Pascal Lafourcade et Cristina Onete

20 ÉNIGMES LUDIQUES POUR SE PERFECTIONNER EN CRYPTOGRAPHIE

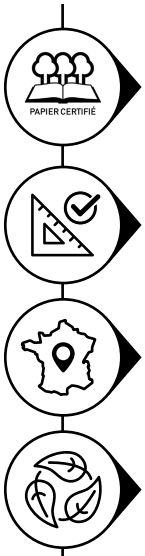
DUNOD

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

NOUS NOUS ENGAGEONS EN FAVEUR DE L'ENVIRONNEMENT :



Nos livres sont imprimés sur des papiers certifiés pour réduire notre impact sur l'environnement.

Le format de nos ouvrages est pensé afin d'optimiser l'utilisation du papier.

Depuis plus de 30 ans, nous imprimons 70% de nos livres en France et 25% en Europe et nous mettons tout en œuvre pour augmenter cet engagement auprès des imprimeurs français.

Nous limitons l'utilisation du plastique sur nos ouvrages (film sur les couvertures et les livres).

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-085511-7

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.

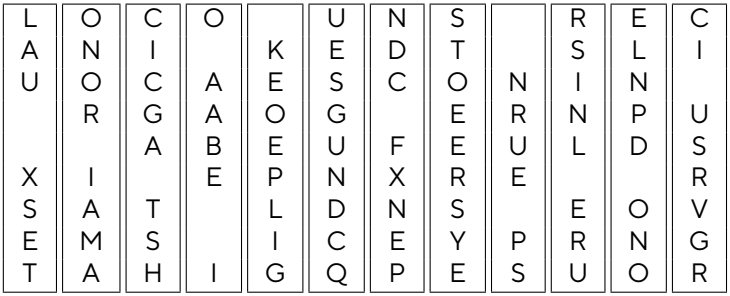
À mes grands-parents,
À mon fils,

1

Les énigmes à résoudre

1 Bandelettes ☆

Les douze bandelettes ci-dessous ont été retrouvées sur une scène de crime. Les policiers sur site sont intrigués et cherchent à trouver le message qui se cache derrière.



Énigme 1 : *Saurez-vous ordonner ces bandelettes pour aider la police à retrouver le texte écrit avec ces lettres ?*

Solution page 73.

2 Une démarche anonyme ☆

Une montre connectée mesure l'activité réalisée par semaine en nombre de kilomètres parcourus à pied. Elle possède un mécanisme de récompenses, qui encourage les utilisateurs à avoir une vie plus saine.

Le fournisseur veut démontrer l'efficacité de cette montre. Avec l'accord de ses clients, il se propose de publier des données (anonymisées) de ses clients et des statistiques qui montrent l'impact positif de son produit sur leur santé. Pour chaque utilisateur, l'entreprise stocke son nom, mais aussi : une tranche d'âge, le sexe, le département de résidence, le revenu par an et le nombre de kilomètres parcourus par semaine dans les cinq premières semaines.

Pour anonymiser la base de données, il faut d'abord enlever les noms des clients, ce qui donne une base de données au format suivant :

Âge	Sexe	Département	Salaire	Nombre km/semaine
40-50	H	23	57 000	12, 13, 13, 15, 14
20-30	H	35	22 000	20, 20, 15, 25, 22
20-30	H	75	25 000	13, 15, 15, 18, 20
30-40	F	75	42 000	25, 28, 30, 30, 32

Est-ce que les données sont anonymisées ? Difficile à dire !

Par exemple si un attaquant connaît une femme qui utilise sa montre, alors avec les entrées de la base de données ci-dessus, il aura directement une information sensible sur elle, notamment son revenu. Un attaquant qui connaît une personne dans le département 23 (Creuse) qui utilise cette montre pourra directement déduire son revenu.

Par conséquent, pour la publication des données, le fournisseur veut garantir le 3-anonymat (un cas particulier du k-anonymat) pour l'âge, le sexe et le département de résidence : chaque valeur de chacun de ces attributs devra apparaître au moins 3 fois.

k-anonymat

En 1998, Pierangela Samarati et Latanya Sweeney tentent de trouver une réponse à la question de recherche suivante : *dans le contexte d'une analyse sur des données sensibles de certains utilisateurs, est-il possible d'anonymiser l'ensemble des données traitées de telle façon que les utilisateurs restent anonymes, mais que l'analyse sur les données anonymisées reste utile ?*
Les deux chercheuses ont répondu à cette question par l'affirmative : elles ont avancé l'idée de trouver les attributs sensibles qui peuvent identifier un utilisateur, des plus identifiants (comme les nom, prénom ou numéro de Sécurité sociale) aux plus vagues (comme la religion, l'âge, le code postal, etc.) – et ensuite de s'assurer que, sur l'ensemble de données, chaque attribut apparaît au minimum *k* fois. Plus la valeur de *k* est élevée, plus l'anonymat est garanti par les données.

Si les attributs identifiants des données sont l'âge, le département et le sexe, alors l'ensemble de données publiées devrait comporter au minimum *k* fois la même tranche d'âge, le même département et le même sexe. Les données de la figure 1 assurent le 3-anonymat, mais pas le 4-anonymat (car il n'y a que 3 occurrences de chaque département, par exemple).

Âge	Sexe	Département	Salaire	Nombre km/semaine
40-50	H	23	57 000	12, 13, 13, 15, 14
30-40	F	75	42 000	25, 28, 30, 30, 32
20-30	H	35	22 000	20, 20, 15, 25, 22
30-40	F	35	27 000	20, 22, 22, 25, 23
20-30	H	75	25 000	13, 15, 15, 18, 20
40-50	F	35	57 000	15, 14, 17, 0, 1
30-40	H	23	57 000	12, 13, 13, 15, 14
40-50	H	75	30 000	6, 6, 7, 6, 8
20-30	F	23	33 000	20, 24, 24, 30, 28

Figure 1 – Base de données 3-anonyme.

Le fournisseur de montres est satisfait de l'extrait de sa base de données. Elle a désormais au moins 3 participants dans chaque tranche d'âge, il y a au moins 3 participants de chaque sexe, et chacun des 3 départements apparaît 3 fois.

Énigme 2 : *Le fournisseur montre sa base de données à un ami cryptographe qui habite la Bretagne. Sa question : la base de données est-elle suffisamment anonymisée ? Son ami regarde… et déclare avoir directement reconnu une voisine, qui s'était cassé la jambe récemment et qui ne s'était toujours pas remise de son accident.*

Quel est le revenu de la voisine en question ?

Solution page 81.

Le défi Snake #1

En mai 2023, un défi a été lancé par un trio de chercheurs français : Louis Béziaud, Tristan Allard et Sébastien Gambs. Ils ont ouvert une compétition sur des algorithmes qui génèrent des données anonymisées à partir d'un ensemble de données. Dans la vraie vie, ces données pourraient appartenir à un hôpital ou à une caisse d'assurances. Pour réaliser des statistiques sur ces données sensibles, il faut bien entendu les anonymiser avant de les utiliser.
Le défi Snake est de trouver des corrélations entre les données – c'est-à-dire des faiblesses dans les algorithmes d'anonymisation. Les participants ont accès à l'ensemble de données que l'algorithme a reçu en entrée, l'ensemble généré par l'algorithme, la paramétrisation des paramètres spécifiques à l'algorithme utilisé et un nombre de cibles. Le but est d'indiquer la probabilité que certaines cibles se trouvent dans l'ensemble de sortie de l'algorithme ou non.
La compétition se trouve en ligne [*].

[*] https://www.codabench.org/competitions/879/