LA TECHNOLOGIE AU COLLÈGE

Sciences et Techniques Industrielles

Portail national de ressources - éduscol

CYCLE 4	**Comment s'assurer d'un usage raisonné des objets communicants ?**	NIVEAU QUATRIÈME

Présentation de la séquence

Cette séquence a pour objectif de sensibiliser les élèves aux risques liés à l'utilisation des environnements numériques.
Elle permet d'identifier les risques liés aux données personnelles et aux traces numériques afin de les aider à appliquer des pratiques permettant un usage raisonné des objets communicants et des environnements numériques.

Thème abordé :	Les objets et les systèmes techniques : leurs usages et leurs interactions à découvrir et à analyser
Attendu de fin de cycle :	Décrire les liens entre usages et évolutions technologiques des objets et des systèmes techniques

Compétences	**Connaissances**
Identifier et appliquer les règles pour un usage raisonné des objets communicants et des environnements numériques (propriété intellectuelle, identité numérique, témoins de connexion, géolocalisation).	Cybersécurité : protection des données personnelles, traces numériques (témoins de connexion, géolocalisation), identification, authentification, respect de la propriété intellectuelle.
Identifier les avantages et les inconvénients associés aux évolutions technologiques et informatiques.	Cyberviolence : usurpation d'identité, usage détourné.

Thème abordé :	Structure, fonctionnement, comportement : des objets et des systèmes techniques à comprendre
Attendu de fin de cycle :	Comprendre et modifier un programme associé à une fonctionnalité d'un objet ou d'un système technique

Compétences	**Connaissances**
Analyser les données et en déduire des modifications à apporter au programme.	-instructions itératives ;
Compléter un programme pour répondre à une fonctionnalité d'un OST.	-instruction conditionnelle ;
Tester et valider, dans un environnement simulé ou réel, une modification d'un programme.	-entrées ou sorties d'un programme (données issues par exemple de capteurs IHM et sorties pouvant être en lien avec un actionneur, fichiers).

PROPOSITION DE DÉROULEMENT DE LA SÉQUENCE

Séance 1 et 2 – 160 min – 1H20 x 2

Ces deux séances permettront aux élèves d'identifier les risques liés aux données personnelles et aux traces numériques comme les cookies de navigation et la géolocalisation afin de les aider à appliquer des pratiques permettant un usage raisonné des objets communicants et des environnements numériques.

Activité 1 (40 min)

Cette activité a pour objectif de mesurer informellement les acquis des élèves puis de proposer un fil conducteur à la séquence afin de donner du sens aux activités réalisées.

- **Mise en situation** (15 min)

  Les élèves visionnent la vidéo (4mn41) en classe entière :
  https://www.youtube.com/watch?v=PZmgvHEKy-Y
  Les élèves contribuent globalement à l'oral à expliciter le vocabulaire.
  L'enseignant synthétise les échanges et note au tableau les définitions à écrire dans le classeur : *objet communicant et environnement numérique*.

  Qu'est-ce qu'un objet communicant ?
  Un objet communicant est un appareil capable de se connecter à un autre ou à Internet. Exemples : téléphone portable, montre connectée, enceinte intelligente, ordinateur / tablette, caméra de surveillance Wi-Fi.
  Qu'est-ce qu'un environnement numérique ?
  C'est un ensemble d'outils et de services numériques qu'on utilise souvent ensemble : espace numérique de travail (ENT), messagerie, services de stockage, réseaux sociaux, jeux en ligne.

  L'enseignant dégage avec les élèves la problématique en les questionnant sur les risques d'utiliser un objet communicant.

- **Problématique**

  L'enseignant note la problématique au tableau :
  Quels sont les règles à respecter pour un usage raisonné des objets communicants dans un environnement numérique ?

- **Investigations** (20 min)

  La classe se sépare en équipe.
  Le document professeur « **S1-A1-Situations »** proposent des situations à adapter à son environnement.
  Chaque équipe traite une situation différente en respectant la même procédure :
  - Coller la situation dans son classeur ;
  - Identifier les risques pour nos données personnelles dans la situation proposée ;
  - Proposer des solutions ou pistes de solutions pour limiter les risques identifiés.

  Un rapporteur est désigné et présentera la situation en 2 minutes maximum.

- **Bilan intermédiaire** (5 min)

  L'enseignant complète la présentation des groupes si nécessaire.
  Le document élève « **S1-A1-Bilan** » est distribué. Il contient le corrigé des situations précédentes.

Activité 2 (55 min)
Cette activité a pour objectif de définir un cookie, de montrer le fonctionnement des cookies et de sensibiliser les élèves à la protection de leurs données personnelles.

- **Mise en situation** (5 min)
  Les élèves visionnent en classe entière la vidéo (1mn06) : **Qu'est-ce qu'un cookie ?**
  https://video.cnil.fr/w/oZnjFZXdwn24YFfdApCAfP
  Suite aux échanges avec la classe, l'enseignant note au tableau le vocabulaire utilisé : *cookies.*
  Les élèves proposent individuellement une définition sur leur classeur.

- **Problématique 1**
  Comment fonctionnent les cookies ?

- **Investigations** (10 min)
  La manipulation s'effectue à l'aide d'un simulateur car il est très difficile d'identifier les cookies utilisés par les sites commerciaux. De plus, accéder aux cookies d'un autre utilisateur ne respecterait pas le RGPD.
  En équipe, sur un ordinateur, les élèves ouvrent la page html avec le navigateur chrome : **Test-cookies.html**
  Les élèves effectuent les manipulations en s'aidant :
  - de la vidéo (58s) : **https://podeduc.apps.education.fr/video/106849-aide_cookies/**
  - ou du document ressource : **Aide_cookies.pdf**

  Les élèves doivent expliquer comment sont créés des fichiers (cookies) et comment ils peuvent être effacés.
  Pour conclure, les élèves expliquent quelles informations sont stockées par un site internet qui utilise ce type de cookies.

- **Problématique 2** (30 min)
  Comment gérer sa vie privée en ligne ?
  L'objectif pour les élèves est de comprendre le fonctionnement de la navigation privée. Les cookies continuent d'être stockés pendant la visite des pages internet mais ils disparaissent une fois le site fermé.
  En groupe, sur un ordinateur, les élèves ouvrent la page html : **Test-navigation_privee.html**
  Les élèves effectuent les manipulations en s'aidant :
  - de la vidéo (1mn11) : **https://podeduc.apps.education.fr/video/106850-aide_navigation_privee/**
  - ou du document ressource : **Aide_navigation_privee.pdf**

  En groupe, les élèves doivent définir une **configuration** sur le navigateur pour limiter les cookies en s'aidant de la ressource vidéo : **Effacer_les_cookies (3mn50)**
  https://www.dailymotion.com/video/xw48jr
  L'enseignant questionne par groupe les élèves sur leur configuration et propose des ajustements. (Remarque : Cette méthodologie assure le respect du RGPD.)

- **Bilan intermédiaire** (10 min)
  Les définitions sont notées dans le classeur.
  Cookies de connexion
  Les témoins de connexion sont des petits fichiers stockés sur l'appareil d'un utilisateur. Ces témoins permettent à un site web de se souvenir de l'utilisateur et de ses actions au fur et à mesure de sa navigation.

Les élèves visionnent en classe entière la vidéo (2mn55) :
Cookies-Les_espions_du_net
https://video.cnil.fr/w/iF5m6HgnshDNRx2dc1gRbJ

Activité 3 (65 min)
Cette activité a pour objectif de sensibiliser les élèves à la protection de leurs données personnelles et principalement les risques de la géolocalisation.

- **Mise en situation** (10 min)
  Les élèves visionnent en classe entière la vidéo (4mn51) :
  Les_dangers_de_la géolocalisation
  https://www.tf1info.fr/high-tech/videos/video-les-dangers-de-la-geolocalisation-comment-nos-applis-nous-traquent-2270-2333151.html
  Suite aux échanges avec la classe, l'enseignant note au tableau le vocabulaire utilisé : *géolocalisation*
  Les élèves proposent une définition sur leur classeur.

- **Problématique**
  Comment gérer la protection de ses données personnelles et la géolocalisation ?

- **Débat :** 20 min de préparation puis 20 min de débat.
  Sous forme d'un débat, les élèves doivent répondre à la question :
  Quels sont les avantages et les risques pour un utilisateur de partager sa géolocalisation ?
  L'organisation suivante doit mettre en évidence l'intérêt d'une réflexion construite en amont du débat.
  La classe est divisée en 2 groupes : POUR la géolocalisation et CONTRE.
  L'enseignant distribue des cartes issues du document : « **S1-A3-Cartes** »
  A partir des sites suivants et de toutes les ressources internet trouvées par les élèves, chaque groupe prépare des arguments courts et justifiés qu'il écrit.
  Attention, un seul couple par carte (argument + justification). Le même argument peut être utilisé plusieurs fois en modifiant la justification.

  Ressources initiales :
  https://cnil.fr/fr/partage-geolocalisation-conseils-de-la-cnil
  https://cybersecurite.orange.fr/la-cybersecurite/protection-des-donnees/geolocalisation-danger-securite-smartphone-localisation.html

  Le hasard désigne le groupe qui débute le débat. Il débute en utilisant une de ses cartes arguments.
  Pour répondre, le groupe « adverse » doit utiliser une carte argument. Et ainsi de suite.
  Lorsqu'un groupe n'a plus de carte, il ne peut plus participer au débat. L'autre groupe peut présenter toutes ses cartes, une par une sans opposition.
  L'enseignant s'assure du respect des règles du débat.
  L'enseignant clos le débat en demandant à chaque participant de se positionner, suite aux échanges et à leur conviction, POUR ou CONTRE la géolocalisation.

- **Bilan** (5 mn)
  Témoins de géolocalisation
  Les témoins de géolocalisation permettent de collecter des informations sur la localisation géographique d'un utilisateur. Ces informations peuvent être obtenues par plusieurs moyens, tels que les adresses IP, le GPS des appareils mobiles ou des réseaux Wi-Fi à proximité.

Piste de conclusion du débat :

*La géolocalisation est à la fois **une opportunité majeure** pour la science et la société, et **un risque important pour les libertés individuelles**.*
*Le débat repose donc sur une **tension permanente entre utilité et protection**, nécessitant des solutions techniques, des garde-fous juridiques, et une **réflexion citoyenne**.*

- **Synthèse** (10 mn)
  Le document synthèse est distribué. Il est lu et explicité en classe.
  S1S2-A123-Synthèse.docx

Ressources pour le professeur	Ressources pour les élèves
Fichiers : S1-A1-Situations.pdf (+docx) S1-A1-Bilan.pdf (+docx) S1-A3-Cartes.pdf (+docx) Aide_cookies.docx Aide_navigation_privee.docx S1S2-A123-Synthèse.pdf (+docx) Liens Vidéo : https://www.youtube.com/watch?v=PZmgvHEKy-Y https://video.cnil.fr/w/oZnjFZXdwn24YFfdApCAfP https://video.cnil.fr/w/iF5m6HgnshDNRx2dc1gRbJ https://www.tf1info.fr/high-tech/videos/video-les-dangers-de-la-geolocalisation-comment-nos-applis-nous-traquent-2270-2333151.html Liens utiles : https://www.cnil.fr/fr/cookies-et-autres-traceurs https://www.cnil.fr/fr/mes-demarches/les-droits-pour-maitriser-vos-donnees-personnelles Autoformation : 1 - Fiche-Pratique_Objets-Connectes.pdf 2 - Memo_Objets-Connectes	Fichiers : Test-cookies.html Aide_cookies.pdf Test-navigation_privee.html Aide_navigation_privee.pdf Liens Vidéo : https://podeduc.apps.education.fr/video/106849-aide_cookies/ https://podeduc.apps.education.fr/video/106850-aide_navigation_privee/ https://www.dailymotion.com/video/xw48jr Liens utiles : https://cnil.fr/fr/partage-geolocalisation-conseils-de-la-cnil https://cybersecurite.orange.fr/la-cybersecurite/protection-des-donnees/geolocalisation-danger-securite-smartphone-localisation.html

Séance 3 – 80 min - 1H20

Cette séance permet aux élèves d'appréhender les technologies qui permettent la transmission sans fil des données. Ils vont être sensibiliser à leurs avantages, leurs limites d'utilisation et les risques de sécurité qu'ils peuvent générer.

- **Situation déclenchante (5 min) :**
  "Quels sont les objets ou les systèmes techniques utilisés au quotidien qui communiquent entre eux ? Quels moyens de liaison utilisent-ils ? "
  Suite aux échanges avec la classe, chaque élève écrit les questions et les réponses validées par l'enseignant.
  Exemples à proposer si nécessaire :
  badges d'accès RFID, paiements sans contact NFC, smartphones pour appels 5G-WIFI, casque audio Bluetooth ou filaire.

Activité 1 : analyse des caractéristiques et des risques des liaisons sans fil (15 min)

L'enseignant questionne la classe sur les caractéristiques d'une liaison sans fil sans donner de réponse.
En équipe, les élèves visionnent la vidéo (7mn03) : **le transfert de données sans fil.** https://www.youtube.com/watch?v=-hXkrpEkPUQ puis complètent le tableau et le schéma distribués.
Document élève : S3-A1-à compléter.pdf

En classe entière, l'enseignant corrige le tableau et le schéma.

Activité 2 : comment fonctionne la technologie RFID ? (50 min)
Cette activité a pour objectif, en prenant l'exemple de la RFID, d'analyser le fonctionnement d'une liaison sans fil pour mieux comprendre les risques.

En effet, l'usage raisonné des objets communicants et des environnements numériques, en particulier avec des technologies comme la **NFC (Near Field Communication)**, **RFID (Radio Frequency Identification)** et **Bluetooth**, nécessite une approche avertie pour la sécurité.

- **Mise en situation** (10 min)
  Les élèves visionnent en classe entière la vidéo déclenchante (2mn05) : **paiement sans contact et ses risques.** https://www.youtube.com/watch?v=vJZ2cuzN2WM

  L'enseignant dégage avec les élèves la problématique en les questionnant sur les risques d'utiliser un objet communicant utilisant le RFID.

- **Problématique : Comment fonctionne la technologie RFID ? Quels sont les risques d'utilisation ?**

- **Investigations** (25 min)
  La classe se sépare en équipe.
  Chaque équipe a pour objectif de « programmer » un TAG NFC en carte de visite Intelligente à l'aide d'une tablette ou d'un smartphone tout en sécurisant les données et l'utilisation de la carte.
  Après la programmation du TAG, l'utilisateur devra accéder aux informations de la carte de visite virtuelle en « badgeant » le TAG.

  L'enseignant distribue des cartes de visites préparées en amont :
  - un tag collé par carte,
  - l'information que doit renvoyer la carte (nom, prénom, numéro virtuel),
  - le mot de passe à utiliser éventuellement.

Les élèves effectuent les manipulations en s'aidant :
- du document ressource : **Utiliser l'application NFC Tools pour écrire sur un TAG NFC : *texte, URL, lien vidéo, application, e-mail, contact, tel, …* et définir un mot de passe**
- de la vidéo : écrire sur un tag NFC (1mn13)
https://podeduc.apps.education.fr/video/111516-ecrire-sur-un-tag-nfc/
- de la vidéo : protéger le tag par mot de passe.mp4 (1mn42)
https://podeduc.apps.education.fr/video/111517-proteger-le-tag-par-un-mot-de-passe/

Remarque : l'enseignant n'impose pas de protéger son TAG. Il peut aussi s'il le souhaite, circuler et modifier « discrètement » les tags de groupe non sécurisé.

En classe entière, l'enseignant badge les cartes et montrent l'information qui s'affiche. L'enseignant questionne la classe sur les risques de badger un TAG NFC. Exemples attendus : modification de l'information, redirection vers un espace dangereux, interception de l'information…

L'enseignant rappelle les domaines d'applications de la technologie NFC et les risques :

Paiement sans contact, paiement mobile, cartes de transport, connexion avec un accessoire, transfert de données, tags (gestion du stock, gestion d'accès à un endroit).

Les risques de sécurité les plus courants rencontrés dans l'utilisation du NFC sont les fraudes et le piratage informatique. À noter cependant que de telles attaques nécessitent une très grande proximité avec la cible, ce qui rend la réalisation du piratage difficile en conditions réelles.

- **Bilan intermédiaire : les clés pour un usage raisonné de la RFID** (15 min)

Les élèves notent les conseils pour une utilisation sécurisée :

- Placer sa carte de crédit dans un étui bloquant les ondes électromagnétiques lorsqu'on ne l'utilise pas (pas derrière son smartphone)
- Ne pas badger de TAG inconnu
- Désactiver le NFC sur son smartphone après chaque usage.

BILAN (10 min)
Comprendre les caractéristiques techniques et les enjeux de cybersécurité d'une liaison pour en faire une utilisation raisonnée.

Le document élève « **S3-Bilan.pdf** » est distribué. Le tableau est complété en classe entière.

Ressources pour le professeur	Ressources pour les élèves
Vidéo déclenchante : https://www.youtube.com/watch?v=-hXkrpEkPUQ Fichiers : S3-A1 Correction.pdf (+docx) S3 Bilan.pdf (+docx) S3 Bilan Correction.pdf (+docx) S3 Synthese.pdf(+docx) Autoformation : Fiche_fuiteDonnéesPersonnelles_Particuliers.pdf Fiche_QuefairecyberAttaque_Dirigeants.pdf	Vidéos : https://podeduc.apps.education.fr/video/111516-ecrire-sur-un-tag-nfc/ https://podeduc.apps.education.fr/video/111517-proteger-le-tag-par-un-mot-de-passe/ Fichiers : S3-A1 à compléter.pdf (+docx) S3-A2 NFCTools.pdf (+docx) Lien utile : NFC tools

Séance 4 – 80 min - 1H20

Prérequis : savoir utiliser le mode radio de la micro-bit (**S4 fiche guide micro-bit radio.pdf**)

L'objectif de la séance est de sensibiliser par l'expérimentation à différentes tentatives de piratage et aux solutions qui peuvent être apportée pour y remédier.

- **Situation déclenchante (5 min) :**

  Les élèves visionnent en classe entière la vidéo déclenchante (3mn42) : https://www.youtube.com/watch?v=wf6TCiF9QiY

  Les élèves doivent définir en notant dans leur classeur ce qu'ils ont compris de la vidéo et ce qu'est une attaque par déni de service *(la correction s'effectuera lors du bilan)*

Activité 1 : Comprendre la mécanique d'une attaque DdoS (20 min)

- **Mise en situation**

  Les élèves sont en équipe.
  Chaque équipe dispose d'1 ou 2 ordinateurs connectés à https://makecode.microbit.org/ et 2 cartes microbit.

- **Problématique**

  Comment fonctionne une tentative d'attaque Ddos ?

- **Investigations**

1. Chaque équipe doit échanger ses prénoms en utilisant un canal radio différent.

Chaque équipe se répartie en 2 groupes : émetteur et récepteur.
Chaque groupe ouvre sur Makecode le programme ressource et modifie le canal radio et les prénoms.
Programmes fournis :
S4-A1 Microbit-emetteur.hex
S4-A1 Microbit-recepteur.hex
Chaque groupe téléverse son programme dans sa carte microbit.

L'équipe vérifie le bon fonctionnement et le présente à son enseignant.

Pour les groupes en avance, il est possible de créer un programme contenant tous les blocs des 2 programmes. Le fonctionnement devient réversible.

2. Tous les groupes modifient le canal radio de leur programme. **Ils utilisent le canal radio 123.**

Chaque groupe téléverse son programme dans sa carte microbit.
L'équipe vérifie le bon fonctionnement et le présente à son enseignant.

L'enseignant questionne les élèves sur le fonctionnement observé. Constat : les informations se croisent et sont lisibles par toute la classe.

3. Le professeur prépare une carte microbit en amont qui émet continuellement « **TECHNO** » sur le canal 123.

Programmes fournis :
S4-A1 Microbit-Prof-hacker.hex

Sans prévenir la classe, l'enseignant démarre sa carte.
L'enseignant questionne les élèves sur le fonctionnement observé.

Le professeur peut être considéré comme un hacker effectuant une attaque (Deni de service ou DDOS), en envoyant continuellement des informations, il sature le réseau et le fonctionnement normal est perturbé.

Suite aux observations, chaque équipe doit proposer des solutions.
L'enseignant note au tableau la problématique de l'activité 2.

Activité 2 : Chercher des solutions afin de sécuriser les échanges. (40 min)

- **Problématique**

Comment échanger des informations en se protégeant d'attaque Ddos ?

- **Investigations**

L'enseignant questionne la classe sur les solutions possibles. Il propose ensuite d'en expérimenter plusieurs.

Solution 1 : ajouter un temps d'attente entre 2 messages

Cette solution doit empêcher une carte de saturer la liaison en envoyant trop de messages radio.

Pour faciliter l'organisation, le fonctionnement est réversible, chaque carte sera programmée pour jouer les 2 rôles. Ainsi les groupes en difficultés pourront utiliser le programme d'un groupe plus avancé.

A partir du document ressource, les groupes doivent compléter le programme fourni afin de respecter le fonctionnement attendu.

Programme fourni :
S4-A2 Microbit-sature-delai-à_modifier.hex

Document ressource :
S4-A2 Ressource fonctionnement attendu.pdf (solution 1).

Chaque groupe téléverse son programme dans sa carte microbit.
L'équipe vérifie le bon fonctionnement et le présente à son enseignant.

L'enseignant remet en fonctionnement sa carte simulant une attaque DDOS.
L'enseignant questionne les élèves sur le fonctionnement observé.
Conclusion possible : le système est très lent. L'attaque DDOS est toujours possible.

Solution 2 : Filtrer les requêtes avec un cryptage simple

Pour faciliter l'organisation, le fonctionnement est réversible, chaque carte sera programmée pour jouer les 2 rôles. Ainsi les groupes en difficultés pourront utiliser le programme d'un groupe plus avancé

Par équipe, les élèves conviennent d'un code à 4 chiffres qui représentera l'information à afficher. (Par exemple : 1234 : PIERRE ou 4567 : JASMIN).
Seul l'équipe connaît le code de cryptage de ses données.

A partir du document ressource, les groupes doivent compléter le programme fourni afin de respecter le fonctionnement attendu.

Programme fourni :
S4-A2 Microbit-cryptage-simple-à_modifier.hex

Document ressource :
S4-A2 Ressource fonctionnement attendu.pdf (solution 2).

Chaque groupe téléverse son programme dans sa carte microbit.
L'équipe vérifie le bon fonctionnement et le présente à son enseignant.

L'enseignant remet en fonctionnement sa carte simulant une attaque DDOS.
L'enseignant questionne les élèves sur le fonctionnement observé.
Conclusion possible : L'attaque DDOS est impossible, mais le système ne permet pas réellement de communiquer car il faut prévoir tous les codes de cryptage lors de la programmation.

Solution 3 : Identifier les requêtes avec un codage simple

Par équipe, les élèves conviennent d'un code à 4 chiffres qui servira à authentifier les informations reçues.
Seul l'équipe connaît le code d'authentification de ses données.

Attention pour faciliter la compréhension des variables, le fonctionnement ne sera PAS réversible.

A partir du document ressource, les groupes doivent compléter le programme afin de respecter le fonctionnement attendu.

Programme fourni :
S4-A2 Microbit-code-émetteur-à_modifier.hex
S4-A2 Microbit-code-récepteur-à_modifier.hex

Document ressource :
S4-A2 Ressource fonctionnement attendu.pdf (solution 3).

Chaque groupe téléverse son programme dans sa carte microbit.
L'équipe vérifie le bon fonctionnement et le présente à son enseignant.

L'enseignant remet en fonctionnement sa carte simulant une attaque DDOS.
L'enseignant questionne les élèves sur le fonctionnement observé.
Conclusion possible : L'attaque DDOS est impossible, et le système permet réellement de communiquer. C'est une version très simplifiée de la méthode utilisée pour communiquer en Wifi.

BILAN (5 min) :

La définition et les propositions de solutions sont notées dans le classeur.
Définition Cybermalveillance.gouv.fr :
Une attaque en déni de service ou DDoS vise à rendre inaccessible un serveur afin de provoquer une panne ou un fonctionnement fortement dégradé du service.

Proposition de solutions :
Les programmes de cybersécurité doivent pouvoir :

- **empêcher** d'envoyer trop de messages pour **saturer** le réseau ;
- vérifier **l'authentification** du message envoyée (ici le code avant le prénom) et donc **filtrer** les envois non autorisés.

Synthèse (10 mn)

Le document synthèse est distribué. Il est lu et explicité en classe.

S4-A12-Synthèse.pdf

Ressources pour le professeur	Ressources pour les élèves
Fichiers : S4 fiche guide radio microbit.pdf (+docx) S4-A2 Ressource Fonctionnement attendu.pdf (+docx) Synthèse S4 microbit.pdf (+docx) Programmes Makecode : S4-A2 Microbit-sature-delai-correction.hex S4-A2 Microbit-cryptage-simple-correction.hex Autoformation : FicheReflexe-DeniService.pdf	Fichiers : S4 fiche guide radio microbit.pdf S4-A2 Ressource Fonctionnement attendu.pdf Programmes Makecode : S4-A1 Microbit-emetteur.hex S4-A1 Microbit-recepteur.hex S4-A2 Microbit-sature-delai-à_modifier.hex S4-A2 Microbit-cryptage-simple-à_modifier.hex Coup de pouce : Programmes correction à distribuer selon les besoins