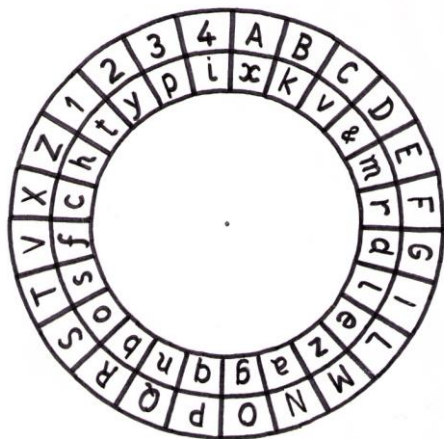




Le cadran d'Alberti (chiffrement poly-alphabétique)



Cadran d'Alberti

BqxbGqvgiMteRkomcoyvXilya ?

Niveau de difficulté : [Primaire, collège, lycée]

Durée de l'activité : [20 minutes]

Nombre de participants : [1 à 5 personnes]

Public cible : [10 ans minimum et pour tout public]

Coût estimé : [5 euros par cadran]

Logistique : [tables/chaises]

MATÉRIEL NÉCESSAIRE

- Deux images du cadran sur deux fiches de carton de diamètres différents
- Une épingle
- Un morceau de bouchon de liège ou de plastique
- Papier et crayon
- Un ou plusieurs messages déjà écrits à décrypter

OBJECTIFS PÉDAGOGIQUES

- **Compétences développées :** La convention secrète est une lettre convenue, par exemple dans cet exemple le « K ».
- **Concepts abordés :** Chiffrement / déchiffrement poly-alphabétique en utilisant les cadrans.
- **Applications pratiques :** Déchiffrer une phrase en tenant compte de la convention secrète et des majuscules et minuscules. Écrire une phrase à déchiffrer en choisissant les lettres majuscules pour le positionnement du cadran interne et des lettres minuscules pour le message.



MODE D'EMPLOI

Le cadran est constitué de deux disques. L'un, fixe, comporte les lettres du clair en majuscule dans l'ordre alphabétique. Le disque mobile comporte les lettres du cryptogramme en minuscule.

1. **Étape de préparation** : Les deux correspondants doivent disposer chacun d'un cadran identique. Ils conviennent d'une lettre, par exemple le « *k* ». Dans le cryptogramme, la première lettre écrite en majuscule, par exemple le *B* indiquera qu'il faut placer le « *k* » en face de cette lettre.

Prévoir des phrases chiffrées.

2. **Chiffrement** : Choisir une lettre majuscule, noter cette lettre dans le cryptogramme. Faire tourner le cadran pour placer la lettre convenue sous cette lettre. Noter ensuite les lettres minuscules en face des lettres majuscules du clair. Au bout de quelques lettres, choisir une autre lettre majuscule et recommencer.

3. **Déchiffrement** : A chaque lettre majuscule, positionner la lettre convenue du cadran interne sous cette lettre sur le cadran externe. Écrire les correspondances de chaque lettre minuscule entre le grand et le petit cadran ainsi positionnés. A la lettre majuscule suivante, refaire tourner le cadran pour mettre la lettre convenue en face de la lettre majuscule.

SCÉNARIO D'ANIMATION

Introduction (5 min) Donner une phrase chiffrée avec les majuscules et les minuscules, la lettre convenue et obtenir la phrase en clair en tenant compte de la lettre choisie (ici le « *K* ») du décalage avec des lettres majuscules et la correspondance pour les lettres minuscules. Inversement, écrire une phrase en clair, puis obtenir la nouvelle phrase « chiffrée ».

- **Accroche pour présenter l'activité** : Dire que cela compliquait le chiffre de César reposant sur un simple décalage. Ici c'est du chiffrement poly-alphabétique.

- **Éléments de langage pour introduire le concept** : Qu'est qu'un chiffrement poly-alphabétique.

Démonstration (10 à 30 min)

- **Instructions pour présenter l'outil** : Montrer une phrase chiffrée, avec majuscules et minuscules

- **Exemple simple à réaliser devant les participants** : Déchiffrer une phrase chiffrée simple

Déchiffrer un message donné en mettant une lettre, par exemple le *K* sous le *B*, écrire la correspondance avec les lettres minuscules, puis placer le *K* sous le *G* puis sous le *M* etc :
BqxboGqvgiMteRkomcoyvXilya

Conclusion (5 min)

- **Questions à poser pour vérifier la compréhension** : Dire que la convention secrète repose sur la possession de deux cadrans identiques pour chacun des correspondants et sur la convention d'une lettre, dans cet exemple le « *k* ».

- **Lien avec la cybersécurité moderne** : chiffrement



CONSEILS POUR L'ANIMATEUR

- **Astuces pour faciliter l'animation** : Très facile, découper en amont de l'animation les deux disques de carton et les assembler avec l'épingle sur le bouchon
- **Adaptations possibles selon le public** : Convient aux jeunes, de 7 à 77 ans et plus

Un CONTEXTE HISTORIQUE

A la renaissance italienne (13ème siècle), plusieurs savants ont proposé des réponses à la sensibilité des chiffrements mono-alphabétiques à l'analyse des fréquences. Cette dernière était pratiquée dans le monde arabe depuis longtemps. Elle a probablement été introduite en occident à l'occasion des croisades.

Né à Florence en 1404, Leon Battista Alberti représente, comme Léonard de Vinci l'idéal de l'homme universel qui prévalait à la renaissance italienne. Il est surtout connu comme architecte, mais fut également peintre, compositeur, poète, philosophe, organiste.

Il a inventé le cadran chiffant qui porte aujourd'hui son nom et qui constitue le premier code poly-alphabétique. L'idée est de changer d'alphabet de substitution au cours du message.