Pascal Lafourcade et Cristina Onete

20 ÉNIGMES LUDIQUES POUR SE PERFECTIONNER EN CRYPTOGRAPHIE

DUNOD

Découvrez aussi :

- P. Lafourcarde et M. More, *25 énigmes ludiques pour s'initier à la cryptographie*, Dunod, 2021.
- P. Lafourcarde et M. More, *15 énigmes ludiques pour s'initier à la programmation Python*, Dunod, 2022.
- J.-G. Dumas, P. Lafourcade, E. Roudeix, A. Tichit et S. Varrette, *Les NFT en 40 questions*, Dunod, 2022.
- J.-G. Dumas, P. Lafourcade, A. Tichit et S. Varrette, *Les blockchains en 50 questions*, 2e éd., Dunod, 2022.
- J.-G. Dumas, P. Lafourcade, P. Redon, *Architectures de sécurité pour Internet*, 2e éd., Dunod, 2020.
- J.-G. Dumas, J.-L. Roch, S. Varrette, E. Tannier, *Théorie des codes : Compression, cryptage, correction*, Dunod, 2018.
- D. Vergnaud, *Exercices et problèmes de cryptographie*, 4e éd. ? Dunod, 2023

Direction artistique : Nicolas Wiel

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-086333-4

Sommaire

Avant-propos

Où ira l'Amiral Yamamoto ? Monsieur Trompe trompe-t-il sa femme ? Jouer à Tetris, c'est de la cryptographie ?

De la confusion de Monsieur Confusious à la tromperie de Monsieur Trompe, du cas du SOS d'un activiste en danger à une partie de Tetris post-quantique et même à un télégramme de guerre, les 20 énigmes présentées dans ce livre permettent de découvrir en s'amusant des concepts importants de la cryptographie moderne. De l'astuce, de l'esprit d'observation, de la réflexion et de la créativité : mettez vos capacités en action pour découvrir des faiblesses, exploiter des failles avec des attaques, ou même pour trouver les solutions.

Pour les lecteurs qui ont déjà découvert le premier livre d'initiation à la cryptographie, vous voilà confrontés à des primitives cryptographiques plus évoluées et utilisées par les cryptographes.

La difficulté des énigmes est indiquée par des étoiles. Le niveau facile est représenté par ☆. Les énigmes de ce niveau sont accessibles à tous, moyennant parfois un peu de persévérance.

Le niveau intermédiaire est noté par ☆☆. Dans ces énigmes, la réflexion ou les calculs sont plus complexes, et il arrive que la solution repose sur une astuce un peu moins évidente que dans le premier niveau.

Le niveau ☆☆☆ est le niveau difficile. Il comporte des énigmes qui nécessitent beaucoup de réflexion ou qui demandent des connaissances en mathématiques et informatique un peu plus avancées.

Pour chaque énigme, il y a trois niveaux progressifs d'indices,proposés dans un chapitre au milieu du livre. Ainsi, si après avoir commencé à réfléchir, vous êtes bloqué, vous trouverez avec les indices une aide graduée pour vous donner un coup de pouce et vous mettre sur la piste de la solution.

Cette collection d'énigmes – un véritable trésor de petits mystères qui n'attendent que d'être résolus – s'adresse surtout à ceux qui aiment comprendre les principes de la cryptographie moderne. Si vous vous demandez comment marche la signature numérique, comment les données de santé peuvent être anonymisées, ou même si « crypter » est un mot du dictionnaire valide en cryptographie (non, il ne l'est pas) – vous retrouverez dans cet ouvrage des réponses

concrètes qui vous permettront de débuter de façon ludique dans un domaine d'actualité, indispensable dans la vie de tous les jours.

L'objectif de cet ouvrage est de proposer des énigmes dont la solution peut être simplement obtenue à l'aide d'un papier et d'un crayon. Ceci permet de bien comprendre les fonctionnements des concepts cryptographiques sous-jacents des énigmes. Ce livre s'adresse aussi, indirectement, à tous les enseignants, car ces énigmes constituent une banque d'exercices corrigés au même titre qu'un manuel de cours.

Les thèmes des énigmes sont l'occasion de débuter de nombreux concepts importants en sécurité et cryptographie. La plus grande partie de cet ouvrage est constituée des solutions détaillées de toutes les énigmes. Chaque solution contient non seulement la résolution de l'énigme, mais aussi des explications détaillées sur le concept cryptographique qui est illustré par chaque énigme. En guise de clin d'œil, chaque solution est accompagnée d'une citation scientifique ou littéraire en rapport avec l'énigme ou sa solution.

L'aspect ludique de cet ouvrage motivera sans aucun doute certains lecteurs à apprendre la cryptographie moderne et à faire preuve de créativité pour résoudre les énigmes.

Les énigmes, indices et solutions contiennent de encarts biographiques, historiques, techniques, mathématiques, culturels, de solution ou encore d'objectifs pédagogiques pour les enseignants en rapport avec les concepts abordés. Ils sont représentés respectivement par :

Remerciements : Nous remercions Cédric Lauradoux pour nous avoir aidés pour la création de ces énigmes. Nous adressons nos remerciements à Emmanuel Delay, Nicolas Desforets, Malika More, Lola-Bay Mallordy, Marianne Mognos, Charles Olivier-Anclin, Vegard Nossum et aux élèves de l'édition 2023 de MATHC2+ de Clermont-Ferrand pour leurs contributions à l'élaboration du contenu de ce livre. Nous exprimons également notre gratitude à Anne Le Duc pour ses commentaires et suggestions constructives et à Nicolas Wiel pour la couverture du livre.

Et bien sûr merci à vous, chers lecteurs !

Limoges et Clermont-Ferrand, le 25 août 2023.
Cristina Onete et Pascal Lafourcade *.

* Nous serons heureux de répondre à vos questions par email.

À mes grands-parents,
À mon fils,