

FICHE PÉDAGOGIQUE

OUTILS DE CHIFFREMENT - COMMISSION JEUNES ARCSI

Nom de l'outil : **La Scytale**



Niveau de difficulté : [Primaire, collège, lycée]

Durée de l'activité : [20 minutes]

Nombre de participants : [1-20 personnes]

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

Coût estimé : [20 euros/coûts variables/coût par participant : 5 euros]

Logistique : [1table/1chaise]

MATÉRIEL NÉCESSAIRE

- Six bâtons de deux diamètres différents
- Deux rubans déjà écrits
- Deux rubans vierges
- Feutre effaçable

OBJECTIFS PÉDAGOGIQUES

-
- [Compétences développées] : Reconnaître que la convention secrète est le diamètre du bâton



- [Concepts abordés] : Chiffrement / déchiffrement connaissant le diamètre du bâton ; décryptement en découvrant le diamètre à l'aide d'un cône qui présente donc tous les diamètres possibles]
- [Applications pratiques] Enroulement : déroulement du ruban entourant le bâton. Utilisation du cône pour trouver le bon diamètre du bâton.

MODE D'EMPLOI

1. [Étape de préparation] : Faire choisir un des bâtons
2. [Étape d'utilisation] :
 - Enrouler le ruban sur le bâton
 - Ecrire un texte longitudinalement sur le ruban
 - Dérouler le ruban écrit et faire constater que les lettres ne mènent pas au message.
 - Constater que le texte devient clair sur le ruban si on choisit le bon bâton (le bon diamètre)
3. [Méthode de chiffrement] : Le texte du ruban n'est pas chiffré, mais les lettres apparaissent sans signification sur le ruban déroulé.
4. [Méthode de déchiffrement] : Enrouler le ruban sur le bâton du bon diamètre et lire le texte dans le sens longitudinal du bâton.

SCÉNARIO D'ANIMATION

Introduction (2 min)

- [Accroche pour présenter l'activité] On va écrire un message en clair et constater que ses lettres ne donnent aucune signification sauf quand on sait résoudre le message en enroulant le ruban sur la bonne scytale.
- [Éléments de langage pour introduire le concept] On chiffre et on déchiffre en enroulant et déroulant le ruban. On décrypte en retrouvant la scytale qui a le bon diamètre grâce au cône.

Démonstration (1 à 5 min)

- [Instructions pour présenter l'outil] Explication que le secret réside dans le diamètre du bâton.
- [Exemple simple à réaliser devant les participants] Le ruban enroulé autour de la scytale, on écrit un petit texte. On déroule le ruban, et on fait constater que le ruban contient des lettres mais qui ne permettent pas de trouver le message.



On enroule le ruban sur une mauvaise scytale (pas le bon diamètre) et on fait constater que les lettres ne donnent pas de signification. On déroule puis enroule le ruban sur la scytale qui a le bon diamètre et on retrouve le message.

Mise en pratique (10 min)

- [Exercices progressifs à proposer]

Donner un ruban déjà écrit que les participants tentent de déchiffrer. Ensuite, on écrit un mot, puis on écrit une phrase.

- [Points d'attention particuliers] Peut-être écrire plutôt le message en lettres majuscules pour éviter que, enroulé sur la bonne scytale, le message ne soit pas incompréhensible suite à une mauvaise écriture.

Conclusion (1 à 10 min)

- [Questions à poser pour vérifier la compréhension] Comment savoir sur quelle scytale enrouler le ruban (grâce au cône).
- [Lien avec la cybersécurité moderne] Manipulation dans la Grèce antique aux environs de 500 avant J.C. Rien à voir avec des algorithmes de chiffrement.

CONSEILS POUR L'ANIMATEUR

- [Difficultés fréquemment rencontrées] Quand un ruban est utilisé, effacer les lettres pour permettre de recommencer.
- [Astuces pour faciliter l'animation] Faire comprendre que le cône est indispensable pour le décryptement (trouver le bon diamètre de la scytale).
- [Adaptations possibles selon le public] 1 seul mot à écrire (un prénom) pour les petits ; une phrase entière pour les grands.

POUR ALLER PLUS LOIN

- [Références bibliographiques]
- [Activités complémentaires]
- [Ressources en ligne]

CONTEXTE HISTORIQUE

Selon Aulu Gelle (115~120, 180). Nous sommes dans la Grèce antique aux environs de 500 avant J.C. Lorsqu'un général part en campagne, il emporte avec lui une scytale. Ce nom est celui donné aux bâtons que se transmettent les coureurs de relais lors des jeux olympiques. Les magistrats de la ville gardent avec eux un bâton parfaitement identique à celui du général.

Lorsque l'État doit communiquer aux généraux une information secrète qui ne doit à aucun prix être connue de l'ennemi, ils roulent un ruban de parchemin autour de la scytale en joignant soigneusement les bords de manière à ne laisser aucun jour. Le ruban est collé à la scytale à l'aide de cire.

Un message est alors écrit transversalement sur le ruban. La bande ainsi chargée d'écriture est alors ôtée de la scytale et envoyée au général par un coursier. La bande ainsi séparée de la scytale ne montre que des fragments de lettres tronquées et cassées qui ne présentent aucune signification.

Si le ruban tombe aux mains de l'ennemi, celui-ci ne reconnaîtra rien de ces traits incohérents.

Arrivé à destination, le coursier présente le ruban au général qui est au fait du procédé. Il enroule le ruban autour de la scytale comme l'ont fait les expéditeurs, joignant les bords bout à bout en ajustant le ruban à l'aide de cire.

Grâce à la dimension rigoureusement égale du diamètre des deux cylindres, les caractères se ramènent au même point et présentent à nouveau la forme des lettres complètes et le général parvient à les lire.