

Nostr

En s'appuyant sur les activités précédentes consacrées à la confiance, à la transmission de messages et à leur interception, les élèves comparent désormais le transfert d'informations en clair à la communication chiffrée. Les élèves découvrent d'abord que la transmission d'informations nécessite de faire confiance à des intermédiaires et que les messages peuvent être interceptés ou altérés. Ils utilisent ensuite des roues de chiffrement pour protéger leurs messages, et constatent ainsi que les informations peuvent rester confidentielles même lorsqu'elles transitent par des canaux non fiables ou publics. Prérequis 4.2 - Téléphone 4.3 - Les cypherpunks écrivent du code

 TYPE D'ACTIVITÉ Simulation · Activité manuelle · Jeu	 DURÉE 50–60 min	 PARTICIPATION Petits groupes
---	--	---

OBJECTIFS

À l'issue de cette activité, les apprenants seront capables de :

- Examinez en quoi la transmission d'informations repose sur la confiance accordée aux intermédiaires
- Prendre conscience de la manière dont les messages peuvent être déformés ou altérés lorsqu'ils sont transmis ouvertement ;
- Il faut comprendre que le chiffrement protège les informations même lorsque les intermédiaires ne sont pas fiables.
- Savoir coder et décoder du vocabulaire à l'aide d'une roue de chiffrement.

MATÉRIEL

- Fiches de mots ou de phrases préparées en vue de leur diffusion
- Modèles de roues de chiffrement pour chaque élève (voir annexe A) — [A · Modèle de roue de chiffrement](#)
- Fiches ou feuilles vierges pour la transcription
- Crayons ou feutres
- Exemples de messages simples et complexes (voir annexe B) (*facultatif*)
- Ciseaux
- Goupilles fendues ou clous pour roues de chiffrement
- Un espace de classe ouvert propice à l'activité physique
- Minuterie (*facultatif*)

DÉROULEMENT

OUVERTURE

1. Aménagez la salle en plaçant deux tables par équipe, bien espacées l'une de l'autre, afin de respecter la distanciation physique.
2. Disposez des cartes de message ouvertes sur chaque table d'invités.
3. Préparez le matériel nécessaire à la roue de chiffrement, mais gardez-le à l'abri des regards jusqu'à la phase 2.

AVANT L'ACTIVITÉ

5 minutes

1. Demandez aux élèves de se remémorer l'activité précédente, au cours de laquelle ils devaient chuchoter ou transmettre des messages.
2. Demandez-leur quels problèmes ils ont constatés en matière de confiance, d'erreurs ou d'écoutes involontaires.
3. Rappelez aux élèves que, la dernière fois, ils n'ont pas réussi à préserver la confidentialité de leurs messages.
4. Expliquez-leur qu'aujourd'hui, ils vont vérifier si ce problème peut être résolu.

L'objectif selon les mots de l'étudiant

- « Trouver un meilleur moyen d'envoyer des messages sans que tout le monde doive être considéré comme digne de confiance. »

ACTIVITÉ

40 à 45 minutes

Configuration

1. Répartissez les élèves en groupes de trois.
2. Attribuez les rôles : le joueur 1 est l'expéditeur, le joueur 2 est le coureur, le joueur 3 est le destinataire.
3. Expliquez que les rôles resteront les mêmes tout au long de l'activité.

Modèle

1. Faites une brève démonstration d'une séance de dictée à la volée à partir d'un message ouvert.
2. Précisez que le messenger doit mémoriser et répéter le message à la lettre.
3. Rappelez aux élèves que toute personne se trouvant à proximité peut entendre le message.

Phase 1 – Transmission ouverte (confiance requise)

1. Le joueur 1 lit en silence le message affiché sur la table de l'expéditeur.
2. Le joueur 1 lit discrètement le message au joueur 2 à la table de l'expéditeur.
3. Le joueur n° 2 court vers le joueur n° 3 et lui transmet le message oralement.
4. Le joueur n° 3 note ce qu'il entend.
5. Le joueur 2 peut faire des allers-retours autant que nécessaire.
6. La première équipe à réussir à transmettre le message remporte la victoire.

Discussion sur les points de contrôle

- Demandez si le message final correspondait à l'original.
- Demandez si les coureurs ont entendu des conversations d'autres équipes.
- Demandez si le messenger avait le pouvoir de modifier le message.
- Insistez sur le fait que le système ne fonctionnait que si le coureur était digne de confiance.

Phase 2 – Transmission cryptée (confiance réduite)

1. Distribuez les éléments nécessaires à la fabrication des roues de chiffrement et laissez les élèves les assembler.
2. L'expéditeur et le destinataire conviennent en privé d'un décalage d'une lettre à l'aide de la roue.
3. Le joueur 1 code un nouveau message à l'aide du chiffrement convenu.
4. Le joueur 2 ne transmet que le message codé sans en connaître la signification.
5. Le joueur n° 3 transcrit et décode le message à l'aide de la roue de chiffrement.

Règlement du concours

- Les équipes marquent des points lorsqu'elles décodent correctement.
- La rapidité et la précision sont toutes deux importantes.
- Les coureurs n'ont pas le droit d'apprendre le code.

Réflexion

1. Demandez ce qui a changé entre la transmission en clair et la transmission cryptée.
2. Demandez-vous s'il était encore nécessaire de faire confiance au coureur.
3. Demandez qui contrôlait l'accès au message à chaque étape.

SUIVI

5 à 10 minutes

1. Rappelons que les activités précédentes ont montré comment des messages peuvent être interceptés ou modifiés.
2. Vérifiez que ce cryptage permet aux messages de circuler en toute sécurité dans l'espace public.

3. Faites le lien avec la question du choix entre les informations publiques et privées.

FERMER

5 minutes

1. Rassemblez le matériel mis à disposition et remettez la salle en ordre.
2. Permettez aux élèves de conserver leurs roues de chiffrement.
3. Message final à l'attention des élèves : « Vous n'avez pas besoin de faire confiance à tout le monde lorsque vos messages sont protégés. »

NOTES

Gestion de la classe

- Les élèves plus âgés peuvent choisir leur rôle dans le relais
- Surveillez les itinéraires de course et imposez la marche si nécessaire.
- Insistez sur le fait que les erreurs sont normales et font partie intégrante de l'apprentissage.

Activités complémentaires et activités avec des éponges

- Changez de rôle et recommencez avec un nouveau code.
- Augmentez la longueur des messages ou ajoutez des messages leurres.

Différenciation

- Élèves plus jeunes : mots isolés et décalage fixe des lettres.
- ELL/Accessibilité : tableaux de l'alphabet et rythme plus lent.
- Sécurité : règles de circulation claires et utilisation des outils sous surveillance.