EPI L'histoire des secrets ou les secrets de l'Histoire

TP

Code César

Connexion à l'activité

▷ Se connecter à l'ENT :
https://e-college.indre.fr/portail/f/welcome/normal/render.uP

▷ sélectionner la brique Capytale : 

▷ sélectionner « accéder à vos activités » puis taper le code : **598b-1968805**

Ouvrir dans Scratch le fichier « Code_ Cesar.sb3 », qui se trouve dans le serveur Commun Classes (H :).
Puis penser à l'enregistrer sur votre compte (« Fichier » → « sauvegarder sur votre ordinateur » → votre compte).

I Cryptographie

Exercice n° 1 — Chiffrement

Chiffrer le message « TESTONSCEPROGRAMMEPOURVOIRSILFONCTIONNEBIEN », avec une clé de 3

Indication :

Vous devez trouver :

Message chiffré

WHVWRQVFHSURJUDPPHSRXUYRLUVLOIRQFWLRQQHELHQ

Exercice n° 2 — Chiffrement

Chiffrer le message « TESTONSCEPROGRAMMEPOURVOIRSILFONCTIONNEBIEN », avec la clé 19 .

Indication :

Vous devez trouver :

Message chiffré

MXLMHGLVXIKHZKTFFXIHNKOHBKLBEYHGVMBHGGXUBXG

Exercice n° 3 — Déchiffrement

Déchiffrer le message « WDZIZIOZIYPGZKMJAVZXMDOZIAMVIXVDN » qui a été chiffré avec la clé de chiffrement 21.

Exercice n° 4 — **Bonus**

1. Chiffrer un message avec la clé de votre choix.
2. Recopier ce message et indiquer votre clé de chiffrement dans le Bloc-notes de la classe sur Pearltrees .
3. Déchiffrer les messages de vos camarades.

II Cryptanalyse

La cryptanalyse cherche à déchiffrer un message sans en connaître la clé de chiffrement. On dit alors qu'on tente de « casser » le chiffrement.

Référence historique :

L'un des premiers outils de la cryptanalyse est l'analyse des fréquences.
Les premières traces écrites de cette technique sont l'œuvre d'Al-Kindi (astronome, médecin, mathématicien et linguiste né en 801 à Bagdad). On a retrouvé en 1987, à Istanbul, une copie de son traité « Manuscrit sur le déchiffrement des messages cryptographiques » où il décrit la technique pour déchiffrer un message, suffisamment long, dont on connaît la langue :

- compter le nombre de fois où chaque lettre apparaît dans le texte à déchiffrer,
- classer ces lettres selon leur fréquence d'apparition dans ce texte,
- comparer avec les fréquences l'apparition des lettres dans un texte de la langue.

On sait, par exemple, que les lettres qui apparaissent le plus souvent dans les textes écrits en français sont : E, S, A, I, N ...

Exercice n° 5

Nous avons intercepté un message chiffré sans la clé de chiffrement, à vous de retrouver le message clair.

Message chiffré

LHNOXGMIHNKLTFNLXKEXLAHFFXLWXJNBITZXIKXGGXGMWXLTEUTMKH
LOTLMXLHBLXTNQWXLFXKLJNBLNBOXGMBGWHEXGMLVHFITZGHGLWX
OHRTZXEXGTOBKXZEBLLTGMLNKEXLZHNYYKXLTFXKLTIXBGXEXLHG
MBELWXIHLXLLNKEXLIETGVAXLJNXVXLKHBLWXETSNKFTETWKHBM
LXMAHGMXNQETBLLXGMIBMXNLXFXGMEXNKLZKTGWXLTBEXLUETGV
AXLVHFFXWXLTOBKHGLMKTBGXKTVHMXWXNQVXOHRTZXNKTBEXVHFF
XBEXLMZTNVAXXMOXNEXENBGTZNXKXLBUXTNJNBEXLMVHFBJNXXM
ETBWENGTZTVXLHGUXVTOXVNGUKNEXZNXNEXETNMKXFBFXXGUHBM
TGMEBGYBKFXJNBOHETBMEXIHXMXXLMLXFUETUEXTNIKBGVXWXLG
NXXLJNBATGMXETMXFIXMXXMLXKBMWXETKVAXKXQBEXLNKEXLHET
NFBEBXNWXLANXXLLXLTBEXLWXZXTGMEXFIXVAXGMWXFTKVAXKVA
TKEXLUTNWXETBKX

Indications :

- On pourra se servir du nouveau *sprite* « Laptop », dans lequel il y a un programme demandant à l'utilisateur une lettre et qui calcule la fréquence d'apparition de cette lettre. Pour l'utiliser, il suffit de cliquer dessus.
- On pourra utiliser les fréquences d'apparition des lettres dans un texte écrit en français avec ce lien Wikipedia

Vous pourrez retrouver l'auteur.

Exercice n° 6

Nous avons intercepté un nouveau message chiffré sans la clé de chiffrement, à vous de retrouver le message clair.

Message chiffré

YTZYHJVZNQAJSFNYIJATNWJYIJSYJSIWJHJYYJKJRRJHTVZJYYJJYAFNSJH
JUJWJFQFKTNXWZXJJYGTWSJVZNJSHTZWFLJFNYXFKNQQJIFSXIJXMFGNY
ZIJXITWLZJNQJYIJIJQTDFZYJHJQZCJIJXANQQJXVZNQZNUFWFNXXFNYZ
SJNSKWFHYNTSFQFINLSNYJIJXRŒZWXIJQFHFRUFLSJHJYJRUXUJWIZFI
JXUFWTQJXTNXJZXJXJYSNFNXJXHJYNSYJWNJZWXNINKKJWJSYIZXNJSJ
YXZWYTZYHJRFQFNXJUWTKTSIVZJQMTRRJIJXHMFRUXJUWTZAJQTWXVZN
QXTWYIJXJXMFGNYZIJXQFGTWNJZXJXYTZYHJVZNQFAFNYXZGNIJSSZNJY
IJHTSKZXNTSIJUZNXVZJQVZJXMJZWJXITSSFNYFLJWRFNSQJSANJIJXJW
JYWTZAJWFAJHXTSJSKFSYJYXFUJYNYJATNXNSJSJZYNQUFXJYJFRTZWJZ
CIJHJYYJIJWSNJWJNQQFZWFNYJSHTWJHMJWHMJJUTZWXJINXYWFNWJJYW
JRJYYWJXJXJXUWNYXIFSXQJZWFXXNJYYJFHHTZYZRJJ

Vous pourrez retrouver l'auteure.

Exercice n° 7 ★★

Nous avons intercepté un nouveau message chiffré sans savoir comment il a été chiffré, à vous de retrouver le message clair.

Message chiffré

KVNKLRBNDMQRSFDKORQVDERKORSKRSOERLRKKRURPPRLVBN
RKKRRKQFDSRLRYRERFMFUVDHENHRRKIVESRBNDRSLVNEFXR
FDKHFUDMMROFSHORHAFIDKNORHOVEXNRDMRKORORMVZFNKR
LRMNWRORHQDMMRHBNDMNDYFEFDHHFDKNSRDSUEFLKDVSFMF
ODXSDKRORHPŒNEHORMFLFPYFXSRLRKRPYHYREONFORHYFEV
MRHVDHRNHRHRKSDFDHRHLRKDSKREDRNEHDODUURERSKONHD
RSRKHNEKVNKLRPFMFDHRYEVUVSOBNRMAVPPRORHLAFPYHRY
EVNQRMVEHBNDMHVEKORHRHAFIDKNORHMFIVEDRNHRHKVNKL
RBNDMFQFDKHNIDORSSNDRKORLVSUNHDVSORYNDHBNRMBNRH
ARNERHOVSSFDKFXREPFDSMRSQDRORHRERKEVNQREFQRLHVS
RSUFSKRKHFYRKDKRQVDHDSRSRNKDMYFHRKRFPVNERNWORLR
KKRORESDRERDMMFNEFDKRSLVERLARELARRYVNEHRODHKEFD
ERRKERPRKKERHRHRHYEDKHOFSHMRNEFHHDRKKRFLLVNKNPRR

Vous pourrez retrouver l'auteure.