Nombre de participant·e·s maximal pour l'atelier	20 par session	Nombre de sessions de 45mn que vous pouvez réaliser	3
Matériel nécessaire (vidéo-projection, grande salle, autre ...)	LES PARTICIPANTS DOIVENT APPORTER UN ORDINATEUR Vidéo-projection + wifi pour les participants + rallonges et multiprises pour les participants		

Un site pour créer des missions cryptographiques

Anaïs Durand[1,2], Séverine Fleury[1], Pascal Lafourcade[1,2], Marianne Mognos[1], Malika More[1,2]

1 IREM de Clermont-Ferrand, 2 LIMOS, Université Clermont Auvergne

RÉSUMÉ *Dans cet atelier, nous proposons aux participant.e.s de découvrir un site permettant de créer des énigmes cryptographiques pour construire une activité collaborative à réaliser en classe ou à la maison. Une cinquantaine de concepts cryptographiques, dans une version débranchée, sont proposés au choix de l'enseignant.e. L'activité peut être adaptée du cycle 3 à la fin du lycée, et au-delà. Les participant.e.s concevront une mission cryptographique personnalisée et repartiront avec tous les fichiers (et les corrections) pour la faire réaliser par leurs élèves.*

MOTS-CLÉS • *Cryptographie – Sécurité informatique – Informatique sans ordinateur – Activité collaborative*

Des élèves en train de réaliser une mission cryptographique.

Cette action a été co-financée 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).

1. Déroulement de l'atelier

L'atelier débutera par une rapide présentation du concept de mission cryptographique et quelques exemples. Ensuite, les participant.e.s seront invités à découvrir la fonctionnalité principale du site, permettant de créer soi-même des missions cryptographiques. Elles et ils seront invités à choisir des énigmes et à paramétrer leur mission personnalisée, puis à télécharger le résultat. Elles et ils pourront donc repartir avec tous les fichiers pour faire réaliser cette mission par leurs élèves, leurs étudiant.e.s ou autres. Pour les personnes intéressées, les autres fonctionnalités du site seront abordées : l'accès à l'ensemble des sources LaTeX, permettant une personnalisation totale de la mission d'une part et l'utilisation de la plateforme CTFD pour proposer la mission en ligne d'autre part. Enfin, le site propose aussi de résoudre en ligne quelques énigmes sans passer par une mission cryptographique.

2. Description de la ressource présentée dans l'atelier

1. 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, les concepts mathématiques mis en jeu sont souvent complexes et peuvent nécessiter un niveau licence ou master pour les aborder ([Dumas, Katz, Perret]). À première vue, il semble donc que cette science soit hors de portée d'écoliers, de collégiens ou de lycéens.

Avec les missions cryptographiques, nous nous proposons d'illustrer des mécanismes cryptographiques aussi bien historiques que modernes et de les faire vivre concrètement aux élèves. Cela peut paraître ambitieux, mais nos expérimentations dans des classes de tous niveaux depuis plusieurs années (voir par exemple [Bultel]) ont montré qu'en s'amusant en groupe et en autonomie, les élèves sont capables de comprendre et de résoudre de nombreux défis.

Dans l'objectif de permettre au plus grand nombre de collègues de réaliser cette activité, nous présentons dans cet atelier le site https://mission-crypto.limos.fr/ permettant de créer des missions cryptographiques personnalisées, en choisissant en quelques clics le nombre, le type et la difficulté des énigmes qui la constituent.

- 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 introduite par le néo-zélandais Tim Bell ([Bell]) 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 que

nous proposons 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.

- Quelques exemples d'énigmes

Nous proposons plus de soixante énigmes, qui s'inspirent de chiffrements classiques, mais aussi de concepts cryptographiques modernes.

Parmi les chiffrements classiques, on trouve bien sûr le code de César et celui de Vigenère mais aussi le chiffrement du parc à cochons (pigpen) 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, nous avons inclus le code Braille, le code Morse, le code des drapeaux maritimes, etc.

Nous proposons également des énigmes permettant d'aborder des notions plus avancées : 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 ([Lafourcade 2023, Lafourcade 2024]), sur la blockchain, sur les chiffrements homomorphes, sur la cryptographie post-quantique... Nous espérons que le site continuera de s'étoffer au fil de nos futurs projets.

- 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 fournir assez d'indices pour que les élèves puissent avancer par eux-mêmes 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 participant.e.s, voire de rendre l'énigme impossible à résoudre.

2. Construire une mission cryptographique

Le site https://mission-crypto.limos.fr/ a été conçu de manière à pouvoir générer des missions adaptées à différents publics et pour différentes occasions. Outre pour préparer des séances dans des classes du cycle 3 au supérieur, ce site (et son ancêtre sous forme d'une série de scripts en Python) a été utilisé pour des animations de type Fête de la Science, Semaine des Mathématiques, Stages MathC2+, Liaison École-Collège, etc.

- 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 nos soins, ce dernier nombre permet d'ouvrir le cadenas d'un coffre contenant généralement des gourmandises.
    - Que fait le site ?

La mission peut être personnalisée de nombreuses façons sur le site, pour l'adapter au temps disponible et au public visé :

- le nombre de lettres du corps de la mission est paramétrable ;
- plus de soixante énigmes différentes sont proposées ;
- 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 récapitulatif des réponses.

3. Conseils pour animer une mission cryptographique

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

Si la résolution des énigmes ne requiert pas de matériel particulier, il est préférable que chaque élève dispose d'une copie de l'énoncé. L'animateurice 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 élèves par groupes de 3 à 5, cela fait partie de ce qu'elles et ils disent souvent par la suite avoir beaucoup apprécié.

Les énigmes sont conçues pour un travail autonome des élèves. C'est pourquoi il nous semble préférable que le rôle de l'enseignant.e se limite à les accompagner dans leurs recherches. Elle ou il n'intervient que si nécessaire, pour les guider avec parcimonie. Elle ou il doit principalement veiller à ce que les élèves ne partent pas trop loin et ne cherchent pas des choses trop complexes. Elle ou il peut aussi donner, si besoin, quelques indices supplémentaires.

En revanche, nous suggérons que l'enseignant.e reprenne la main, une fois la mission terminée, pour expliciter ce que les élèves ont découvert : elle ou il formalise leurs découvertes avec les mots et les concepts correspondants, leur fait décrire comment elles et ils ont fait, ce qui était difficile et comment elles et ils ont surmonté ces défis.

4. Conclusion

Nous proposons dans cet atelier de découvrir un site permettant de créer des missions cryptographiques personnalisées. Elles constituent une manière ludique d'initier les élèves à des concepts fondamentaux de cryptographie et de sécurité informatique. Nous espérons montrer la flexibilité et la facilité d'utilisation de notre proposition. Nous encourageons les enseignant.e.s à s'en saisir, pour adapter leurs énigmes préférées à l'âge de leurs élèves, au temps disponible et à la forme qu'ils souhaitent donner à « leur » mission cryptographique.

5. Remerciements

Nous tenons à remercier Cédric Lauradoux pour nous avoir inspiré.e.s et aidé.e.s dans la création de cette activité, ainsi que les nombreux enseignant.e.s, élèves et étudiant.e.s qui ont subi nos diverses énigmes expérimentales depuis des années.

3. Expérimentations réalisées ou envisagées

Nous proposons à travers cet atelier et plus généralement le site https://mission-crypto.limos.fr/ un partage de ressources à l'attention des collègues enseignant.e.s et animateurices souhaitant faire découvrir la cryptographie et la sécurité informatique grâce à une activité ludique et collaborative. Cette proposition est issue des très nombreuses missions cryptographiques que nous animons plusieurs fois par an dans des cadres scolaires, para-scolaires ou grand public depuis plusieurs années. Lors de ces séances, nous n'avons pas déployé de procédures expérimentales rigoureuses, ni réalisé d'analyse didactique. Au-delà de nos observations informelles et des retours d'enseignant.e.s ayant réalisé cette activité dans leur classe, il serait certainement intéressant d'envisager une analyse des apports didactiques de cette activité, en collaboration avec des experts du domaine.

4. Liens vers les ressources et point de contact

- *Site Mission Crypto* : https://mission-crypto.limos.fr/, dernier accès 10 février 2026
- anais.durand@uca.fr, severine.fleury@ac-clermont.fr, pascal.lafourcade@uca.fr, marianne.mognos@ac-clermont.fr, malika.more@uca.fr

5. Références

Bell, T., Witten, I. H., Fellows, M. : *Computer Science Unplugged: Offline activities and games for all ages*. 1998

Xavier Bultel, Jannik Dreier, Pascal Lafourcade, and Malika More. *How to Explain Modern Security Concepts to your Children*, Journal Cryptologia, volume 41, numero 5, pages 422–447, 2017.

Dumas, J.-G., Roch, J.-L., Varette, S., Tannier, É. : *Théorie des codes : Compression, cryptage, correction*. Dunod, Paris (2018)

Katz, J., Lindell, Y. : *Introduction to Modern Cryptography*. Chapman and Hall/CRC (2020)

Lafourcade, P., Onete, C. : *20 énigmes ludiques pour se perfectionner en cryptographie*. Dunod, Paris (2023)

Lafourcade, P., More, M. : *25 énigmes ludiques pour s'initier à la cryptographie*.
2nd édition. Dunod, Paris (2024)

Ludovic Perret, Pierre-Alain Fouque et Pascal Lafourcade, *Cryptographie post-quantique*, Dunod, Paris (2026)