone, en l'occurrence le français pour nous.

Une application très sympa, à télécharger sur son téléphone sur Google Play Store ou sur :

https://play.google.com/store/apps/details?id=com.nitramite.cryptography

## 4. LES FILMS

### *Imitation Game* (2014, de Morten Tyldum)

*Imitation Game* raconte la vie du mathématicien anglais Alan Turing qui avec ses collaborateurs est parvenu à décrypter les messages de la machine Enigma à Bletchley Park, près de Londres, durant la Seconde Guerre mondiale (voir fiche n° 6).

L'acteur britannique Benedict Cumberbatch est remarquable dans le rôle du célèbre mathématicien. Il faut l'écouter bafouiller en interprétant ce personnage, timide, introverti, mal à l'aise en société, mais extrêmement intelligent. Bien sûr, le film est un peu romancé : Alan Turing n'était pas en opposition permanente avec ses supérieurs ni avec les membres de son équipe. Mais il faut bien pimenter un peu le récit, et la scène où le héros réalise par quel moyen il peut « casser » Enigma ne suffirait pas à elle toute seule à remplir le film, même si c'est l'un des moment fort et émouvant. De nombreux flash-backs permettent de mieux comprendre la vie d'Alan Turing et sa fin tragique .

Un très beau film, passionnant et agréable à voir.

## 5. LES SÉRIES

### *Le Bureau des Légendes*

Une série que ne traite pas spécifiquement de cryptographie, mais plutôt de certains aspects du travail de la DGSE. Elle comporte 5 saisons de 10 épisodes, et raconte la vie quotidienne d'agents de renseignement français à l'étranger et sur le territoire national.

Réalisée par Eric Rochant, cette série a été unanimement saluée par la critique française et internationale. Les scénarios des différentes saisons collent remarquablement bien à la réalité géopolitique des périodes concernées (2015 à 2020), comme par exemple la question de l'armement atomique de l'Iran, du ver informatique Stuxnet ou de la lutte contre l'État Islamique en Syrie et en Irak.

A certains moments, et spécialement dans la saison 4, on y découvre le travail des spécialistes des cyberattaques, qui nécessitent une très grande technicité. Les séquences de piratage de téléphones portables en Russie sont assez jubilatoires.

Attention : les scènes d'ouvertures de certains épisodes de la saison 5 sont un peu délicates pour des jeunes de moins de 13 / 14 ans.

*******
*****
***
*