Pascal Lafourcade et Malika More

25 ÉNIGMES LUDIQUES POUR S'INITIER À LA CRYPTOGRAPHIE

2e édition

DUNOD

Découvrez aussi :

P. Lafourcarde et C. Onete, *20 énigmes ludiques pour se perfectionner en cryptographie*, Dunod, 2023.
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
Graphisme de couverture : Pierre-André Gualino

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-086620-5

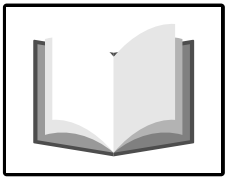

Table des matières

Avant-propos

Ces 25 énigmes sont des challenges que nous vous proposons pour vous faire découvrir des concepts importants de la cryptographie en vous amusant. Cette nouvelle édition contient trois nouvelles énigmes qui ont remplacé trois des énigmes les plus classiques. Les énigmes nécessitent plus ou moins de logique, de réflexion et d'astuce. Cependant, elles sont toutes accessibles à l'aide d'outils mathématiques abordés au lycée et ne demandent *a priori* pas de connaissances particulières en cryptographie ni en sécurité informatique.

Pour chaque énigme, nous avons conçu trois niveaux progressifs d'indices, qui se trouvent dans un chapitre séparé. 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.

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 de la fin du lycée. Ces énigmes de niveau ⋆⋆⋆ se rapprochent du fonctionnement des challenges de hacking (CTF [*]).

Enfin, une énigme bien plus difficile que les autres a été notée ⋆⋆⋆⋆. Elle consiste en effet à démontrer un résultat surprenant et important en sécurité informatique. Les trois indices seront-ils suffisants pour permettre aux lecteurs les plus habiles de la résoudre ?

Ces 25 énigmes visent à introduire des concepts de cryptographie ou de sécurité informatique. Les thèmes des énigmes abordent des chiffrements historiques, des chiffrements modernes, mais aussi les attaques par canaux cachés et les principes de la cryptomonnaie Bitcoin.

[*] Capture The Flag

La plus grande partie de cet ouvrage est constituée des solutions détaillées de toutes les énigmes. En guise de clin d'œil, chaque solution est accompagnée d'une citation scientifique ou littéraire en rapport avec le thème de l'énigme ou sa solution.

Les énigmes, indices et solutions contiennent de nombreux encarts biographiques, historiques, techniques, mathématiques ou culturels en rapport avec le concept présenté. Ils sont représentés respectivement par :

Enfin, ces énigmes s'inscrivent dans la démarche de l'*Informatique Sans Ordinateur*, initiée par *Computer Science Unplugged*[#], qui vise à proposer des activités ludiques, réalisables sans ordinateur, pour découvrir des concepts de la science informatique. Elles sont issues de plusieurs années d'expérimentations, à l'occasion d'activités de diffusion de la culture scientifique, auprès d'élèves du CM2 à la terminale, d'étudiants, d'enseignants et du grand public.

Remerciements : Nous remercions Cédric Lauradoux pour nous avoir montré la voie pour la création de ces énigmes. Nous adressons aussi nos remerciements à Guenaëlle De Julis, Emmanuel Delay et Matthieu Giraud pour leurs contributions à l'élaboration du contenu de ce livre. De plus, nous exprimons également notre gratitude à Flavien Binet, Jean-Luc Blanc, Olivier Blazy, Orel Cosseron, Daniel Matthieu, Colette More, Benoît Petitcollot, Maxine Pouzet, Garance Pautot, Léo Robert, Elias Tahhan-Bittar et Christel Tahhan-Doumat pour leurs commentaires et suggestions constructives, à la suite de leurs relectures assidues.

Clermont-Ferrand, le 4 août 2024.
Malika More et Pascal Lafourcade[†].

[#] https://csunplugged.org/

[†] Nous serons heureux de répondre à vos questions par email.

Depuis toujours, des groupes cachés utilisent des codes,
saurez-vous les percer ?

1

Les énigmes à résoudre

Un message dans le texte

★

1

Le principe de la stéganographie est de cacher un message ou un mot comme le ferait un habile magicien avec un objet. Et ainsi faire croire que la réalité n'est pas ce qu'elle est. Pour cela, le magicien envoie un message au spectateur pour détourner son attention de l'objet caché qu'il ne doit pas voir, par exemple un lapin dans son chapeau ou une colombe dans sa manche. Dans cette prestidigitation comme en stéganographie le secret de l'énigme réside dans l'art de dissimuler les choses.

Énigme 1 : *Ce texte cache un message secret, saurez-vous le découvrir ?*

Solution page 81.

Stéganographie

Cette énigme illustre la différence entre cryptographie et stéganographie. La *stéganographie*, du grec ancien *steganós* (*couvert, qui ne laisse rien dépasser*) et *graphein* (*écrire*), signifie que *le message secret est juste dissimulé, mais reste lisible* par toute personne qui sait comment le trouver. Par opposition, *en cryptographie*, qui vient aussi du grec ancien *kruptos* (*caché*) et *graphein* (*écrire*), le message secret n'est pas directement accessible : *pour pouvoir le lire, le destinataire doit effectuer une transformation* plus ou moins complexe en fonction des garanties de sécurité souhaitées.

1 JAN Hérodote (484-445 avant J.-C.)

Hérodote (voir figure 1) est considéré comme le premier historien. Dans ses ouvrages, il relate deux techniques de stéganographie :

- dans le Livre VII au paragraphe 239, il écrit que Démarate envoie un message caché à Xerxès. Le message est d'abord écrit sur une planchette de bois, puis recouvert de cire pour que la tablette semble être vierge et ainsi pouvoir la transmettre en toute discrétion ;
- dans le Livre V au paragraphe 35, Hérodote indique que Histiée utilise un esclave pour transmettre un message à son gendre Aristagoras. Il rase la tête de l'esclave, lui tatoue le messsage sur la peau du crâne, et attend que ses cheveux repoussent. Ensuite, il l'envoie à Aristagoras, qui n'aura plus qu'à lui raser la tête de nouveau pour accéder au message. L'esclave peut ainsi faire passer en toute sécurité le message de son maître à travers les lignes ennemies.

Dans ces deux exemples, les messages secrets sont dissimulés à la vue des indésirables, mais ils restent lisibles par toute personne qui sait comment les trouver.

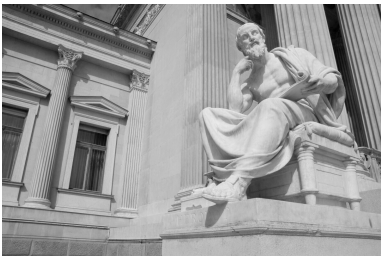

Figure 1 – Hérodote.

Un autre exemple de dissimulation des messages secrets, bien connu et simple à réaliser à la maison, est l'utilisation d'*encre invisible*, aussi appelée *encre sympathique*. Cette technique était déjà employée au premier siècle avant J.-C., comme le décrit Pline l'Ancien dans ses textes. Pour cela, il suffit d'écrire sur un rouleau de papyrus (une feuille de papier blanche fait aussi l'affaire) avec du lait de l'euphorbe tithymallus (le jus de citron fonctionne aussi). Une fois que le message a séché, la feuille est comme vierge et le texte est dissimulé. Pour révéler le texte, il suffit de chauffer légèrement la feuille à l'aide de la flamme d'une lampe à huile (ou à l'aide d'un fer à repasser). La chaleur va faire apparaître comme par magie le message écrit en marron.

2 Enigma

Figure 2 – Machine Enigma.

Enigma est une machine de chiffrement électromécanique utilisée pendant la Seconde Guerre mondiale par les Allemands pour communiquer de manière sécurisée. Inventée par Arthur Scherbius en 1923, plusieurs variantes de la machine ont par la suite été commercialisées.

Une de ses versions militaires est constituée des sept éléments suivants :

Clavier : un clavier des 26 lettres de l'alphabet, pour saisir le message à chiffrer [#].

Clavier lumineux : un clavier lumineux des 26 lettres de l'alphabet, sur lequel les lettres obtenues par chiffrement de chaque lettre du message s'allument tour à tour.

Tableau de connexions : un ensemble de 26 trous, sur le devant de la machine, représentant les lettres de l'alphabet et permettant de les relier deux à deux par un câble. La position de ces câbles est un des éléments de la clé de chiffrement utilisée par la machine Enigma : deux lettres reliées sont permutées.

Trois rotors : la machine utilise trois rotors, aussi appelés rouleaux ou tambours situés à droite, au milieu et à gauche. Un rotor est un disque opérant une substitution, chaque lettre de l'alphabet est ainsi remplacée par une autre lettre. Il y a cinq rotors différents, numérotés de I à V, qui peuvent être placés indifféremment. La clé de chiffrement contient les numéros des rotors à utiliser, ainsi que leur position initiale dans la machine. Cette position initiale est importante, car Enigma est un chiffre-

[#] En cryptographie, ce verbe possède un sens technique particulier qui n'est pas le même que le sens commun. Il signifie transformer un message clair, à l'aide d'un algorithme de chiffrement et d'une clé, pour le rendre incompréhensible, à moins de disposer de la clé secrète de déchiffrement.

ment polyalphabétique, c'est-à-dire que deux chiffrements d'une même lettre ne donnent pas le même résultat en raison de la rotation des rotors. Le rotor de droite tourne d'un cran après chaque relâchement d'une touche du clavier, le rotor du milieu tourne d'un cran toutes les 26 lettres, et le rotor de gauche tourne d'un cran toutes les $26^2 = 676$ lettres. Bien entendu, la lettre suivant *Z* est *A*.

Réflecteur : un réflecteur (rotor d'inversion) qui, comme les rotors, applique une substitution, mais sans rotation (il reste toujours dans la même position). Trois réflecteurs différents sont disponibles.

Comme l'illustre la figure 3, le chiffrement d'une lettre passe par le tableau de connexions, par les 3 rotors de droite à gauche, puis par le réflecteur. Ensuite, le signal repasse dans les rotors, cette fois de gauche à droite, et enfin, de nouveau par le tableau de connexions. Sur le schéma du haut il est clair que la lettre *A* est chiffrée par *G*. Sur le schéma du bas, le rotor de droite a tourné d'un cran vers le bas, et cette fois, la lettre suivante, qui est de nouveau *A* est chiffrée par *M*.

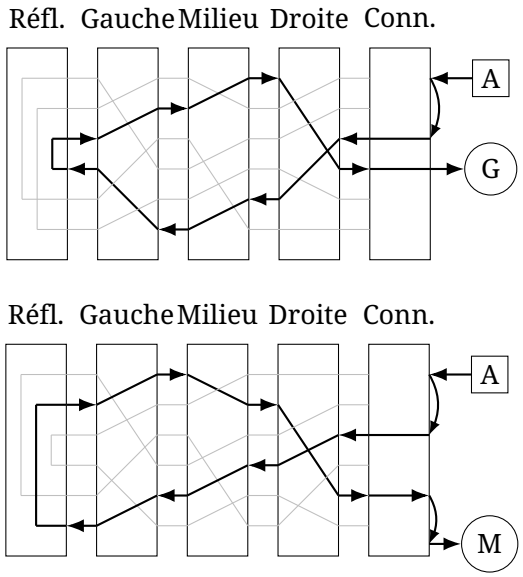

Figure 3 – Fonctionnement d'Enigma.

Énigme 2 : *Dans cette énigme, une machine Enigma simplifiée constituée d'un seul rotor est utilisée. Elle est représentée sur la figure 4 : la roue inté-*

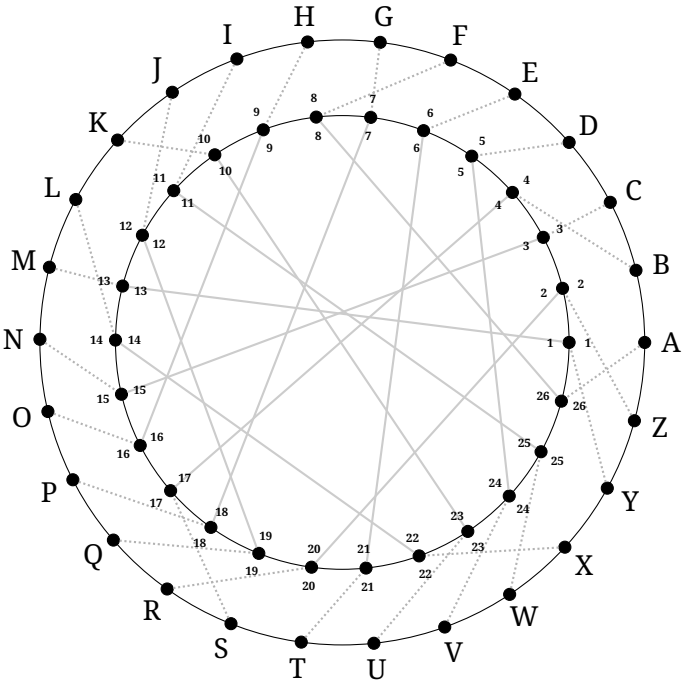

Figure 4 – Machine Enigma simplifiée.

rieure peut tourner, tandis que la roue extérieure est fixe. Chaque lettre de l'alphabet est associée à une autre en suivant les traits pointillés et pleins. Pour chiffrer un message, il faut d'abord régler la roue intérieure dans la position initiale pour chiffrer la première lettre, puis la tourner d'un cran dans le sens inverse des aiguilles d'une montre après avoir chiffré chaque lettre.

Saurez-vous déchiffrer le message ci-dessous ?

GQJJLVQUGOMMRZZXSXZQJOBXGMIDYJPAQKGC

Voici un indice : le message clair commence par LA*.*

Solution page 83.

Cryptanalyse d'Enigma

L'armée allemande utilise des machines Enigma à partir de 1926, au grand désarroi des services de renseignements des autres pays, en particulier la France, le Royaume-Uni et la Pologne. La difficulté résidait dans le très grand nombre de clés possibles changées chaque jour, en plus des parasites qui brouillaient les écoutes des espions. Cependant, par l'intermédiaire d'un agent français, les polonais obtiennent en 1931, d'un employé du bureau du chiffre de Berlin, les plans de l'Enigma allemande, à cette époque plus simple que la version présentée au début de l'énigme.
Au bout d'une année de travail acharné, trois mathématiciens polonais, Marian Rejewski, Jerzy Różycki et Henryk Zygalski, exploitant ces plans et des failles dans la mise en œuvre du chiffrement, et réussissent la cryptanalyse. Concrètement, il s'agissait de trouver le réglage des différents rotors, le même un jour donné pour toutes les machines, mais modifié tous les jours. Les messages militaires allemands sont ainsi décryptés pendant plusieurs années. Par la suite, Marian Rejewski construit une machine électromécanique, appelée *Bombe*, pour réaliser ces calculs plus rapidement et faire face à une nouvelle version, plus sophistiquée, d'Enigma.

Figure 5 – National Museum of Computing à Bletchley Park.

Malheureusement, en 1939, quand la guerre éclate et que la Pologne est envahie, l'Allemagne dispose d'une nouvelle version d'Enigma (celle présentée au début de l'énigme), qui met la Bombe en échec. Cependant, les deux machines Enigma reconstruites à partir des plans obtenus par le renseignement français et les schémas de la Bombe de Rejewski sont transmis *in extremis* au Royaume-Uni. C'est dans l'immense centre de recherches secret de Bletchley Park en Angleterre (plus de sept mille personnes en 1945), aujourd'hui devenu un musée (voir figure 5), que des scientifiques et des ingénieurs reprennent ses travaux. Malheureusement, pendant de longs