Activité - Initiation à la cryptographie

TOUTES LES FICHES

par Salomé Hurel

CC BY SA

PUBLIC	PARTICIPANTS	ANIMATEURS	NIVEAU	PRÉPARATION	ACTIVITÉ

Description

Cette activité permet de comprendre comment peuvent être cryptés des messages.

Objectifs

Cryptographie

Matériel

Ordinateurs
Connexion internet
Vidéo-projecteur

Contenus utilisés

https://www.dcode.fr/
https://cryptii.com/

Pré-requis

Aucun

WORKFLOW

1 Introduction

Cet atelier est un jeu de piste dans lequel les participant.e.s devront utiliser un outil simple pour déchiffrer un message qui les emmènera sur un site web ou se trouve un vrai mystère crypté (toujours non résolu à ce jour). Au cours du jeu, les participant.e.s aborderont des notions de chiffrement simples grâce à un outil en ligne : Cryptii.

L'adresse web du message mystère est divisée en trois parties, chaque partie est chiffrée avec une méthode différente.

- L'inversement des lettres d'un message
- L'alphabet de César
- Le morse

Les participant.e.s devront les déchiffrer une à une grâce au site cryptii.com.

Conseil médiation :

Cette activité est un prétexte pour expliquer comment protéger ses données personnelles en les cryptant, notamment les messages envoyés, et l'intérêt de le faire.
N'hésitez pas à vous référer aux fiches outils "Les données personnelles"

2 Qu'est-ce que la cryptographie ?

La cryptographie ou système de chiffrement sert à cacher un message à la vue de regards indiscrets, seuls celleux qui connaissent la méthode utilisée pour chiffrer le message en premier lieu sont en mesure de le lire. La méthode utilisée est souvent un secret partagé entre l'expéditeur.rice et le.a destinataire du message (le nombre de décalages de lettres par exemple).

3 Présentation de Cryptii

Cryptii est un site qui permet de chiffrer et déchiffrer des phrases avec différentes méthodes. Nous allons utiliser sur ce service trois procédés de chiffrement simple à

maîtriser :

1. L'inversement des lettres d'un message
2. L'alphabet de César
3. Le morse

Rendez-vous sur https://cryptii.com, il s'agit de prendre en main l'interface très simple pour la montrer aux participant.e.s:

- Dans la partie gauche se trouve le texte à déchiffrer,
- Dans la partie centrale, le choix de la méthode de chiffrement (ici reverse)
- Dans la partie droite, le résultat de l'opération de déchiffrement

Pour commencer, présenter rapidement aux participant.es "le chiffre de César" , appelé aussi chiffrement par décalages. Cette méthode est appelée ainsi car on dit que c'est ainsi que Jules César chiffrait ses messages pour ses correspondances secrètes. Il ne faut pas rentrer dans les détails, et expliquer le fonctionnement de ce cryptage, car l'objectif juste après est de demander aux participant.es de comprendre par eux.elles-mêmes comment il fonctionne.

Pour cela, aller sur Criptii et cliquer sur *Reverse* en orange. La fenêtre de sélection s'ouvre, choisir *Casear cipher.* Le chiffrement de César a ainsi été sélectionné comme méthode de chiffrement. Pour le faire comprendre aux participant.e.s, dans le module gauche de texte écrire le mot "absolument" et régler la jauge à zéro à l'aide du – ou +. Le mot n'est pas alors pas encore codé.

Cliquer 1 fois sur le – , à droite "absolument" est maintenant codé ! Mais comment ? Laissez 3-5 min les participant.e.s y réfléchir.

Explications :

Le chiffrement de César est simple : on décale chaque lettre du message d'une ou plusieurs positions dans l'alphabet. Avec la jauge à 1, on obtient cette grille de déchiffrement :

b = **a**
c = **b**
t = **s**
p = **o**
m = **l**
v = **u**
n = **m**
f = **e**
o = **n**
u = **t**

Pour lire ce codage il faut connaître le décalage de lettres, tout simplement.

Montrer le site *https://www.dcode.fr/chiffre-cesar* qui permet de casser informatiquement le chiffrement de César, en effet un programme essaie tous les

décalages et les affiche dans la colonne de gauche. Reste à trouver le mot ou la phrase cohérente.

4 Déroulé

Une fois le fonctionnement du site Cryptii expliqué, donner l'adresse chiffrée aux participant.e.s. Pour accéder au message secret contenu à cette adresse, les participant.e.s vont devoir déchiffrer une à une les 3 parties de l'adresse. En fonction du nombre de participant.e.s et de leur autonomie :

- soit les mettre par groupe et organiser une compétition de vitesse – le premier groupe qui a déchiffré l'adresse et qui accède au message gagne –
- soit faire jouer chaque participant.e seul.e

Une fois les participant.es réparti.es

Écrire l'adresse chiffrée complète au tableau :

> gro.euqiremunudsruegayov.sptth://dw-jvualua/bwsvhkz/2020/—— …–/ .-
> .. . – – .-. . -.. ..- –.. — -.. .. .- -.-. .-.-.- .— .–. –.

L'adresse finale une fois déchiffrée est :

> https://voyageursdunumerique.org/wp-
> content/uploads/2020/03/1457972964.jpg

Le chiffrement a été réalisé en 3 étapes différentes. Chaque groupe va donc devoir deviner pour chaque partie la méthode de chiffrement utilisée. Pour que ce soit plus facile, expliquer aux participant.e.s que l'adresse a été chiffrée en trois parties, chaque fois avec une méthode différente.

Partie 1 :

Le début de l'adresse https://voyageursdunumerique.org/a été chiffré avec la méthode "miroir". Une fois chiffré, on obtient

> gro.euqiremunudsruegayov.sptth://

Demander aux participant.e.s de déchiffrer cette partie grâce à Cryptii. Si l'opération prend trop de temps, on peut les aiguiller en leur indiquant par exemple que c'est une adresse web et que celle-ci commence donc par https://. C'est un gros indice !

Partie 2

La deuxième partie de l'adresse wp-content/uploads/2020

Elle été chiffrée avec le chiffrement de César. Une fois chiffrée (décalage 7), nous

avons

dw-jvualua/bwsvhkz/2020/

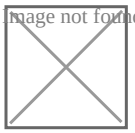
Astuce CHUUUUT : https://www.dcode.fr/chiffre-cesar coller le message codé et sélectionné, tester tous les décalages en-dessous .. puis déchiffrer, observer la colonne à gauche ?

Partie 3

Le nom du fichier “03/Lettreduzodiac.jpg”, nous avons voulu le coder en Morse plus pour la culture que pour le challenge et pour démontrer que un chiffre et une lettre peuvent être remplacés par un signe ou un dessin :

Ce qui donne en morse

—– …–/ .-.. . – – .-. . -.. ..- –.. — -.. .. .- -.-. .-.-.- .— .–. –.

Une fois décodé, les participant.e.s pourront coller le lien dans le navigateur …

Cette lettre est une vraie lettre écrite par le tueur en série le Zodiak jamais identifié à ce jour, le tueur en série a signifié qu’en décryptant cette lettre, il trouverait son identité. Le FBI n’a rien trouvé, cette lettre a été rendue publique pour que tout le monde puisse essayer de la décrypter. En effet, une des premières lettres écrite et envoyée à la presse par le tueur a été déchiffrée par un couple adepte des jeux codés dans les magazines de l’époque.