Pascal Lafourcade et Malika More

25 ÉNIGMES LUDIQUES POUR S'INITIER À LA CRYPTOGRAPHIE

DUNOD

Découvrez aussi :

- J.-G. Dumas, P. Lafourcade, A. Tichit et S. Varrette, *Les blockchains en 50 questions – Comprendre le fonctionnement et les enjeux de cette technologie*, Dunod, 2019.
- J.-G. Dumas, P. Lafourcade, P. Redon, *Architectures de sécurité pour internet – Protocoles, standards et déploiement*, Dunod, 2020.
- J.-G. Dumas, J.-L. Roch, S. Varrette, E. Tannier, *Théorie des codes – Compression, cryptage, correction*, Dunod, 2018.
- S. Ghernaouti, *Cybersécurité – Analyser les risques, mettre en œuvre les solutions*, Dunod, 2019.
- D. Vergnaud, *Exercices et problèmes de cryptographie*, Dunod, 2018.

Direction artistique : Élisabeth Hébert
Graphisme de couverture : Pierre-André Gualino

© Dunod, 2021
11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-082430-4

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. Elles 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 mode CTF *, qui est le mode de fonctionnement des challenges de hacking.

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. Nous commençons par les énigmes dont les notions sous-jacentes sont les plus anciennes, remontant parfois à l'Antiquité. Cependant, seules six des vingt-cinq énigmes sont datées d'avant 1945. Ainsi, la majorité des énigmes de cet ouvrage portent sur des idées apparues après les débuts de

* Capture The Flag

l'informatique [♯] en 1946 et ceux d'Internet [†] en 1969. 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.

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 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 :

En fin d'ouvrage, un glossaire explicite les termes techniques importants introduits tout au long du texte.

Enfin, ces énigmes sont issues de 50 énigmes cryptographiques en ligne [‡]. Elles 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, Colette More, Benoît Petitcollot, Maxine Pouzet, 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 24 mars 2021.
Malika More et Pascal Lafourcade [⋆].

[♯] Le premier ordinateur entièrement électronique, a été construit en 1946 par Presper Eckert et John William Mauchly. Il s'appele ENIAC pour *Electronic Numerical Integrator and Computer*.

[†] Le 2 septembre 1969, Len Kleinrock, Stephen Crocker et Vinton Cerf ont, pour la première fois de l'Histoire, réussi à échanger des données entre deux ordinateurs reliés par un câble. C'est ce qui a permis par la suite de créér le réseau Arpanet, ancêtre d'Internet.

[‡] `https://sancy.iut-clermont.uca.fr/~lafourcade/mission-crypto.html`

[⸸] `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

1 Un message dans le texte ☆

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 ?*

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 simplement 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 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.

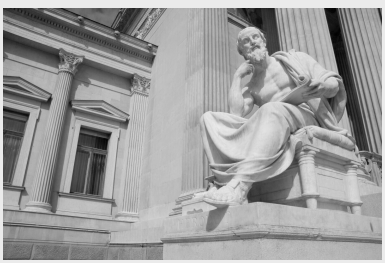


Figure 1 – Hérodote.

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 Les secrets de Jules ☆

Énigme 2 : *Dans la cave d'un bâtiment de l'U.S. Navy, des brouillons de lettres, certaines chiffrées et d'autres en clair, ont été retrouvés dans un vieux carton. À l'aide la lettre de la figure 2, saurez-vous décrypter celle de la figure 3 ?*

Le 26 avril 1942 à Washington D.C.,

À qui de droit,
J'ai fait des découvertes importantes sur la cryptanalyse de la machine ENIGMA. J'ai utilisé mes connaisances en cryptographie antique pour protéger mes travaux des curieux, mais je n'ai aucun doute qu'un expert en cryptographie saura y accéder.

Elizebeth Smith Friedman.

Post-Scriptum : Portez ce vieux whisky au juge blond qui fume.

Figure 2 – Un brouillon en clair retrouvé dans la cave.

Oh 28 dyulo 1942 d Zdvklqjwrq G.F.,

D txl gh gurlw,
Pd ghfrxyhuwh sruwh vxu od vwuxfwxuh gh od pdfklqh HQLJPD. Hooh shuphw gh idluh ghv vxffhvvlrqv gh vxevwlwxwlrqv hw gh shupxwdwlrqv. M'dl dxvvl o'lpsuhvvlrq txh od vwuxfwxuh ghv phvvdjhv hfkdqjhv hvw vrxyhqw od phph, fh txh qrxv doorqv hvvdbhu g'hasorlwhu.

Holchehwk Vplwk lulhgpdq.

Srvw-Vfulswxp : Sruwhc fh ylhxa zklvnb dx mxjh eorqg txl ixph.

Figure 3 – Un brouillon chiffré retrouvé dans la cave.

1 JAN ENIGMA

Figure 4 – Machine ENIGMA.

Avant la création de machines électromécaniques, les chiffrements étaient réalisés à la main par des personnes instruites qui savaient écrire. Avec les progrès de la mécanique, des machines à chiffrer utilisant des roues et des engrenages, et plus tard l'électricité, ont été fabriquées. Une des plus célèbres est la machine ENIGMA, utilisée par l'armée allemande durant la Seconde Guerre mondiale. De nos jours, les chiffrements sont effectués de manière électronique : par exemple, les serveurs des sites internet en https * (voir page 155) chiffrent l'ensemble des communications de façon transparente pour les utilisateurs.

* HyperText Transfer Protocol Secure

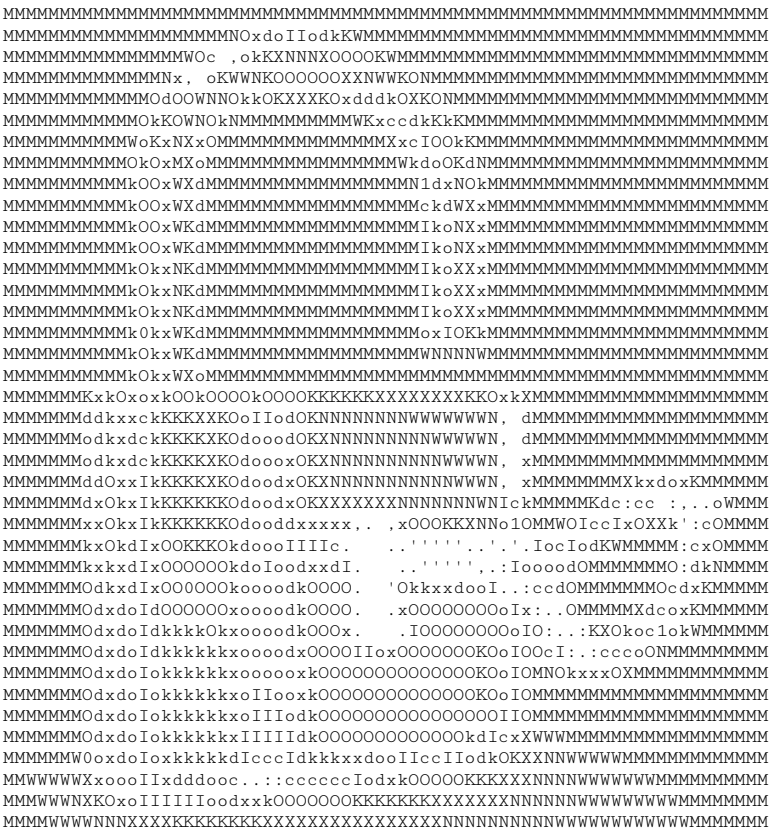
Elizebeth Smith Friedman (1892-1980)

Figure 5 – Elizebeth Smith Friedman.

Elizebeth Smith Friedman est considérée comme la première femme cryptanalyste aux États-Unis. Le livre *The Woman Who Smashed Codes* par Jason Fagone (non traduit en français) retrace sa vie. Travaillant à l'U.S. Navy, elle a participé à la cryptanalyse de la machine ENIGMA utilisée par l'armée allemande pour chiffrer les communications pendant la Seconde Guerre mondiale (cette histoire est racontée dans l'ouvrage de Simon Singh [Sin99]). Les lettres utilisées dans cette énigme sont complètement imaginaires.

La méthode de chiffrement de la machine ENIGMA a été cassée par les cryptanalystes de l'armée britannique travaillant à Bletchley Park en partie grâce à une idée similaire à celle utilisée pour cette énigme. En effet, les militaires allemands commençaient par la date dans leurs communications quotidiennes et terminaient par « Heil Hitler ». Ces répétitions ont grandement aidé les chercheurs anglais à cryptanalyser ces échanges.

3 Une image mystérieuse ☆☆☆



Énigme 3 : *Cette image en ASCII [ϟ] art cache un nombre secret compris entre 32 et 63. Saurez-vous le découvrir ?*

[ϟ] American Standard Code for Information Interchange