



Pocket Enigma

Niveau de difficulté : Débutant à Intermédiaire

Durée de l'activité : 5 à 30 minutes

Nombre de participants : 1-10 personnes

Public cible : collège, lycée et au-delà

Coût estimé : quelques € par participant (punaise + bouchon ou attache parisienne + impression sur feuille cartonnée)

Logistique : prévoir au moins une table et des chaises pour les participants

MATÉRIEL NÉCESSAIRE

Pour chaque participant :

- Impression sur papier (idéalement cartonné) du PDF de la mini Enigma
- Punaise + morceau de bouchon (ou attache parisienne)
- Paire de ciseaux

Optionnel : venir avec une machine à chiffrer de la seconde guerre mondiale pour pouvoir faire le parallèle.

Éléments à préparer en amont :

Dans le cas d'un atelier de durée réduite, venir avec des pocket Enigma déjà montées en nombre suffisant pour les participants

OBJECTIFS PÉDAGOGIQUES

• [Compétences développées]

Logique, décryptement

L'atelier permet de voir très vite les enfants qui ont développé leur sens mathématique

• [Concepts abordés]

L'atelier commence en présentant le concept de fonctionnement de la machine Enigma. Il se veut ensuite un exercice d'application concret et simplifié du décryptement d'Enigma par les anglais pendant la seconde guerre mondiale.

• [Applications pratiques]

Permet de chiffrer des messages entre amis.

SCÉNARIO D'ANIMATION

Introduction (5 min)

Mettre en contexte l'atelier : s'assurer que les participants connaissent ce qu'est Enigma, sinon leur expliquer.

Optionnel : commencer par des travaux pratiques et faire monter les pocket Enigma par les participants. A défaut prévoir les pocket Enigma déjà assemblées en nombre suffisant.

La punaise permet de laisser le rotor mobile. Le bouchon est enfoncé dans la punaise pour empêcher que le rotor ne se détache mais aussi pour éviter de se blesser avec la punaise, une fois la pocket Enigma montée.



Démonstration (5 min)

- **[Instructions pour présenter l'outil]**

Présenter le fonctionnement de la pocket Enigma : la clef de chiffrement est la lettre choisie sur le pourtour. La mise à la clé consiste à faire tourner le rotor pour que la flèche pointe sur cette lettre. À partir de la lettre du clair on suit le fil sur le rotor pour trouver la lettre chiffrée. Le mécanisme est réciproque. Suivre le fil depuis la lettre chiffrée montre la lettre claire. La méthode est la même pour déchiffrer. À chaque nouvelle lettre on tourne le rotor d'un cran dans le sens des aiguilles d'une montre, ce qui change la correspondance entre clair et chiffré.

- **[Exemple simple à réaliser devant les participants]**

Pour s'assurer de la bonne compréhension du mécanisme par les participants, leur faire chiffrer leur prénom en leur donnant une clef à respecter. Les participants écrivent le message chiffré sur un papier et le transmettent à leur voisin qui doit réussir à le déchiffrer.

Mise en pratique (10-15 min)

Une fois le fonctionnement compris par tous, l'animateur explique la méthode employée par Alan Turing pour décrypter Enigma pendant la seconde guerre mondiale, à savoir partir d'un clair connu : « Wetterbericht » (bulletin météo en Allemand) en début de message et « Heil Hitler » en formule de conclusion puis tester toutes les combinaisons de rotor jusqu'à trouver celle qui donne un texte lisible.

Dire que l'on va faire la même chose avec notre pocket Enigma. Le principe est que la signature du message est connue (HZV) et qu'il faut, comme Turing, utiliser cela pour retrouver le message complet.

La feuille présente 3 exercices de difficulté croissante. En fonction de leur habileté, les participants vont, soit péniblement finir le premier exercice, soit aller jusqu'au bout.

- Dans le premier exercice, une seule position de rotor est possible pour trouver les lettres de la signature. Le décodage est donc trivial.
- Dans le second exercice, deux positions de rotor sont possibles pour les lettres de la signature, toutefois une seule position donne le texte clair. Les participants commencent généralement par la mauvaise position du rotor et l'animateur doit faire un apport pédagogique pour expliquer cela par le nombre de liens de même longueur sur le rotor.
- Dans le troisième et dernier exercice, trois positions de rotor sont possibles pour les lettres de la signature, toutefois une seule position donne un texte intelligible. Cela ne présente pas de difficulté si le second exercice a été réussi et cela permet de s'assurer de la compréhension du concept.

Conclusion (1 min)

- **[Questions à poser pour vérifier la compréhension]**

Implicite, notamment au travers de l'introduction où chacun chiffre et déchiffre un prénom, puis par la réussite du second niveau de l'exercice.

- **[Lien avec la cybersécurité moderne]**

Présente la technique de force brutale par recherche exhaustive avec le clair connu comme critère d'arrêt.



CONSEILS POUR L'ANIMATEUR

• [Difficultés fréquemment rencontrées]

Être au moins 2 animateurs pour gérer l'hétérogénéité du groupe et donner de la fluidité : certains enfants comprennent tout de suite, d'autres ont besoin de plus de temps et d'explications.

• [Astuces pour faciliter l'animation]

Éventuellement apporter une vraie machine à chiffrer de la 2^e guerre mondiale pour illustrer et ancrer dans le concret.

• [Adaptations possibles selon le public]

Sur un salon, la pocket Enigma permet de présenter de manière didactique le fonctionnement d'une machine Enigma en quelques minutes. Prévoir une pocket Enigma déjà montée et dérouler uniquement la présentation de l'outil

Avec des enfants, il peut être intéressant de démarrer par une phase de travaux pratiques en construisant la mini Enigma. Toutefois il est possible de venir avec des machines déjà montées pour ne pas faire de bricolage et aller plus vite.

La durée de l'atelier peut être adaptée en ne faisant qu'un ou deux des exercices.

Un CONTEXTE HISTORIQUE

Différence avec la « vraie » machine ENIGMA :

La machine Enigma était constituée de trois rotors câblés en série et d'un réflecteur fixe qui renvoyait l'impulsion électrique dans les rotors dans l'ordre inverse.

La pocket Enigma présentée ici est en fait constituée du seul réflecteur, mais rotatif.

