50 MESSAGES CODÉS

Pour découvrir la cryptographie
en s'amusant !

Énigmathèque
www.enigmatheque.com

www.enigmatheque.com

ISBN : 979-8-3171-1669-9

Table des matières

Introduction

Mode d'emploi

Ce livre a vocation à vous initier à la cryptographie en vous proposant de déchiffrer 50 messages codés avec des techniques de chiffrement très diverses, classiques ou plus originales. Certaines de ces techniques datent de l'Antiquité et permettaient aux armées de l'époque d'échanger des messages en toute discrétion, sans que leurs ennemis ne puissent les comprendre. D'autres sont beaucoup plus modernes et toujours utilisées de nos jours, notamment pour chiffrer les communications sur internet et les transactions bancaires. Lorsque vous aurez déchiffré tous les messages codés de ce livre, vous aurez un bon aperçu de ce qu'est la cryptographie et maîtriserez un certain nombre de concepts mathématiques qui y sont liés. De plus, vous trouverez de nombreuses anecdotes historiques, ainsi que des photos et des documents d'archives qui accompagnent les énigmes.

Les énigmes proposées dans ce livre sont de difficulté variable. Les plus faciles d'entre elles sont indiquées par une étoile (*), celles de difficulté moyenne par deux étoiles (**) et les énigmes les plus difficiles par trois étoiles (***). Les trois premiers messages codés sont volontairement très simples à déchiffrer et ont pour but de vous faire découvrir des concepts qui seront utilisés tout au long du livre. D'autres messages seront plus difficiles à décoder, et certains feront appel à des notions de mathématiques de niveau lycée ou supérieur, mais tout en restant ludiques. Si vos cours de mathématiques sont enfouis loin dans votre mémoire, ou si vous n'êtes pas encore au lycée, ne vous inquiétez pas, toutes ces notions sont expliquées simplement et illustrées d'exemples dans les annexes à la fin de ce livre. De manière générale, n'hésitez pas à vous référer aux annexes, vous y trouverez de nombreuses informations utiles à la résolution des énigmes. Aussi, pour certains messages codés, il pourrait être pratique d'utiliser des outils informatiques tels qu'un tableur (Excel, Open Office Calc...), une calculatrice graphique (GeoGebra), ou encore créer vos propres scripts pour automatiser le déchiffrement, mais cela n'est évidemment pas une obligation. Pour vous éviter de recopier les messages codés à la main sur votre ordinateur, vous

pourrez les retrouver en scannant le code QR ci-dessous.

`www.enigmatheque.com/50-messages-codes`

Vous n'aurez alors plus qu'à entrer l'identifiant de l'énigme en question situé en pied de page et copier-coller le message codé dans votre logiciel préféré, ou télécharger le fichier associé. Toutes les énigmes sont indépendantes et peuvent donc être résolues dans l'ordre que vous souhaitez. Cependant, le livre comporte aussi plusieurs séries d'énigmes sous la forme de petites histoires qu'il est préférable de résoudre dans l'ordre afin de suivre le scénario.

Si vous rencontrez des difficultés sur une énigme, vous pouvez consulter les indices qui vous aideront certainement à prendre un bon départ ou à vous écarter de fausses pistes. Si malgré les indices vous ne parvenez toujours pas à résoudre une énigme, vous trouverez les solutions détaillées étape par étape dans le chapitre « Solutions ». Les numéros de page des indices et des solutions sont indiqués en bas à droite de chaque énigme. N'hésitez pas à lire les solutions détaillées, même après résolution d'une énigme, car elles sont souvent accompagnées d'anecdotes historiques et d'informations supplémentaires.

Un exemple de page d'énigme est présenté sur l'image suivante vous permettant de visualiser facilement les différents éléments qui la composent : le numéro de l'énigme à gauche, suivi de son titre de sa difficulté, ainsi que son identifiant à renseigner pour copier-coller ou télécharger le message, et les numéros de pages d'indices et de solution dans le pied de page. Les chapitres de ce livre sont facilement identifiables grâce à sa tranche colorée. Les pages d'énigmes sont repérées par une marge bleue, comme indiqué sur la page d'exemple, celles des indices par une marge violette, celles des solutions par une marge verte et celles des annexes par une marge orange.

Tout au long du livre, vous allez rencontrer et suivre les aventures de trois personnages clés, Ada, Charles et Alan. Vous en apprendrez plus sur ces trois amis dans le prochain paragraphe.

Numéro de l'énigme

Titre de l'énigme

Difficulté

#6 - Message d'Ada, Charles et Alan *

Après avoir déchiffré les 5 premiers messages de ce livre, vous recevez un message d'Ada, Charles et Alan. On dirait bien qu'ils souhaitent vous rencontrer... Parviendrez-vous à déchiffrer leur message ?

Message

De : Ada, Charles et Alan
À : Moi
Objet : Rencontre ?

Zgfpgwk,

Fgwl xtfgfl r'mhhktfrkt jwt ago mwllo aw a'ofatktllmol m sm ekbhagukmhiot, ta aw ml dtdt s'mok hswaga rgwt hgwk em ! Fgwl gkumfolgfl ktuwsotktdtfa rtl ktfegfaktl mwagwk rt sm ekbhagukmhiot, ta aw tl zotfxtfwt.
Lo aw lgwimoatl at pgofrkt m fgwl, ktakgwxt-fgwl et lgok mw emyt rtl mkaolatl m 21i.

M zotfaga !

Mrm, Eimkstl ta Msmf.

Marge colorée bleue indiquant qu'il s'agit d'une page d'énigme

Numéros de pages des indices et de la solution

Identifiant énigme : NPO6

Indices p.59 / Solution p.83

18

Identifiant de l'énigme à renseigner sur enigmatheque.com/50-messages-codes pour copier-coller le message codé

Qui sont Ada, Charles, et Alan?

Ada, Charles et Alan sont trois amis qui se sont rencontrés au cours de leurs études à Toulouse. Ils sont librement inspirés d'Ada Lovelace, de Charles Babbage et d'Alan Turing, qui sont des figures pionnières de l'informatique. Tous ces personnages vous sont présentés dans les encadrés suivants.

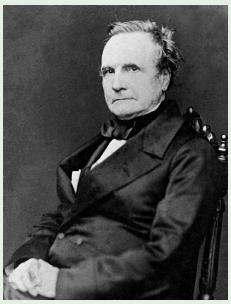
Ada

Ada a 20 ans, elle est d'origine anglaise et est arrivée en France il y a 5 ans. Elle est étudiante en troisième année de licence mathématiques à l'Université de Toulouse. Élève brillante, elle a un goût prononcé pour l'abstraction et la résolution de problèmes complexes. Son charmant accent anglais et ses fautes de français, bien qu'elles soient rares, font souvent rire Charles et Alan.

Ada Lovelace (1815–1852) est une femme de sciences anglaise. Enfant, elle reçoit une éducation scientifique et se passionne très vite pour les mathématiques. À l'âge de 17 ans, elle rencontre Charles Babbage et se fascine pour ses machines de calcul. Ada créé le premier véritable programme informatique, destiné à être exécuté par la « machine analytique » de Babbage. Elle est ainsi considérée comme la première programmeuse de l'histoire. Le langage de programmation Ada est d'ailleurs nommé ainsi en son honneur.

Charles

Charles a 21 ans, il est étudiant dans une école d'ingénieurs informatique toulousaine. C'est le bricoleur du groupe, il touche à tout, que ce soit de l'électronique, de la mécanique ou de l'informatique. Il est aussi amateur d'énigmes et de challenges de programmation en tout genre. Sportif, il pratique le football et le tennis en club depuis plus de 10 ans.



Charles Babbage (1791–1871) est un ingénieur et mathématicien britannique considéré comme l'un des précurseurs de l'informatique. Il est connu pour ses travaux sur les machines à calculer mécaniques destinées à améliorer la précision des tables nautiques et astronomiques. Il a travaillé avec Ada Lovelace sur sa « machine analytique », qu'il n'a jamais pu construire de son vivant car les technologies de l'époque étaient insuffisantes.

Alan

Alan a 22 ans, c'est le plus âgé du groupe. Il est en deuxième année de master mathématiques à Toulouse. Il est passionné d'échecs et de mots de croisés, activités qui occupent la plupart de ses week-ends. Sérieux et travailleur, il envisage de faire une thèse en cryptographie l'année prochaine. Alan est un ami de confiance, Charles et Ada savent qu'ils pourront compter sur lui en toutes circonstances.

Alan Turing (1912–1954) est un mathématicien, logicien et cryptologue anglais. Il est reconnu comme étant l'un des pionniers de l'informatique et de l'intelligence artificielle. Durant la Seconde Guerre mondiale, il a joué un rôle crucial dans le décryptage des messages allemands codés par la machine Enigma, ce qui a grandement contribué à la victoire des Alliés. Ses travaux fondamentaux sur les machines de Turing posent les bases conceptuelles de l'informatique moderne.

Un peu de vocabulaire

Voici quelques définitions autour de la cryptographie qui pourraient vous être utiles avant de commencer à résoudre les énigmes de ce livre.

• Cryptologie

La cryptologie, du grec kruptos (caché) et logie (science), est ce que l'on pourrait appeler la « science du secret ». Elle englobe la cryptographie et la cryptanalyse.

• Cryptographie

La cryptographie, éthymologiquement « écriture secrète », vise à protéger des informations, souvent à l'aide de clés de chiffrement, en les rendant inintelligibles pour toute personne ne possédant pas la clé. Les premières utilisations de la cryptographie remontent à l'Antiquité, avec par exemple le célèbre chiffre de César. Aujourd'hui, la cryptographie est omniprésente et sert notamment à sécuriser nos transactions bancaires ou nos informations personnelles sur internet.

• Cryptanalyse

La cryptanalyse est le nom donné à l'ensemble des techniques permettant de décrypter un message codé sans en connaître la clé de chiffrement.

• Chiffrement

Le chiffrement est le processus de transformation, à l'aide d'une clé, d'un message clair en un message incompréhensible pour quiconque ne disposant pas de la clé. Une méthode de chiffrement est dite symétrique si le chiffrement et le déchiffrement se font à partir de la même clé secrète. Par opposition au chiffrement symétrique, le chiffrement asymétrique nécessite une clé publique avec laquelle l'émetteur chiffre son message, et une clé privée avec laquelle le destinataire le déchiffre.

• Stéganographie

La stéganographie consiste à dissimuler une information dans un média d'apparence anodin comme une image, un son ou une vidéo. Elle se distingue de la cryptographie car ici l'information n'est pas cryptée. L'intérêt de la stéganographie est qu'un acteur extérieur ne peut se douter de la nature sensible de l'information cachée, ce qui n'est évidemment pas le cas lorsque celle-ci est chiffrée.

Énigmes

Vous vous sentez prêt(e) à faire vos premiers pas de cryptographe ? Alors lancez-vous dans l'aventure ! Et n'oubliez pas, pour certaines énigmes il va vous falloir faire preuve de logique, d'observation, et de patience... Ce sont les trois atouts indispensables à tout bon cryptographe !

Bonne chance !

#1 - Pour bien commencer 1 *

Les trois messages codés de la série « Pour bien commencer » sont particulièrement simples à déchiffrer et ont pour but de vous faire découvrir l'esprit du livre et la démarche à suivre pour les prochaines énigmes, qui seront bien sûr plus difficiles ! ;)

Ce premier message est assez court et peut être facilement déchiffré à la main...

1 8 4 13 9 14 20 4 !

Remarque

Les annexes de la page 146 peuvent éventuellement vous aider à déchiffrer ce premier message, et vous seront très utiles tout au long du livre...

Identifiant énigme : MKL1

Indice p.58 / Solution p.78

#2 - Pour bien commencer 2 *

Vous avez réussi à déchiffrer le premier message codé « Pour bien commencer 1 » ? Félicitations ! La petite subtilité de ce premier message est le fait que la lettre A soit codée par le chiffre 0, et non par 1 comme cela pourrait paraître plus naturel. Il est en effet d'usage en cryptographie d'utiliser la convention A=0,...,Z=25 pour des raisons mathématiques, et en particulier pour clarifier la notion de modulo qui sera abordée dès le troisième message codé de cette série tutorielle. Cette convention sera celle utilisée dans la majorité des énigmes de ce livre. Toutefois, pour certaines énigmes, la convention A=1,...,Z=26 sera aussi utilisée. Il vous faudra donc faire attention à ce point dans la suite.

Le deuxième message codé de ce livre est beaucoup plus long que le premier et peut s'avérer fastidieux à déchiffrer à la main. Lorsqu'un message est long, il est plus judicieux d'utiliser un outil informatique comme un tableur pour en automatiser le déchiffrement. Si vous aimez les défis informatiques, vous pouvez aussi créer votre propre script pour déchiffrer un message codé.

Essayez de déchiffrer le message suivant à l'aide d'un tableur ou d'un script pour automatiser la tâche. En fonction de la méthode que vous choisirez, vous aurez peut-être besoin de la table ASCII fournie en annexe à la page 166.

11 8 0 21 0 17 19 4 11 17 4 18 8 19 0 12 14 19 20 0
17 20 14 15 4 20 16 8 19 0 12 17 14 5 13 8 11 8 19
20 14 13 20 19 13 0 18 8 11 8 19 20 13 4 4 6 0
18 18 4 12 17 4 8 12 4 17 15 4 17 19 14 21 17 4
17 5 5 8 7 2 4 3 4 3 25 4 13 4 21 18 20 14 21
18 13 14 8 19 0 19 8 2 8 11 4 5

Remarque

Il n'est heureusement pas nécessaire de recopier ce message codé à la main sur votre ordinateur. Vous le retrouverez en scannant le code QR de la page 8 et n'aurez alors plus qu'à entrer l'identifiant de l'énigme ci-dessous pour copier-coller le message dans votre logiciel préféré et le déchiffrer.

Identifiant énigme : XFK2

Indices p.58 / Solution p.79

#3 - Pour bien commencer 3 *

Cette fois-ci, le message n'est plus codé par des chiffres mais par des lettres, comme la plupart des messages codés que vous rencontrerez dans ce livre. Parviendrez-vous à le déchiffrer ? Encore une fois, n'hésitez pas à vous aider d'un tableur ou à créer votre propre script pour automatiser le déchiffrement.

```
T+C I+G V+Z Y+U    A+A N+I B+D V+E    F+G   A+A E+I S+M
 B+C    M+I Y+P    A+C P+C N+L I+H Q+D T+V O+S J+I A+A
                      L+E C+F D+B.
   A+B M+C R+W T+U C+C    B+B F+C A+A J+E C+A B+D
 H+I U+U N+H J+I    T+S A+A    H+L J+L F+D Z+U M+S !
```

Remarque

Il est fort probable que vous ayez besoin de la notion de modulo pour déchiffrer ce message. Si vous n'avez jamais entendu parler de modulo, vous pouvez consulter la page 150 des annexes où cette notion est expliquée simplement et illustrée d'exemples. Les modulos sont très importants en cryptographie, vous les rencontrerez souvent dans ce livre...

Identifiant énigme : DOF3

Indices p.58 / Solution p.80