Comment créer des missions cryptographiques ?

Anaïs Durand
IREM de Clermont-Ferrand, LIMOS, université Clermont Auvergne

Séverine Fleury
IREM de Clermont-Ferrand

Pascal Lafourcade
IREM de Clermont-Ferrand, LIMOS, université Clermont Auvergne

Marianne Mognos
IREM de Clermont-Ferrand

Malika More
IREM de Clermont-Ferrand, LIMOS, université Clermont Auvergne

Cet article propose de découvrir un site permettant de créer des énigmes cryptographiques pour construire une activité collaborative à réaliser dans un cadre scolaire, universitaire ou grand public. Plus d'une cinquantaine de concepts cryptographiques, dans une version débranchée, sont proposés au choix de l'enseignante ou de l'animateur. Les énigmes sont conçues pour être utilisées du cycle 3 à la fin du lycée, et au-delà. Grâce à ce site, il est possible de générer une mission cryptographique personnalisée avec tous les fichiers (et les corrections) pour la mettre en œuvre.

Introduction

Depuis les révélations d'Edward Snowden en 2013, le grand public a pris conscience que la sécurité informatique et la cryptographie sont des disciplines à part entière et qu'elles concernent tout le monde. Ces domaines sont ainsi devenus des incontournables de l'éducation au numérique. Cependant,

DOI:10.48556/SIF.1024.27.21

les concepts mathématiques mis en jeu sont souvent complexes et peuvent demander un niveau licence ou master pour être abordés [1, 2, 3]. À première vue, il semble donc que cette science soit hors de portée d'écoliers, de collégiens ou de lycéens.

Les *missions cryptographiques* permettent d'illustrer des mécanismes cryptographiques aussi bien historiques que modernes et de les faire vivre concrètement aux participantes et aux participants. Cela peut paraître ambitieux, mais des expérimentations dans des classes de tous niveaux depuis plusieurs années ont montré qu'en s'amusant en groupe et en autonomie, les élèves, et même les adultes, sont capables de comprendre et de résoudre de nombreux défis.

Dans l'objectif de permettre au plus grand nombre de collègues de mettre en œuvre cette activité, cet article présente le site *Mission crypto*[1] permettant de créer des missions cryptographiques personnalisées, en choisissant en quelques clics le nombre, le type et la difficulté des énigmes qui les constituent[2]. La figure 1 présente la page d'accueil du site.

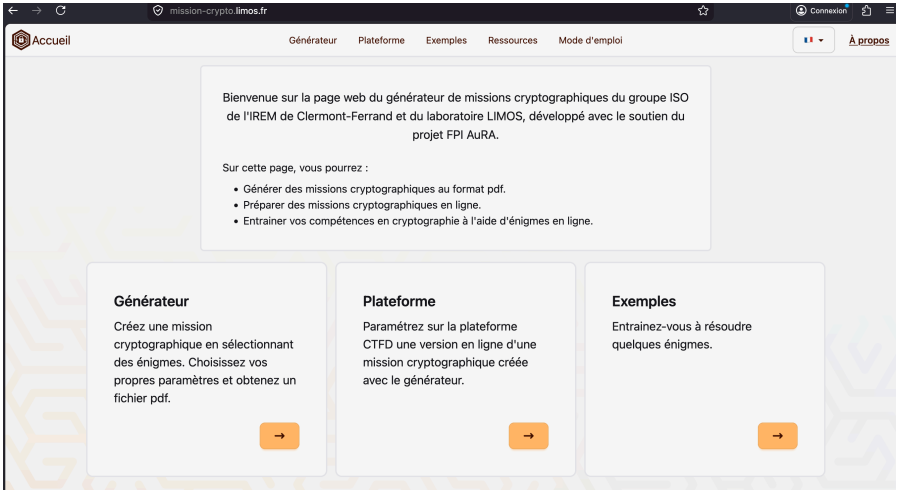

Fig. 1. Page d'accueil.

1. `https://mission-crypto.limos.fr`.
2. Cette action a été cofinancée par le projet FPI AuRA, une opération soutenue par l'État dans le cadre de l'AMI « Compétences et métiers d'avenir » du programme France 2030, opéré par la Caisse des dépôts (la Banque des territoires).

L’informatique sans ordinateur

Nous sommes convaincus que certains concepts fondamentaux de la science informatique peuvent être enseignés en partie grâce à des activités sans ordinateur, permettant découverte, réflexion et prise de recul, d’une manière complémentaire de celles qui se déroulent sur des machines. Cette drôle d’idée a été popularisée par le néo-zélandais Tim Bell [4] dans les années 1990. Dans cette démarche, les activités donnent l’occasion aux élèves de se concentrer sur les concepts informatiques, sans être distraits par les facilités et les difficultés liées à l’utilisation des objets numériques. Dans cet esprit, toutes les énigmes de cryptographie proposées sont réalisables à l’aide d’un papier, d’un crayon (parfois aussi d’une règle et de ciseaux), et surtout d’une bonne dose de curiosité et de réflexion.

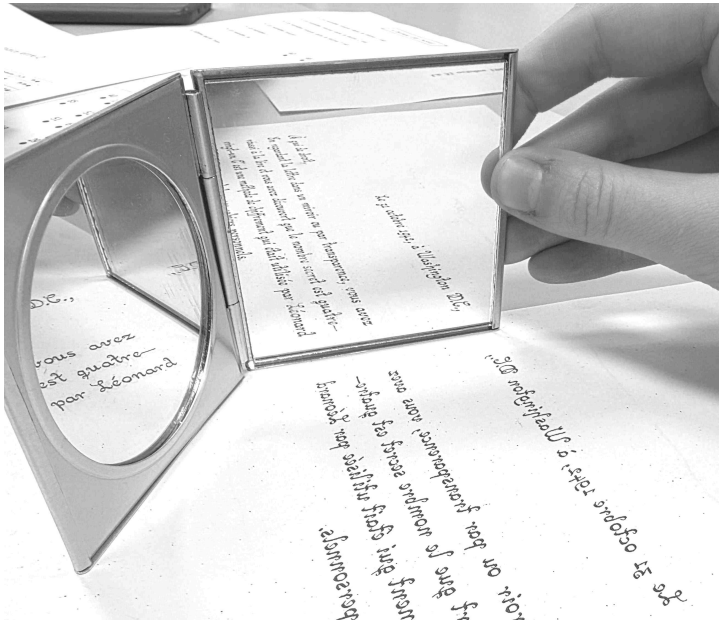

Fig. 2. De l’autre côté du miroir.

Quelques exemples d’énigmes

Le site propose plus d’une cinquantaine d’énigmes, qui s’inspirent de chiffrements classiques, mais aussi de concepts cryptographiques modernes.

Parmi les chiffrements classiques, il y a bien sûr le chiffre de César et celui de Vigenère mais aussi le chiffre du parc à cochons (*pig pen*) des francs-maçons, et celui des hommes dansants de Sherlock Holmes. Certaines énigmes s'inspirent de machines cryptographiques historiques, comme la machine Sphinx, le cylindre de Jefferson, la scytale grecque ou la célèbre machine Enigma. Comme la notion de chiffrement par substitution est très proche de celle de codage, le code Braille, le code Morse, le code des drapeaux maritimes, etc. ont été inclus.

Certaines énigmes permettent également d'aborder des notions plus avancées ou plus modernes : les attaques par canal caché, les preuves sans divulgation de connaissance, le renseignement d'origine sources ouvertes, la cryptographie visuelle, la stéganographie, la sécurité des mots de passe, etc.

De nombreuses autres énigmes sont encore en projet (comme celles présentées dans les ouvrages [5] et [6]), sur la *blockchain*, sur les chiffrements homomorphes, sur la cryptographie postquantique, etc. Le site continue d'être alimenté pour qu'il s'étoffe au fil des créations et découvertes des auteurs[3].

Construire une mission cryptographique

Le site *Mission crypto*[1] a été conçu de manière à pouvoir générer des missions adaptées à différents publics et pour différentes occasions. Il a été utilisé pour préparer des séances dans des classes du cycle 3 au supérieur, mais aussi pour des animations de type fête de la Science, Semaine des mathématiques, stage MathC2+, liaison École-Collège, Journée portes ouvertes, festival Les nuées ardentes (avec plus de 3000 participants chaque année).

Qu'est-ce-qu'une mission cryptographique ?

Il s'agit d'une série de lettres permettant d'accéder à un secret en résolvant des énigmes cryptographiques :

- la lettre d'introduction présente la mission et son but ;
- le corps de la mission est constitué par un nombre variable de lettres, proposant chacune une énigme cryptographique, et dont la solution est un nombre ;
- la lettre de conclusion présente une dernière énigme, utilisant tous les nombres trouvés dans les lettres précédentes, et dont la solution est un dernier nombre. Lors des séances animées par les auteurs, ce dernier nombre permet d'ouvrir le cadenas d'un coffre contenant généralement des bonbons.

3. Les propositions d'énigmes de la part des lecteurs de 1024 sont les bienvenues.

La figure 3 présente la page de création d'une mission composée de cinq énigmes. La première porte sur la cryptanalyse de la machine Sphinx, commercialisée vers 1930 par la Société des codes télégraphiques de Georges Lugagne à Marseille, la seconde énigme utilise les fameux hommes dansants de Sherlok Holmes, la troisième propose un codage musical, la quatrième est une initiation à la rétro-ingénierie d'un programme et enfin, la dernière énigme illustre le concept de preuve à divulgation nulle de connaissance (zero knowledge proof, ZKP). Ensuite l'utilisateur du site va pouvoir choisir le début et la fin de la mission, effectuer le réglage de divers paramètres et configurer le secret de chaque énigme.

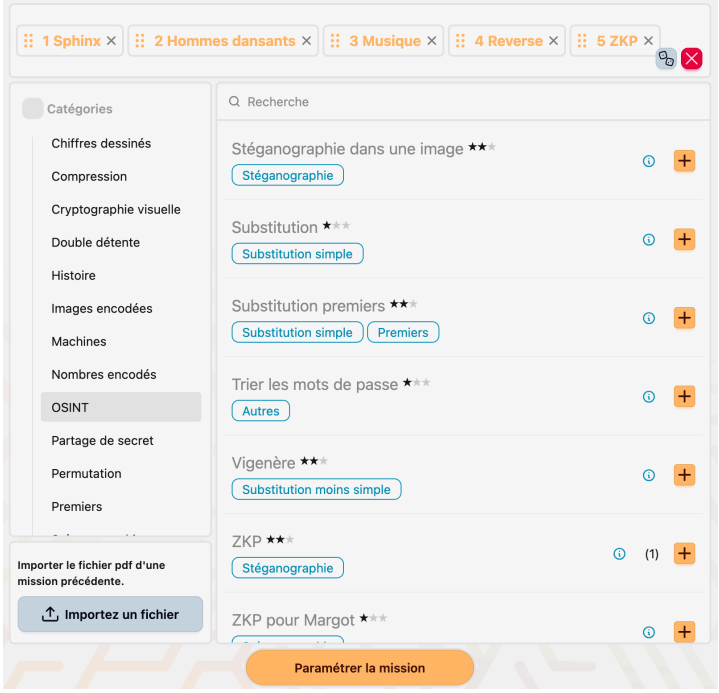

Fig. 3. Page de création d'une mission.

Que fait le site ?

Le site *Mission crypto*[1] permet de créer sur mesure une mission de façon à l'adapter au temps disponible et au public visé :
– le nombre de lettres du corps de la mission est paramétrable ;
– plus d'une cinquantaine d'énigmes différentes sont proposées ;

– l'ordre des lettres du corps de la mission est modifiable ;
– il est possible d'utiliser plusieurs fois la même énigme, avec des solutions différentes et, chaque fois que cela s'y prête, une clé de chiffrement différente ;
– le type de l'énigme de la lettre de conclusion est à choisir parmi plusieurs possibilités de difficultés différentes ;
– la date et la signature des lettres sont personnalisables, de même que les textes des énigmes ;
– les nombres constituant les solutions des énigmes peuvent être choisis aléatoirement par le site ou fournis par l'utilisateur. Dans tous les cas, le site vérifie que les nombres sont cohérents avec les contraintes de la lettre de conclusion, selon le type choisi.

Une fois ce paramétrage effectué, le site génère l'ensemble des fichiers nécessaires aux formats Latex et PDF : l'introduction, les énigmes, la conclusion et un carnet de bord pour noter les réponses. Bien entendu, les solutions sont aussi fournies pour que le maître du jeu puisse aider les participantes et les participants et vérifier leurs réponses.

Cerise sur le gâteau, il est possible de créer une version en ligne, totalement dématérialisée, de la mission. Cette fonctionnalité est utile pour éviter d'imprimer lorsque des ordinateurs connectés sont disponibles. En effet, le site permet en un clic de créer une instance de CTFd, une plateforme *open source* de gestion de CTF (*capture the flag*[4]). Les comptes des personnes participant à la mission sont créés et elles accèdent aux énigmes au format PDF et suivent leur progression sur le tableau de bord de la plateforme. Lors d'un challenge en 2025, cette solution a permis à 200 personnes regroupées en équipes de 5 de s'affronter pendant deux heures.

Conception des énigmes

Chaque énigme a été élaborée dans le but d'illustrer un concept important en matière de cryptographie ou de sécurité informatique. La « mise en énigme » en est parfois simple et évidente, mais peut parfois aussi demander une longue réflexion et de nombreux essais. Ensuite, il faut donner assez d'indices pour que les personnes puissent avancer en autonomie en faisant appel à leur sens de l'observation, leur créativité et leur esprit de déduction. Pour finir, les énigmes sont testées plusieurs fois car une erreur ou une formulation ambiguë risquent de démotiver totalement les participantes et participants, voire rendre l'énigme impossible à résoudre.

4. *Capture the flag* est un jeu utilisé en cybersecurité pour simuler des attaques au cours lesquelles l'on doit, par exemple, trouver un fichier caché dans un environnement informatique réputé confidentiel et sûr.

Conseils pour générer et animer une mission

Il est important d'adapter les énigmes et leurs énoncés au public visé (âge, compétences, temps imparti, nombre de personnes par groupe), pour proposer un défi de difficulté raisonnable et progressive, assurant la motivation du public.

Si la résolution des énigmes ne requiert pas de matériel particulier, il est préférable que tout le monde dispose d'une copie de l'énoncé. L'animateur ou l'animatrice peut choisir de distribuer les lettres une par une, deux par deux, etc., ou même toutes à la fois. Il est souhaitable de faire travailler les personnes par groupes de 3 à 5, cela fait partie de ce qu'elles disent souvent avoir beaucoup apprécié.

Les énigmes sont conçues pour un travail autonome. C'est pourquoi il semble préférable que le rôle de l'adulte qui supervise l'activité se limite à accompagner les participantes et les participants dans leurs recherches : n'intervenir que si nécessaire, pour les guider avec parcimonie, les empêcher de partir trop loin et de chercher des choses trop complexes, et donner, si besoin, quelques indices supplémentaires.

En revanche, il est conseillé de reprendre la main, une fois la mission terminée, pour expliciter ce qui a été découvert : cela permet de formaliser les découvertes avec les mots et les concepts correspondants, de faire décrire les méthodes de résolution utilisées, ce qui était difficile et comment ces défis ont été surmontés. Pour une séance d'une heure, il est recommandé de réserver au moins dix minutes pour cette étape de prise de recul et de mise en commun.

Conclusion

Le site *Mission crypto*[1] permet de créer des missions cryptographiques personnalisées. Elles constituent une manière ludique d'initier les élèves, les étudiants et le grand public à des concepts fondamentaux de cryptographie et de sécurité informatique. Les collègues sont encouragés à s'en saisir, pour adapter leurs énigmes préférées à leur public, au temps disponible et à la forme qu'ils souhaitent donner à « leur » mission cryptographique. Cela constitue une bonne initiation à la cryptographie moderne. Ces énigmes sont égalements utilisées dans des cours, TD, TP ou examens dans le supérieur.

Remerciements

L'auteur et les autrices tiennent à remercier Cédric Lauradoux pour son inspiration et son aide dans la création de cette activité, ainsi que les nombreux enseignants et enseignantes, élèves, étudiantes et étudiants qui ont testé leurs diverses énigmes expérimentales depuis des années.

Références

[1] J.-G. Dumas, J.-L. Roch, S. Varette & É. Tannier. 2018. *Théorie des codes — Compression, cryptage, correction*. Dunod.

[2] J. Katz & Y. Lindell. 2020. *Introduction to Modern Cryptography*. Chapman and Hall/CRC.

[3] P-A. Fouque, P. Lafourcade, L. Perret. 2026. *Cryptographie post-quantique*. Dunod.

[4] T. Bell, I. H. Witten, M. Fellows. 1998. *Computer Science Unplugged… offline activities and games for all ages*.

[5] P. Lafourcade, M. More. 2024. *25 énigmes ludiques pour s'initier à la cryptographie*. 2nd ed. Dunod.

[6] P. Lafourcade, C. Onete. *20 énigmes ludiques pour se perfectionner en cryptographie*. Dunod.