mallettes
MERITE

itinéraires
en sciences
et techniques :
expérimenter
et comprendre

CLASSES DE CYCLE 4

3e
4e
5e

Technologie

itinéraire

Communication informatique : tout un protocole

Concret pour les élèves

Démarche d'investigation

Clé en main
pour l'enseignant

Matériel dédié

Conçu par des scientifiques
et des enseignants

Testé en classe

mallettes
MERITE

itinéraires
en sciences
et techniques :
expérimenter
et comprendre

La collection

mallettes MERITE

Itinéraires en sciences et techniques : expérimenter et comprendre

Conçues pour les enseignants du CM1 jusqu'à la classe de 3e, les mallettes MERITE sont des ressources pédagogiques abordant plusieurs disciplines et laissant une grande part à l'expérimentation par les élèves. Apprendre en se confrontant au réel, utiliser du matériel approprié, réfléchir et progresser en groupe sur des questions ouvertes issues du quotidien, s'entraîner à raisonner sur des faits et des observations, s'approprier des concepts scientifiques et des savoir-faire techniques, tout cela est au cœur de la collection MERITE.

Des progressions clés en mains pour les enseignants

Chaque mallette MERITE est composée d'un guide pour l'enseignant détaillant l'itinéraire pédagogique réparti en modules et séances et du matériel nécessaire pour réaliser les expériences. Elle constitue ainsi une ressource complète pouvant être utilisée en autonomie et de façon flexible par l'enseignant. Les contenus s'inscrivent dans les programmes scolaires et ouvrent sur la découverte des métiers.

Une approche concrète s'appuyant sur la démarche d'investigation

Les activités de classe s'appuient sur la démarche d'investigation pour encourager l'apprentissage progressif des élèves par l'action. Le matériel fourni est adapté au niveau des élèves et permet de réaliser des activités scientifiques et techniques pour toute une classe, disposée le plus souvent en îlots.

Une collection conçue par des scientifiques et testée en classe

Riche de 12 thématiques, cette collection de mallettes pédagogiques a été conçue par des scientifiques de 7 établissements d'enseignement supérieur, en co-construction avec des enseignants, et testée dans des classes de cycle 3 et 4 durant trois années scolaires.

Une collection au service de la diffusion de la culture scientifique et technique

La collection MERITE encourage la diffusion et la diversification de la culture scientifique et technique et s'adresse à tous. Les thématiques proposées se font parfois écho en utilisant des outils communs (outils mathématiques, utilisation de protocoles d'expérimentation…), démontrant ainsi que les disciplines ne sont pas cloisonnées. L'approche proposée permet de construire des apprentissages utiles au citoyen : réflexion, esprit critique, confiance en soi, créativité et innovation pour devenir capable de choix éclairés par des connaissances et compétences scientifiques et techniques bien comprises.

Cette collection est le fruit du projet MERITE (2015-2020) coordonné par IMT Atlantique en partenariat avec 7 établissements d'enseignement supérieur du Grand Ouest et le Rectorat de l'Académie de Nantes. MERITE a été financé au titre du Programme d'Investissements d'Avenir lancé par l'Etat, ainsi que par le Fonds européen de développement régional, la Région des Pays de la Loire et le groupe Assystem.

Sommaire

Introduction 9

Matériel 15

Séances 19

Itinéraire pédagogique 21

MODULE 1 **LA COMMUNICATION HUMAINE** 22

Séance 1 **Adresser un message** 25
- Organisation de la classe 30
- Interprétations possibles des trames 32
- S'envoyer des messages 33
- Règles protocolaires 34

Séance 2 **Distribuer un message** 35
- Notions sur le routage 39
- Exemple de solution : une carte sur une trame 40
- Panneaux de routage 41

Séance 3 **Transmettre un message long** 42
- Les paquets 50
- Tableau de conversion décimal-binaire 51

Séance 4 **Sécuriser un message** 52
- Sécurité informatique 56

MODULE 2 **LA COMMUNICATION INFORMATIQUE** 57

Séance 1 **Discuter avec l'application Tchat** 60
- Tchat (réseau en étoile ou en anneau) 64

Séance 2 **Échanger des messages numériques** 66
- Application (réseau mixte) 68
- Codage en base binaire 71

Séance 3 **Sécuriser les messages de l'application Tchat** 72
- Notions sur le chiffrement 76
- Chiffrement asymétrique 78

Glossaire 81

Technologie

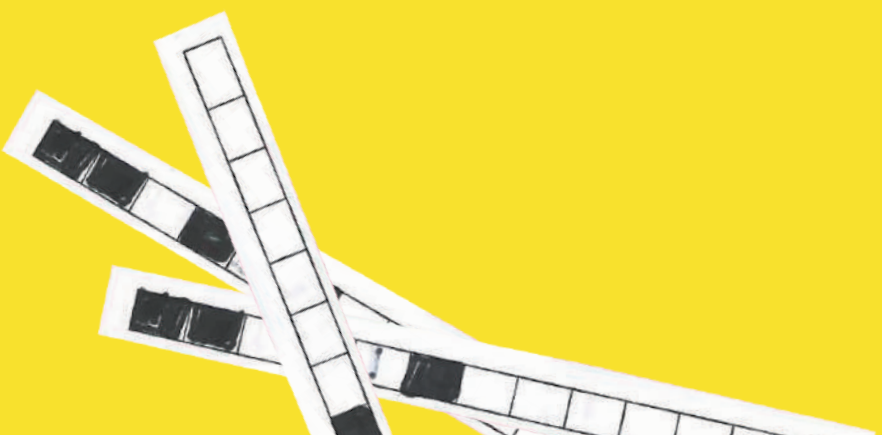
Communication informatique : tout un protocole

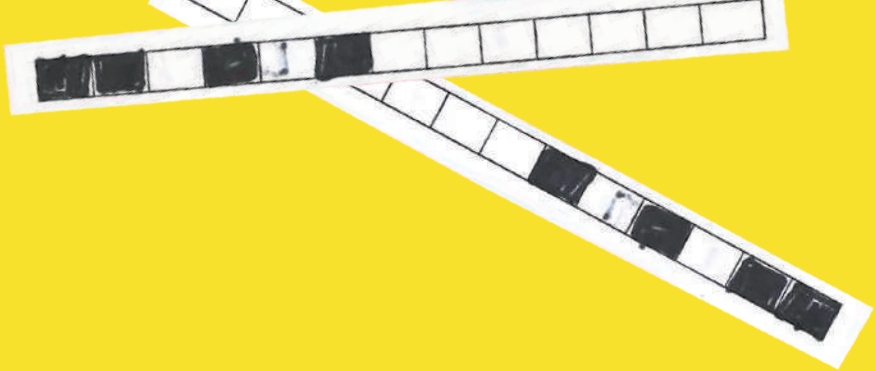
CLASSES DE CYCLE 4

5e 4e 3e

Contenus pédagogiques conçus
par IMT Atlantique

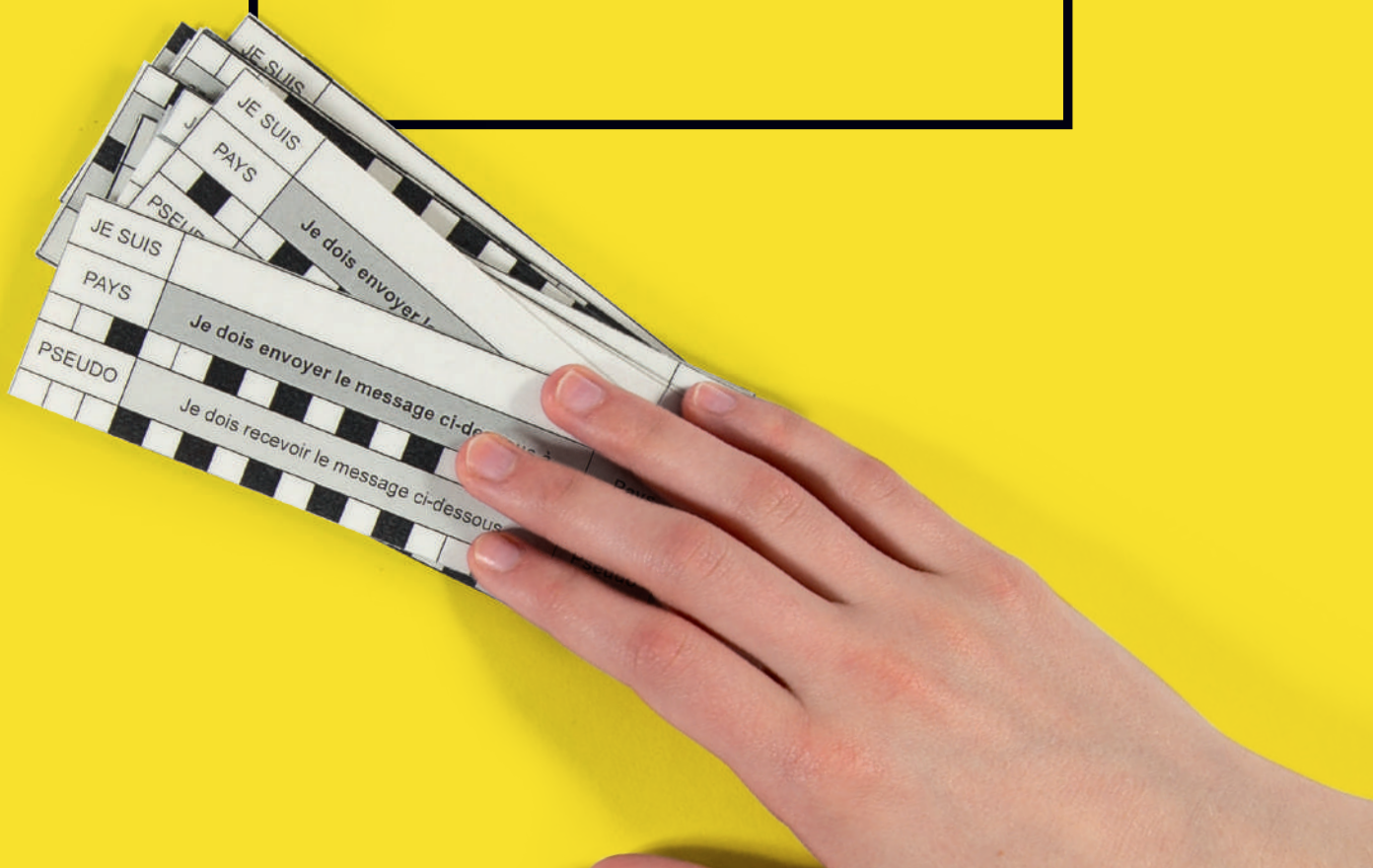
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom





Communication informatique : tout un protocole

Introduction



Communication informatique : tout un protocole

Lorsqu'on parle de communication informatique, on pense aux SMS, aux e-mails et à tout autre échange d'informations qui peut avoir lieu entre des ordinateurs, des smartphones ou encore des tablettes. Ce qu'on ignore bien souvent, c'est que les informations échangées subissent un certain nombre d'opérations tout au long de leur transmission entre émetteur et récepteur. Pour que les données transmises arrivent au bon destinataire et qu'elles soient correctement interprétées, des protocoles bien précis doivent être mis en place pour régir ces opérations.

Objectifs de la thématique

La progression pédagogique a pour objectif de faire découvrir aux élèves quelques concepts fondamentaux utilisés dans la communication entre machines (ordinateurs, tablettes, objets connectés, smartphones ou autre). À travers des activités concrètes et en progressant par « essais-erreurs », les élèves seront amenés à comprendre le fonctionnement d'un réseau : organisation du protocole en couches, architecture et routage du réseau...

2 modules
7 séances

La progression est organisée en deux modules :

Le premier module permet d'aborder de manière simple les notions importantes qui interviennent dans les protocoles en faisant appel à l'analogie avec la communication humaine : les élèves s'échangent matériellement des messages en papier, leur permettant de se familiariser avec des concepts de base tels que l'adressage, le routage, les paquets et la sécurité.

Cette approche est complétée, dans le **second module**, par une expérimentation logicielle, avec des ordinateurs, qui permet aux élèves de faire la transition vers une véritable communication informatique.

L'enseignant pourra s'approprier les contenus de la thématique en paramétrant et en générant lui-même les consignes des activités via des ressources numériques : toutes les informations concernant celles-ci sont disponibles sur www.projetmerite.fr. Conformément à l'usage en informatique, les instructions sont récapitulées dans un fichier README.

Itinéraire pédagogique p. 21

Pédagogie

Les séances privilégient largement le travail en groupe. La classe est organisée en îlots de 4-5 élèves et les activités amènent les îlots à intéragir ensemble. Cette organisation favorise les échanges, la mutualisation et la comparaison des résultats. La pédagogie est rythmée en général par des questions déclenchantes auxquelles l'on propose de répondre par la démarche d'investigation.

Mots-clés

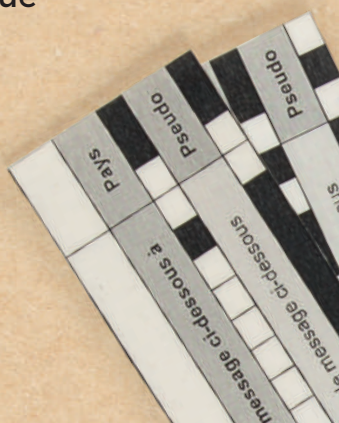
Protocole de communication

Informatique

Adressage

Routage

Sécurité



Synthèse des compétences travaillées

Les langages pour penser et communiquer

Comprendre, s'exprimer en utilisant la langue française à l'oral et à l'écrit

- L'élève parle, communique, argumente à l'oral de façon claire et organisée.
- Il écoute et prend en compte ses interlocuteurs.
- L'élève s'exprime à l'écrit pour raconter, décrire, expliquer ou argumenter de façon claire et organisée.
- Il emploie à l'écrit comme à l'oral un vocabulaire juste et précis.

Comprendre, s'exprimer en utilisant les langages mathématiques, scientifiques et informatiques

- Il produit et utilise des représentations d'objets, d'expériences, de phénomènes naturels tels que schémas, croquis, maquettes, patrons ou figures géométriques. Il lit, interprète, commente, produit des tableaux, des graphiques et des diagrammes organisant des données de natures diverses.
- Il sait que des langages informatiques sont utilisés pour programmer des outils numériques et réaliser des traitements automatiques de données. Il connaît les principes de base de l'algorithmique et de la conception des programmes informatiques. Il les met en œuvre pour créer des applications simples.

Les méthodes et outils pour apprendre

Organisation du travail personnel

- Il comprend le sens des consignes ; il sait qu'un même mot peut avoir des sens différents selon les disciplines.
- Pour acquérir des connaissances et des compétences, il met en œuvre les capacités essentielles que sont l'attention, la mémorisation, la mobilisation de ressources, la concentration, l'aptitude à l'échange et au questionnement, le respect des consignes, la gestion de l'effort.
- Il sait identifier un problème, s'engager dans une démarche de résolution, mobiliser les connaissances nécessaires, analyser et exploiter les erreurs, mettre à l'essai plusieurs solutions, accorder une importance particulière aux corrections.

Coopération et réalisation de projets

- L'élève travaille en équipe, partage des tâches, s'engage dans un dialogue constructif, accepte la contradiction tout en défendant son point de vue, fait preuve de diplomatie, négocie et recherche un consensus.
- Il apprend à gérer un projet, qu'il soit individuel ou collectif. Il en planifie les tâches, en fixe les étapes et évalue l'atteinte des objectifs.
- L'élève sait que la classe, l'école, l'établissement sont des lieux de collaboration, d'entraide et de mutualisation des savoirs. Il aide celui qui ne sait pas comme il apprend des autres. L'utilisation des outils numériques contribue à ces modalités d'organisation, d'échange et de collaboration.

Outils numériques pour échanger et communiquer

- L'élève utilise les espaces collaboratifs et apprend à communiquer notamment par le biais des réseaux sociaux dans le respect de soi et des autres. Il comprend la différence entre sphères publique et privée. Il sait ce qu'est une identité numérique et est attentif aux traces qu'il laisse.

La formation de la personne et du citoyen

La règle et le droit

- L'élève comprend et respecte les règles communes, notamment les règles de civilité, au sein de la classe, de l'école ou de l'établissement, qui autorisent et contraignent à la fois et qui engagent l'ensemble de la communauté éducative. Il participe à la définition de ces règles dans le cadre adéquat.

Réflexion et discernement

- Il fonde et défend ses jugements en s'appuyant sur sa réflexion et sur sa maîtrise de l'argumentation. Il peut discuter… de quelques grands problèmes éthiques liés notamment aux évolutions sociales, scientifiques ou techniques.

Responsabilité, sens de l'engagement et de l'initiative

- L'élève coopère et fait preuve de responsabilité vis-à-vis d'autrui. Il respecte les engagements pris envers lui-même et envers les autres.
- L'élève sait prendre des initiatives, entreprendre et mettre en œuvre des projets.

Les représentations du monde et l'activité humaine

Invention, élaboration, production

- Pour mieux connaître le monde qui l'entoure comme pour se préparer à l'exercice futur de sa citoyenneté démocratique, l'élève pose des questions et cherche des réponses en mobilisant des connaissances sur :

  - les grandes découvertes scientifiques et techniques et les évolutions qu'elles ont engendrées, tant dans les modes de vie que dans les représentations.

Les systèmes naturels et les systèmes techniques

Démarches scientifiques

- L'élève sait mener une démarche d'investigation. Pour cela, il décrit et questionne ses observations ; il prélève, organise et traite l'information utile ; il formule des hypothèses, les teste et les éprouve ; il manipule, explore plusieurs pistes, procède par essais et erreurs ; il modélise pour représenter une situation ; il analyse, argumente, mène différents types de raisonnements (par analogie, déduction logique...) ; il rend compte de sa démarche. Il exploite et communique les résultats de mesures ou de recherches en utilisant les langages scientifiques à bon escient.

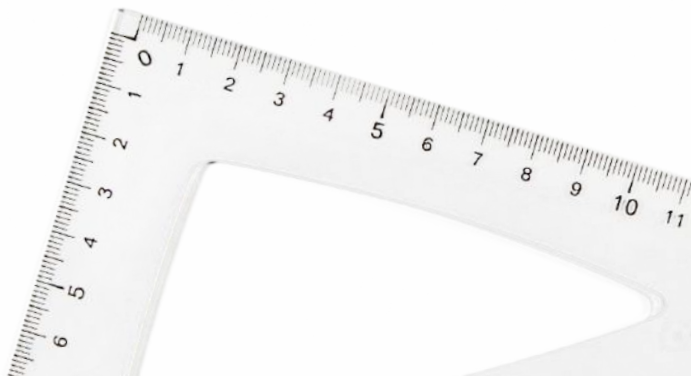
Conception, création, réalisation

- L'élève imagine, conçoit et fabrique des objets et des systèmes techniques. Il met en œuvre observation, imagination, créativité, sens de l'esthétique et de la qualité, talent et habileté manuels, sens pratique, et sollicite les savoirs et compétences scientifiques, technologiques et artistiques pertinents.

Responsabilités individuelles et collectives

- L'élève connaît l'importance d'un comportement responsable vis-à-vis de l'environnement et de la santé et comprend ses responsabilités individuelle et collective. Il prend conscience de l'impact de l'activité humaine sur l'environnement,
- Il observe les règles élémentaires de sécurité liées aux techniques et produits rencontrés dans la vie quotidienne.
- Pour atteindre les objectifs de connaissances et de compétences de ce domaine, l'élève mobilise des connaissances sur :

  - les grandes caractéristiques des objets et systèmes techniques et des principales solutions technologiques.



Comment utiliser ce guide ?

ITINÉRAIRE

Un **itinéraire pédagogique progressif** organisé en **modules** et **séances** est présenté. L'ordre de mise en œuvre des séances peut être adapté par l'enseignant en fonction de ses projets.

Des **pictogrammes** caractérisent les types de séances :

- Découverte / Observation
- Créativité / Réflexion
- Expérimentation
- Réinvestissement
- Synthèse / Communication

Le nombre de **fiches pédagogiques** est précisé pour chaque séance :

- fiches enseignant
- fiches élève

Chaque module, composé de plusieurs séances, est présenté globalement et annonce les **compétences travaillées** ainsi que les **attendus de fin de cycle**.

MATÉRIEL

Une liste exhaustive du matériel contenu dans la mallette est présentée dans le **catalogue du matériel**. Chaque élément porte un numéro de référence.

Chaque page *Séance* contient une liste du matériel utile pour son bon déroulement. Pour faciliter la préparation de la séance et l'identification du matériel, les pictogrammes suivants indiquent :

- nf le matériel non fourni
- 1 le numéro de référence dans le catalogue

SÉANCES

Les pages *Séance* (liseré jaune) contiennent tout ce dont l'enseignant a besoin pour mener la séance :

- les objectifs visés
- une liste du matériel
- un déroulement détaillé de la séance

45' Une durée de la séance est donnée à titre indicatif.

Le déroulement des séances s'organise toujours de la même manière :

- une activité d'immersion
- des points de passages pour développer l'apprentissage visé
- une synthèse des découvertes réalisées par les élèves

Des **post-it roses** récapitulent le vocabulaire spécifique de la séance et renvoient aux définitions du glossaire (situé à la fin du guide).

Des **post-it kraft** renvoient à des conceptions naïves des élèves ou bien resituent une notion dans son contexte.

DES ENCARTS JAUNES

attirent l'attention sur des points d'organisation pédagogique ou de sécurité.

DES ENCARTS GRIS

soulignent les pistes pour aller plus loin.

Les **FICHES** Enseignant viennent compléter les pages *Séance* en apportant des notions supplémentaires ou en donnant des conseils sur l'organisation de la séance.

Des **FICHES** Élève , à imprimer et à distribuer à la classe sont à disposition dans le guide et téléchargeables sur le site du projet MERITE.

Les ressources numériques utiles à la séance sont accessibles depuis le site du projet MERITE (www.projetmerite.fr).

Communication informatique : tout un protocole

Matériel

Matériel

Comment utiliser ce catalogue du matériel ?

Ce catalogue présente l'ensemble du matériel inclus dans la mallette, ainsi que des conseils sur l'utilisation de chaque élément. Le matériel non fourni utile pour mener les séances est listé.

Après chaque séance, au moment de ranger le matériel, vérifiez que le **nombre d'exemplaire**(s) correspond à la mallette d'origine.

Cette référence est rappelée dans le listing matériel des séances. Elle vous permettra d'identifier et de préparer plus rapidement le matériel nécessaire avant une séance.

Matériel manquant

Si des éléments du matériel sont manquants ou ont été endommagés, consultez le site du projet MERITE (www.projetmerite.fr) pour en savoir plus sur les modalités de remplacement.

6 x **Kit de communication**	Réf. 1

Ce kit de communication est constitué de deux grosses pinces à linge en bois qui sont à fixer sur les tables de deux îlots différents. Elles sont reliées par un fin cordon sur lequel est enfilé une petite pince à suspendre métallique. Ainsi, les élèves de deux îlots peuvent s'échanger un message en l'insérant dans la petite pince métallique. Il est conseillé de ne pas tendre le cordon au maximum, pour permettre aux messages de se déplacer sous le simple effet de la gravité.

6 x **Tirelire en bois**	Réf. 2

Cette tirelire, sur laquelle on peut mettre un cadenas, permet de contenir un message sécurisé qui ne peut être lu que par ceux connaissant le code du cadenas. Elle est munie d'une fente (ainsi on peut continuer à y glisser des informations, même sans connaître le code).

Telle que distribuée aux élèves

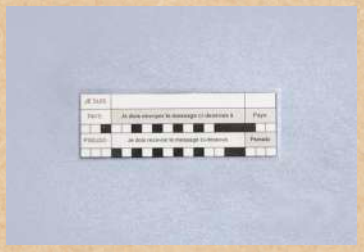
Fixée sur la pince métallique du kit de communication

6 x **Cadenas à code** | Réf. 3

Ces cadenas permettent de sécuriser les tirelires au cours de la séance 4 (module 1). Chaque îlot a son propre code :

- **îlot 1 (000)** → code : 001
- **îlot 2 (001)** → code : 010
- **îlot 3 (010)** → code : 011
- **îlot 4 (011)** → code : 100
- **îlot 5 (100)** → code : 101
- **îlot 6 (101)** → code : 110

24 x **Carte Consignes (13 cases)** | Réf. 4



Ces cartes sont à distribuer en respectant le schéma d'organisation de la classe donné dans la progression pédagogique. Elles doivent réintégrer la mallette après chaque séance. L'enseignant peut choisir de les générer lui-même à partir des ressources numériques.

24 x **Carte Consignes (15 cases)** | Réf. 5

Ces cartes ne sont utilisées que lors de la séance 3 du premier module (transmettre un message long).

Contrairement aux cartes précédentes, le message à envoyer sur la consigne est de 15 cases (plutôt que de 13).

Matériel non fourni

Certains éléments utiles au bon déroulement des séances ne sont pas inclus dans la mallette. Les quantités données sont celles pour une organisation de la classe en 6 îlots.

Désignation du matériel	Séances concernées	Quantité nécessaire par îlot	Quantité pour une classe
Trames papier (13 cases recto et 13 cases verso) : à imprimer à partir du fichier disponible sur la clé USB ou sur www.projetmerite.fr	**Module 1** - Séances 1 à 4	Variable, prévoir un nombre suffisant de trames découpées avant chaque séance	
Boîtes ou contenants quelconques pour comptabiliser les messages	**Module 1 -** Séance 1 à 4	Commun à la classe	3
Feuilles A4 blanches	**Module 1 -** Séance 2	4	24
Ordinateurs connectés à Internet	**Module 2 -** Séances 1 à 3	1 par élève ou par binôme	Idéalement autant que d'élèves

Ressources numériques

L'enseignant pourra trouver, sur la clé USB incluse dans la mallette, des documents imprimables.

Les fichiers permettant de générer lui-même les consignes des activités sont disponibles sur www.projetmerite.fr.

Communication informatique : tout un protocole

Séances

Commentaires sur l’itinéraire pédagogique

La page ci-contre présente une proposition d’itinéraire pédagogique. La progression a été conçue pour une mise en œuvre des modules à la suite l'un de l'autre, dans l’ordre, ou bien de façon imbriquée. L’enseignant est libre d’adapter son itinéraire au gré de ses projets et de ses besoins. Il peut choisir de modifier l’ordre de certaines séances, de ne pas en réaliser certaines voire d’imaginer des séances supplémentaires en s’appropriant le matériel de la mallette.

Légendes

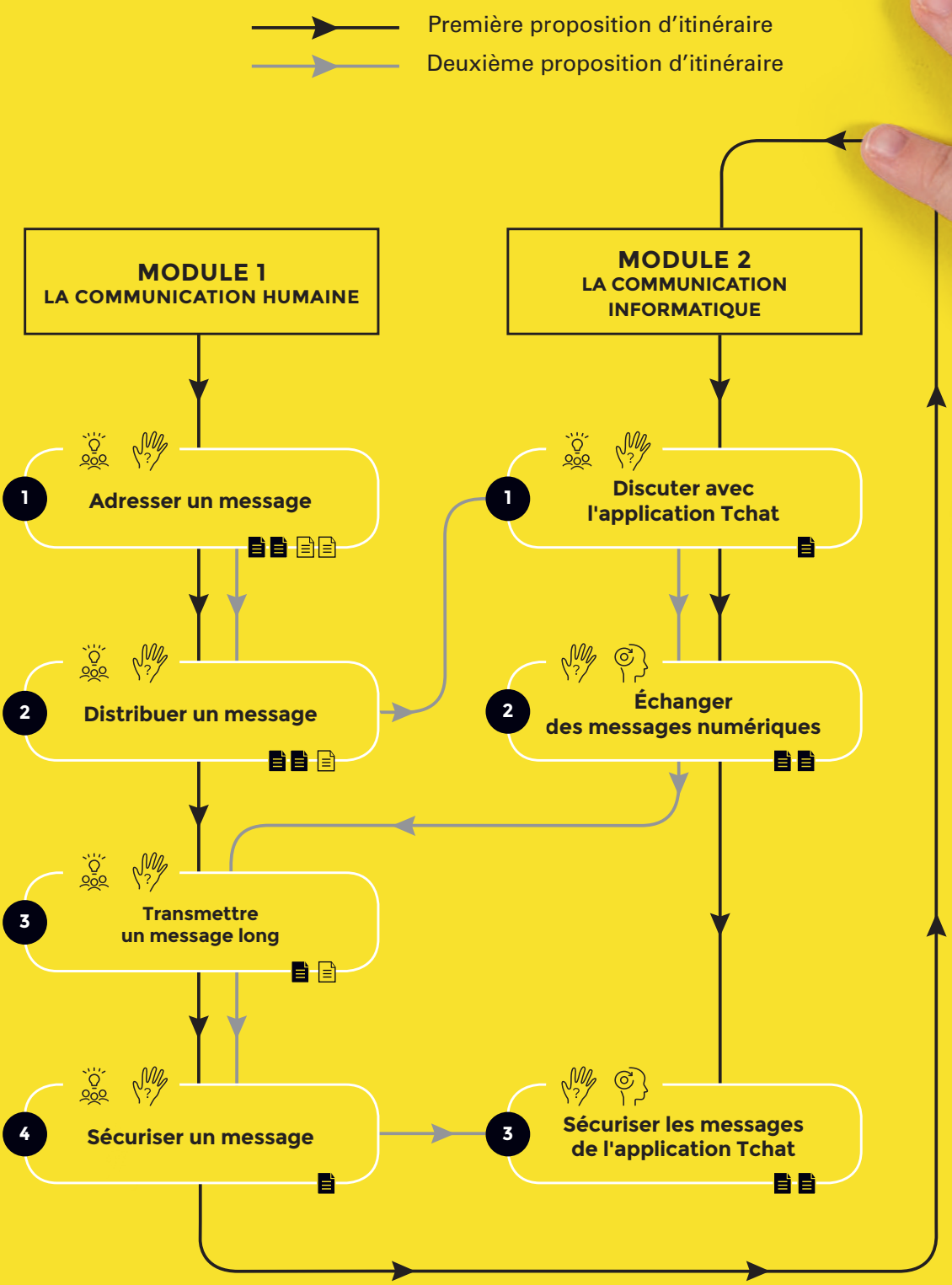
Types de séances

- Découverte / Observation
- Créativité / Réflexion
- Expérimentation
- Réinvestissement
- Synthèse / Communication

Fiches pédagogiques

- Fiches enseignant
- Fiches élève

Itinéraire pédagogique



MODULE 1

LA COMMUNICATION HUMAINE

Présentation générale

Ce premier module propose de mettre les élèves en situation de communiquer en réseau grâce à des messages très simples, sur un simple support papier, pour découvrir les premières couches d'un protocole de communication : adressage, routage, découpage. Ils découvrent que des règles partagées et utilisées par tous sont la condition d'une communication efficace. Au fur et à mesure de leur compréhension de ces règles, ils deviennent capables de se poser de nouvelles questions et abordent les notions de sécurité et de confidentialité. Ils découvrent ainsi les premiers rouages de la communication entre machines et deviennent curieux du fonctionnement du réseau informatique qu'ils utilisent quotidiennement.

Apprentissages visés

Pratiquer des démarches scientifiques et technologiques

Imaginer, synthétiser, formaliser et respecter une procédure, un protocole

Rechercher des solutions techniques à un problème posé, expliciter ses choix et les communiquer en argumentant

Concevoir, créer, réaliser

Associer des solutions techniques à des fonctions

Imaginer des solutions en réponse au besoin

Réaliser, de manière collaborative, le prototype de tout ou partie d'un objet pour valider une solution

S'approprier des outils et des méthodes

Exprimer sa pensée à l'aide d'outils de description adaptés : croquis, schémas, graphes, diagrammes, tableaux (représentations non normées)

Pratiquer des langages

Décrire, en utilisant les outils et langages de descriptions adaptés, la structure et le comportement des objets

Adopter un comportement éthique et responsable

Développer les bonnes pratiques de l'usage des objets communicants

4 séances

Séances du module

SÉANCE 1 — Adresser un message

SÉANCE 2 — Distribuer un message

SÉANCE 3 — Transmettre un message long

SÉANCE 4 — Sécuriser un message

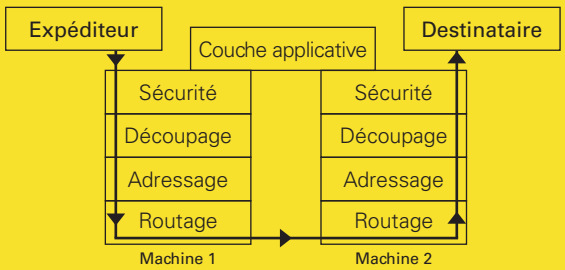
Références

Socle commun de connaissances de compétences et de culture BO N°17 du 23 avril 2015
Programmes scolaires B0 N° 11 du 26 nov 2015 et B0 N°48 du 24 déc 2015

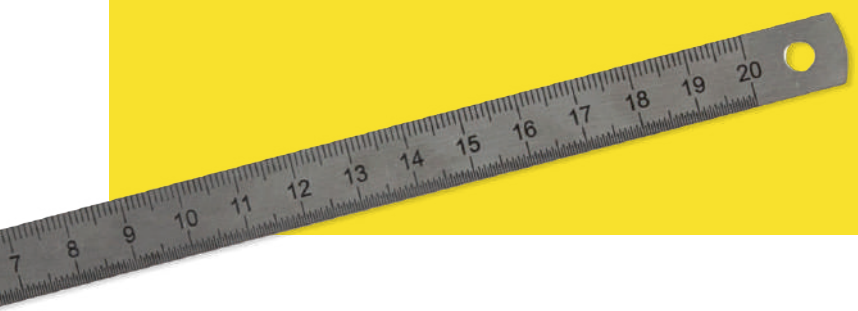
Attendus Fin de Cycle (AFC)	Compétences et Connaissances Associées (CCA)
• **Technologie :** **Design, innovation et créativité** Imaginer des solutions en réponse aux besoins	Identifier un besoin et énoncer un problème technique ; identifier les conditions, contraintes (normes et règlements) et ressources correspondantes, qualifier et quantifier simplement les performances d'un objet technique existant ou à créer Imaginer, synthétiser et formaliser une procédure, un protocole
L'informatique et la programmation Comprendre le fonctionnement d'un réseau informatique	Composants d'un réseau, architecture d'un réseau local, moyens de connexion d'un moyen informatique Notion de protocole, d'organisation de protocoles en couche, d'algorithme de routage Internet

Conseils pour la mise en œuvre

On propose dans ce module de comprendre que toute communication entre machines engage un protocole, dit en couches, en abordant quatre d'entre elles (routage, adressage, découpage et sécurité). Le schéma suivant peut être reproduit au tableau pour expliquer ce principe aux élèves. Une des normes de communication en réseau les plus complètes, le modèle OSI (*Open Systems Interconnection*), comporte 7 couches en tout. Pour plus d'informations, consulter l'entrée *Couche (protocolaire)* du glossaire.



NB - Découpage : en informatique, on rencontre aussi le terme Transport



SÉANCE 1

Adresser un message

Objectifs

Expérimenter la circulation non organisée (sans règles communes, sans protocole) de messages sur papier, et constater que celle-ci est compliquée.
Proposer et formaliser collectivement un protocole qui fixe les règles de lecture et de circulation des messages, puis tester ces règles.
Rédiger un protocole et le conserver pour les séances suivantes.

Matériel

Pour l'ensemble de la classe :

- **6 kits de communication** [1]
  constitués d'une paire de pinces à linge reliées par un cordon sur lequel est enfilée une petite pince métallique
- **cartes *Consignes* (13 cases)** [4]
  1 par élève ou binôme (peuvent aussi être générées grâce aux ressources disponibles sur www.projetmerite.fr)
- **trames papier** nf
  13 cases recto-verso, plusieurs par élève ou binôme, à imprimer depuis la clé USB ou www.projetmerite.fr
- **3 boîtes** nf
  pour comptabiliser les succès, échecs et pertes en fin de séance
- **FICHE** S'envoyer des messages
  1 photocopie par élève
- **FICHE** Règles protocolaires
  1 photocopie par élève

nf Matériel non fourni
[0] Référence dans le catalogue du matériel

Déroulement pédagogique

50'

En amont de la séance, l'enseignant organise la salle de classe en suivant la **FICHE** Organisation de la classe. Si l'enseignant décide de générer lui-même les consignes de la séance (facultatif), il pourra se référer au site web du projet MERITE (www.projetmerite.fr).

Immersion

L'enseignant pose la question suivante à la classe :

Comment fait-on pour communiquer entre humains ?

Réponses possibles : l'écriture, la parole, la gestuelle, les signes, le morse, le braille, les sms…

Les réponses sont notées au tableau. Pour chaque réponse, l'enseignant demande aux élèves d'identifier les deux aspects fondamentaux de la communication :

- le codage de l'information,
- le médium (= moyen) utilisé pour son transport.

Exemples :

- l'écriture : codage = l'alphabet ; médium = support papier,
- la parole : codage = ondes sonores ; médium = air.

L'enseignant annonce que, pour la suite des activités réalisées, le médium imposé consiste en une trame recto-verso comportant 13 cases (sur chaque face) qui peuvent être noircies ou laissées blanches.

GLOSSAIRE
Médium

La classe est alors interrogée :

Quel est le codage de l'information correspondant à ce médium (la trame de 2x13 cases) ?

Quel est le nombre total de messages que l'on peut écrire avec un tel médium ?

Note pour l'enseignant

Le codage est le binaire, composé de deux chiffres, zéro (0) et un (1), correspondant dans notre cas, à blanc et noir respectivement. Comme au total, la trame comporte 26 cases (recto-verso), le nombre total de messages est de deux à la puissance 26 (2^{26}). Cela veut dire qu'avec une trame de 13 cases recto-verso, il y a 64 millions de messages possibles.

EXPLICATION DES CONSIGNES

L'enseignant annonce aux élèves qu'ils vont devoir relever un défi :

- faire circuler des messages papier en respectant un protocole de communication, c'est-à-dire des règles pour communiquer,
- utiliser un codage binaire pour rédiger un message,
- respecter un délai maximal (l'enseignant fixe une durée entre 5 et 7 minutes).

Les cartes *Consignes* ainsi que les trames qui serviront à écrire les messages sont distribuées aux élèves en respectant bien la distribution décrite sur le schéma de la **FICHE** Organisation de la classe.

Le but de l'activité est annoncé à la classe : chaque élève doit envoyer son message au bon destinataire, en faisant le nécessaire pour qu'il lui parvienne.

Trois boîtes (Succès, Échec et Perte) sont mises à disposition dans la salle et permettront, en fin d'activité, de comptabiliser combien de messages sont bien arrivés à destination.

Il est important, à ce stade, que l'enseignant explique bien aux élèves les différents éléments (code pays, pseudo, message à envoyer, message à recevoir) et les consignes de l'activité. Tous ces éléments sont détaillés dans la **FICHE** S'envoyer des messages qui est distribuée aux élèves.

Aucune consigne supplémentaire n'est donnée à ce stade.

Points de passage

1RE ACTIVITÉ : SANS PROTOCOLE

Les élèves ont quelques minutes pour compléter leurs trames. Chaque élève est un expéditeur (= émetteur), et doit donc recopier son message et l'adresse du destinataire (= récepteur) sur le support-papier (la trame).

Une fois que tous les élèves sont prêts, l'activité est lancée. Les élèves ont alors 5 (à 7) minutes pour faire circuler les messages, en faisant passer les trames pliées en deux à un îlot voisin avec lequel ils peuvent communiquer, en utilisant les cordes de liaison et les pinces à linge.

À tout moment, un élève peut décider d'ouvrir une trame et de lire le message. Pour déterminer si le message reçu est le bon, il doit comparer le contenu du message qu'il a reçu au message à recevoir donné dans la consigne.

Au bout du temps imparti, on compte les messages qui :

- sont arrivés au bon destinataire = **succès**,
- ont été ouverts mais pas par le bon destinataire = **échec**,
- ne sont pas arrivés = **perte**.

Bilan : le taux d'échec et de perte est vraisemblablement important.

L'enseignant explique que ce faible taux de succès est essentiellement dû au fait que les élèves ne se sont pas mis d'accord sur les règles de protocole :

- règles pour écrire l'adresse du destinataire (pseudo et pays, soit six cases sur les treize possibles),
- règles pour lire le message, puisque la trame intérieure peut être lue dans un sens ou dans l'autre,
- règles pour faire circuler le message, car un message peut faire des allers et retours sans jamais progresser.

FIXATION DE RÈGLES PROTOCOLAIRES

L'enseignant demande aux élèves d'identifier les problèmes rencontrés et de proposer des solutions/pistes d'amélioration. Il vise à mettre en évidence les 8 interprétations possibles d'une trame (voir **FICHE** Interprétations possibles des trames).

Pour ce faire, la **FICHE** Règles protocolaires est distribuée.

Les élèves devront fixer des règles protocolaires pour améliorer la communication :

- règles d'adressage,
- règles d'interprétation du contenu,
- règles de routage pour la circulation.

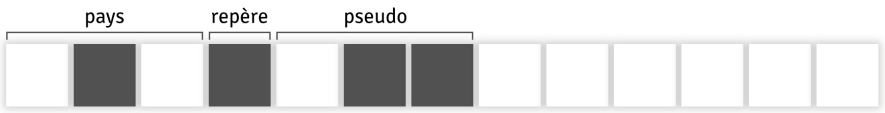
Il est possible de relier ces règles à celles utilisées en informatique :

- règles d'adressage : adresses Web, avec les URL,
- règles d'interprétation du contenu : le boutisme,
- règles de routage : le routage sur Internet, observable avec l'outil *traceroute*.

EXEMPLES DE RÈGLES : ÉCRITURE DE L'ADRESSE

Exemple 1 : *3 cases noires (repère pour le sens de la lecture), suivies du pays, et ensuite du pseudo*

Exemple 2 : *le repère (case noire) est la 4e case, les pays et pseudo sont placés de part et d'autre*



Exemple 3 : *idem pour le repère et le pays, seul l'emplacement du pseudo est modifié*

D'autres exemples sont possibles. L'essentiel est que le choix soit fait par les élèves et discuté avec eux.

GLOSSAIRE

Adressage
Boutisme
Routage
Traceroute
Web

EXEMPLES DE RÈGLES : LECTURE DU MESSAGE

Une convention est choisie pour la rotation de la trame. En l'absence de cette convention, une inversion du contenu peut parfaitement se produire, faussant ainsi l'interprétation du message.

Exemple 1 : *la trame est tournée relativement à son petit côté – rotation selon le grand côté de la trame*

Exemple 2 : *la trame est tournée relativement à son grand côté – rotation selon le petit côté de la trame*

EXEMPLES DE RÈGLES : CIRCULATION DES MESSAGES

Solution 1 : *les liaisons de communication sont unidirectionnelles, les messages circulent toujours dans le même sens, horaire ou antihoraire*

Solution 2 : *les liaisons sont bidirectionnelles, le message circule soit dans un sens, soit dans l'autre, mais pas les deux : lorsqu'un message est reçu par un point d'accès (ou port d'entrée), et s'il doit être transmis, il le sera par l'autre point d'accès (ou port de sortie)*

Bilan : la classe fait le choix d'une règle pour chacun des 3 problèmes rencontrés (adressage, interprétation du contenu, routage). Ce choix constituera le premier protocole élaboré par la classe, qui sera utilisé pour toute la suite du module 1. Il est conseillé de l'écrire au tableau.

2E ACTIVITÉ : AVEC PROTOCOLE

Les élèves complètent leurs trames.

Ils font circuler les messages pendant le temps imparti (5 ou 7 minutes selon le choix de l'enseignant).

Le comptage des succès, échecs, et pertes est fait au bout du temps imparti.

Bilan : Le taux de succès est plus important.

L'application du protocole permet un déchiffrement des messages plus aisé, et une meilleure circulation des messages, ce qui conduit tout logiquement à l'augmentation du nombre des messages qui arrivent à temps à leur destinataire.

Découvertes réalisées

Un réseau de communication ne peut fonctionner efficacement qu'avec des règles : l'ensemble de ces règles forme un protocole de communication. Le protocole doit être suivi par tous, sans exception. C'est pourquoi, très souvent, les protocoles deviennent des normes internationales.

Les élèves retiennent les termes vus pendant l'activité :

- adressage,
- routage,
- interprétation.

La classe prend conscience que chaque élève a rempli trois rôles, celui :

- d'émetteur (expéditeur),
- de récepteur (destinataire),
- de routeur (de messages).

Les élèves ont appris que, pour définir le sens de lecture, il faut définir un marquage. Celui-ci doit être bien pensé, afin d'éviter que la lecture en sens inverse puisse faire penser à une adresse (erronée). Par exemple, un marquage de la case du milieu (la septième), avec le pays à gauche et le pseudo à droite, est incorrect : la lecture d'une adresse est possible dans les deux sens. ■

GLOSSAIRE

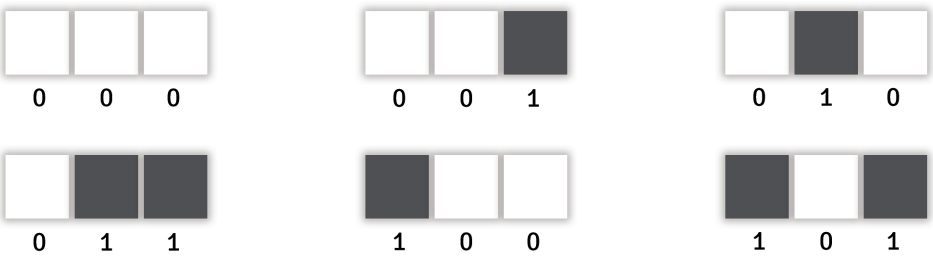
Émetteur

Récepteur

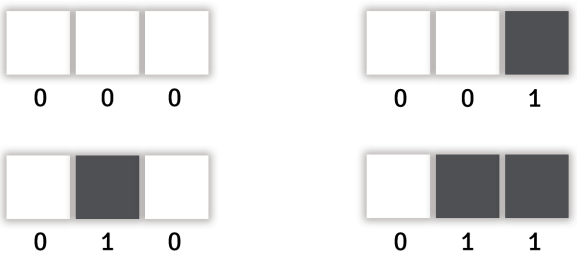
Organisation de la classe

La classe est idéalement organisée en 6 îlots de 4 élèves (voir schéma ci-contre). Pour les classes plus nombreuses, le plus simple est de créer des binômes qui travailleront sur la même trame et joueront le rôle d'un seul expéditeur. Il est également possible de créer des îlots supplémentaires, mais dans ce cas, les cartes *Consignes* disponibles dans la mallette ne sont plus pertinentes et l'enseignant devra générer lui-même les cartes *Consignes* des élèves (voir **FICHE** Paramétrisation des consignes).

Chaque îlot symbolise un pays, numéroté à partir de 0 en binaire :



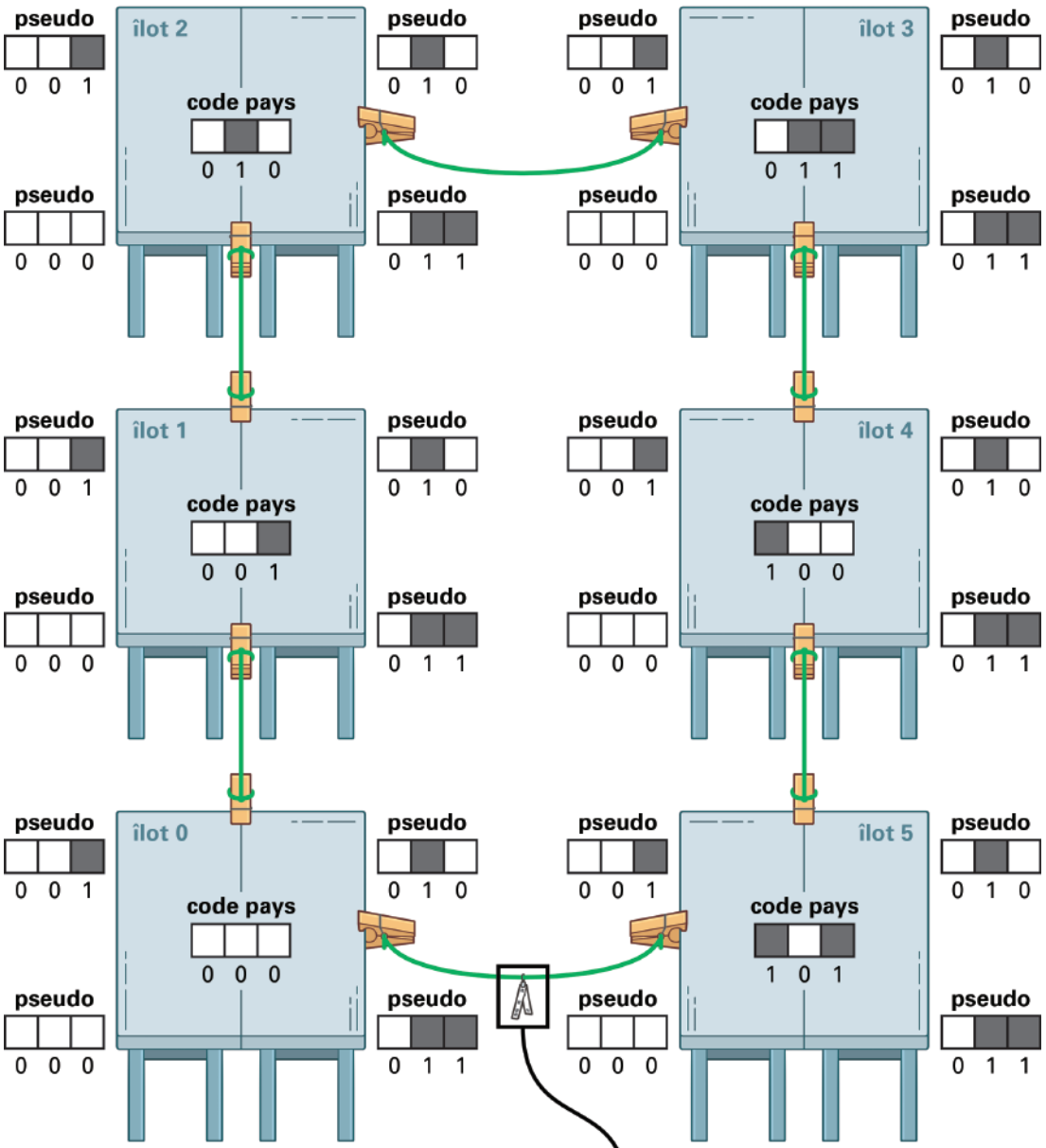
Chaque élève (ou binôme, le cas échéant) se voit adresser un pseudo, numéroté à partir de 0 en binaire :

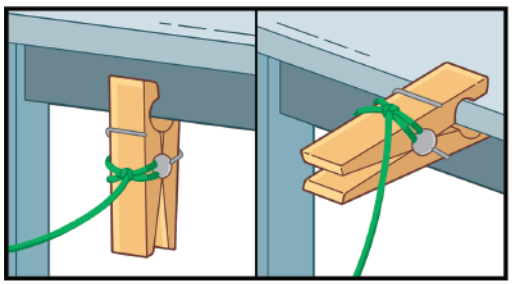


INFORMATIONS NON COMMUNIQUÉES AUX ÉLÈVES

La liste des pseudos est identique dans tous les îlots.

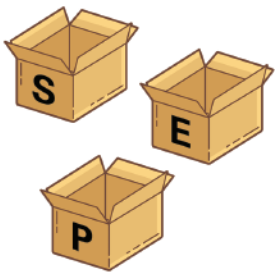
Le destinataire du message d'un élève est toujours situé dans un îlot situé à 3 sauts (par exemple : les messages de l'îlot 0 (0, 0, 0) ont pour destinataires les élèves de l'îlot 3 (0, 1, 1) et doivent donc d'abord transiter par deux autres îlots). Les cartes *Consignes* doivent donc être distribuées en suivant l'organisation présentée dans le schéma ci-contre.





2 façons d'accrocher les pinces à linge aux tables

Circulation des messages sur les cordons à l'aide de la pince métallique



3 boîtes pour collecter les messages en fin d'activité

Interprétations possibles des trames

Comment interpréter une trame ?

Il y a au total 8 possibilités, résultant de trois choix binaires à réaliser consécutivement.

1. Déterminer le recto et le verso. Il est imposé que la trame soit pliée en deux lorsqu'elle est envoyée. Le pliage permet de déterminer le recto (les cases à l'extérieur) et le verso (les cases à l'intérieur).

2. Déterminer le sens de lecture de la face au recto : soit de la gauche vers la droite, ou inversement.

3. Déterminer le sens de lecture de la face au verso : soit en partant de la même case, ou en partant de la case opposée, ou autrement dit, soit après rotation de la trame relativement au grand côté (longueur), soit après rotation de la trame relativement au petit côté (largeur).

Conclusion : 2∗2∗2, soit 8 interprétations différentes d'une trame sont possibles.
Les règles protocolaires doivent donc viser à en déterminer une, et une seule.

UN PROTOCOLE POUR ENVOYER UN MESSAGE – SOLUTION EXEMPLAIRE

Rappel : il est imposé que la trame soit pliée en deux lors de son envoi.

Les règles suivantes sont choisies pour leur simplicité en respectant quelques grands principes :

- les marqueurs sont en bout de trame, puisque c'est par les bouts que commencent la lecture,
- les informations importantes précèdent celles de moindre importance,
- aucune information connue n'est supposée concernant le voisinage d'un îlot.

Règles d'interprétation de la trame

- **recto :** face externe de la trame pliée, **verso :** face interne
- **sens de lecture du recto :** marquage du début par une case noire, celle à l'autre bout restant blanche
- **sens de lecture du verso** : rotation suivant le grand côté, donc début de lecture par l'autre face de la même case que le recto

La première règle est naturelle (pensez aux enveloppes), la seconde applique le premier principe, la troisième est simplement pratique.

Règles d'adressage

- **recto :** case noire + pays (3 cases) + pseudo (3 cases)

La règle applique le second principe.

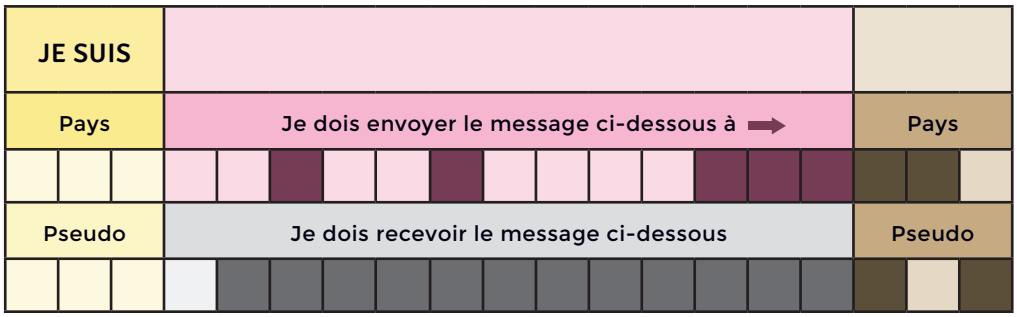
Règles de routage

- circulation bi-directionnelle avec sortie d'un message à l'opposé de l'entrée

La règle respecte le troisième principe. À l'inverse, la circulation horaire ou anti-horaire suppose le partage d'une orientation entre îlots.

S'envoyer des messages

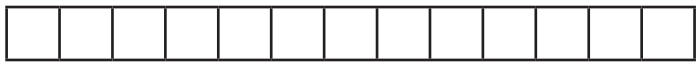
PRÉSENTATION DE LA CARTE CONSIGNES

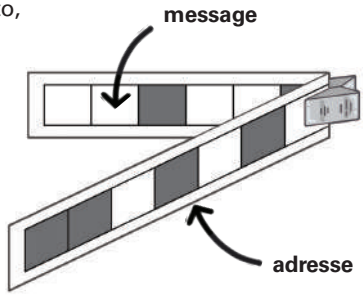


Code couleur : Identité de l'élève expéditeur du message | Message envoyé par l'expéditeur | Message reçu par l'expéditeur | Identité de l'élève destinataire du message

Sur ta trame, tu dois noircir les cases pour :

- renseigner l'adresse du destinataire de ton message sur le recto,
- reproduire le message à envoyer au verso.





La trame doit ensuite être pliée, **l'adresse à l'extérieur** et **le contenu du message à l'intérieur**.
La trame est ensuite insérée dans la pince métallique.

BUT DE L'ACTIVITÉ

Les messages doivent parvenir à leurs destinataires. Tu dois donc diffuser ton message en l'envoyant à un îlot voisin pour faire en sorte que ton destinataire le reçoive.

CONSIGNES DE L'ACTIVITÉ

Le temps global pour la circulation des messages est limité (quelques minutes, durée fixée par l'enseignant).

Les messages ne peuvent transiter que par le réseau des cordes, en anneau (le message envoyé doit absolument passer par un îlot voisin).

Lorsque tu reçois un message, observe l'adresse (formée du pays et du pseudo) et compare-la à la tienne :

- si l'adresse ne correspond pas, le message ne t'est pas destiné, tu ne dois donc pas l'ouvrir et tu dois poursuivre sa distribution, au sein de ton îlot (si le pays correspond), sinon à un îlot voisin,
- si tu penses que l'adresse correspond à la tienne, ouvre la trame et compare le message avec celui que tu es censé recevoir :
  - si le message sur la trame est le même que celui que tu devais recevoir, conserve le message devant toi,
  - si le message ne correspond pas, le message est donc perdu et tu le mets de côté.

À l'issue du temps imparti, les trames sont placées dans des boîtes :

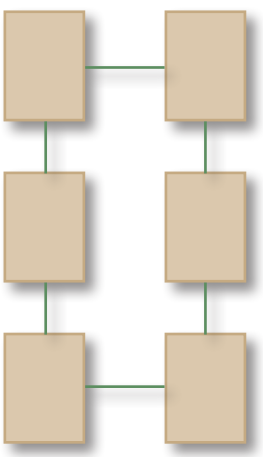
- les trames ouvertes et lues par le bon destinataire avec le bon message sont placées dans la boîte **Succès**,
- les autres trames ouvertes sont placées dans la boîte **Échec**,
- les trames non ouvertes (donc les messages non distribués) sont placées dans la boîte **Perte**.

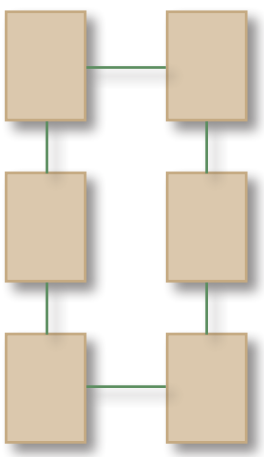
Règles protocolaires

Quelles règles d'écriture de l'adresse pourrait-on proposer ?

Quelles règles d'ouverture du message pourrait-on proposer ?

Quelles règles de circulation des messages pourrait-on proposer ?





SÉANCE 2

Distribuer un message

Objectifs

Proposer (collectivement) un protocole de routage.
Tester sa mise en œuvre.

Matériel

Pour l'ensemble de la classe :

- **6 kits de communication** [1]
  constitués d'une paire de pinces à linge reliées par un cordon sur lequel est enfilée une petite pince métallique
- **cartes *Consignes* (13 cases)** [4]
  1 par élève ou binôme (peuvent aussi être générées grâce aux ressources disponibles sur www.projetmerite.fr)
- **trames papier** [nf]
  13 cases recto-verso, plusieurs par élève ou binôme, à imprimer depuis la clé USB ou www.projetmerite.fr
- **feuilles A4 blanches** [nf]
  1 par îlot
- **3 boîtes** [nf]
  pour comptabiliser les succès, échecs et pertes en fin de séance
- **FICHE** S'envoyer des messages
  fiche de la séance précédente
- **FICHE** Panneaux de routage
  1 photocopie par élève

[nf] Matériel non fourni
[0] Référence dans le catalogue du matériel

Déroulement pédagogique

50'

En amont de la séance, l'enseignant organise la salle de classe comme à la séance précédente, en suivant la **FICHE** Organisation de la classe (séance 1). Il imprime les panneaux de routage (**FICHE** Panneaux de routage) que les élèves découperont. L'impression d'une fiche permet de fournir des panneaux de routage à 1 îlot (2 panneaux par îlot), la fiche est donc à imprimer en 6 exemplaires si la classe est organisée en 6 îlots.

Ne pas découper le long des pointillés qui représentent la ligne de pliage du panneau une fois rempli (les panneaux pliés pourront ainsi être posés sur les tables des élèves).

Immersion

En séance 1, les élèves ont envoyé et reçu des messages avec plus ou moins de succès, en raison notamment d'une circulation non optimale. L'enseignant annonce qu'afin d'améliorer cette circulation des messages, la séance va aborder une nouvelle notion : le **routage**.

Le routage est un moyen qui permet de cibler plus rapidement les destinataires, à condition de bien connaître la topographie du réseau. Pour cela, il faudrait déterminer la carte du réseau (l'emplacement de chaque îlot) et le meilleur chemin (la distance la plus courte) pour parcourir les îlots. Pour en apprendre plus sur le sujet, l'enseignant peut consulter la **FICHE** Notions sur le routage.

GLOSSAIRE
Routage

La notion de routage est introduite aux élèves en prenant l'exemple de la carte du métro parisien ou encore d'une carte routière.

Il annonce aux élèves qu'ils vont devoir relever deux défis :

- déterminer la carte du réseau des îlots,
- compléter les panneaux de routage (**FICHE** Panneaux de routage).

L'enseignant distribue une feuille A4 blanche à chaque élève, ainsi que deux panneaux de routage pour chaque îlot.

Les consignes sont expliquées en détail :

- **étape 1 :** dessiner la carte des îlots (la position de chaque îlot par rapport aux autres) sur la feuille blanche,
- **étape 2 :** compléter les panneaux de routage en indiquant le nombre de sauts qui séparent leur îlot des autres (à chaque pays et associé un nombre de sauts pour le rejoindre), puis les placer devant chacune des deux sorties (les cordes) pour l'envoi des messages vers les différents pays (îlots),
- **étape 3 :** échanger les messages (même activité qu'en séance 1, mais en utilisant les panneaux de routage).

Les contraintes suivantes sont imposées à la classe :

- utiliser comme messages les feuilles blanches ou les trames,
- échanger les messages en utilisant les cordes comme précédemment,
- ne pas communiquer oralement des informations à des voisins.

Points de passage

ÉTAPE 1 : ÉTABLISSEMENT DE LA CARTE DU RÉSEAU

Les consignes de l'activité restent les mêmes que pour la séance 1.

CARTE DU RÉSEAU

Ce terme renvoie à des exemples de la vie de tous les jours que les élèves connaissent bien : carte routière, plan d'un réseau de transport en commun… L'enseignant ne doit pas hésiter à y faire référence pour établir un lien entre l'activité et le quotidien des élèves.

L'enseignant peut poser des questions pour faire émerger la solution :

Pourquoi la circulation des messages de l'activité de la séance 1 était lente ?

Le fait de ne pas utiliser le chemin le plus court.

De quoi avons-nous besoin pour améliorer cette circulation ?

Connaitre l'emplacement de chaque îlot.

Comment obtenir cette amélioration ?

Définir une carte du réseau.

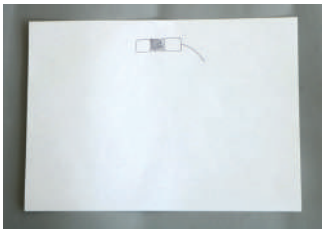
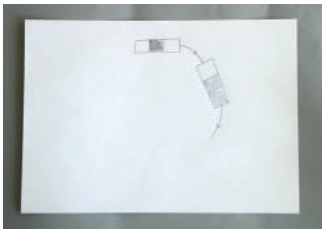
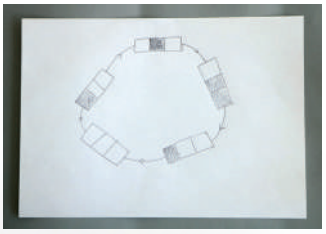
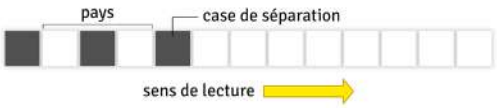
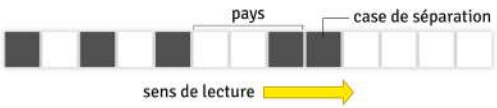
Comment la définir sans communiquer oralement ?

En définissant progressivement la carte, en diffusant les informations utiles à ses voisins.

Pour ce premier défi, les élèves vont devoir définir collectivement la carte du réseau de la salle.

Pour cela, ils vont faire circuler une feuille ou trame (voir tableau suivant), pour que chaque îlot note/dessine sur cette feuille le nom de son pays (trois cases). Ainsi, lorsque la feuille aura fait le tour complet, toutes les informations seront ainsi connues par toutes les équipes (îlots). Pour définir cette carte, deux scénarii sont possibles en fonction de la réactivité des élèves et/ou du temps disponible.

Le tableau suivant détaille ces deux démarches :

Scénario simple	Scénario complexe
Chaque élève dispose d'une feuille blanche. Le but est qu'à la fin du défi, il obtienne la carte du réseau dessiné sur cette feuille (et pouvoir ainsi compléter les panneaux). **Pour ce faire :** **1** – L'élève d'un îlot indique sur la feuille son pays, puis la liaison le reliant à l'îlot à qui il va donner sa carte.  **2** – Un des élèves de l'îlot suivant complète la carte avec son pays, puis indique la liaison suivante (chaque élève complète une carte que l'îlot a reçue afin que tout le monde soit actif).  Ainsi de suite jusqu'à ce que la carte revienne au premier îlot qui l'a émise.  **Exemple :** *un réseau de 5 îlots (on voit bien ici que le sens de lecture n'est pas évident, à préciser donc avec les élèves).*	Les élèves disposent d'une trame de 13 cases, comme pour le premier défi. Le but est qu'à la fin du défi, ils obtiennent la carte du réseau grâce aux informations contenues sur cette trame (permettant ainsi à l'îlot de compléter ses panneaux). **Pour ce faire :** **1** – L'élève indique sur la trame son pays, puis transmet la trame à un îlot voisin. Le sens est défini auparavant.  Ce scénario nécessite la mise en place de règles pour compléter la trame. En effet, la présence d'un îlot « blanc / blanc / blanc » implique que chaque îlot fasse suivre d'une case noire son pays. **2** - Le suivant complète la trame avec son pays (chaque élève complète une trame que l'îlot a reçue afin que tout le monde soit actif).  **3** – Ainsi de suite jusqu'à ce que la trame revienne au premier îlot qui l'a émise. Pensez à fixer une règle pour retourner la trame car une difficulté apparaît lorsqu'on ajoute le 3e pays. En effet, la case de séparation (appelée césure) ne doit pas remplacer le repère blanc qui sert à l'orientation (voir **FICHE** Exemple de solution : une carte sur une trame).

ÉTAPE 2 : REMPLISSAGE DES PANNEAUX DE ROUTAGE

Une fois la carte du réseau établie, les élèves de chaque îlot remplissent les panneaux en indiquant les différentes distances (évaluées en nombre de sauts) qui séparent leur îlot des autres îlots. Ils font cette opération pour les deux sens de circulation. Ce travail va aider les élèves à choisir le sens de circulation le mieux adapté, donc celui qui permet au message d'arriver au destinataire en parcourant le plus court chemin. Ici, la solution choisie est nécessairement bidirectionnelle, mais c'est l'îlot qui choisit le sens de circulation.

ÉTAPE 3 : CIRCULATION DES MESSAGES

Les élèves font circuler leurs messages (comme en séance 1), en utilisant cette fois-ci les panneaux de routage.

Bilan : les panneaux de routage améliorent le temps de circulation des messages en optimisant les trajets.

Découvertes réalisées

Les élèves ont établi une carte du réseau (de la classe).

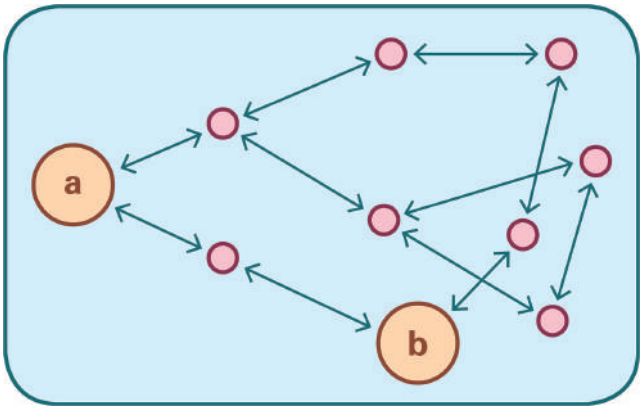
Grâce à cette carte, ils ont pu compléter leurs panneaux de routage, les ont utilisés, et ont constaté leur efficacité dans les envois des messages.

Dans beaucoup de réseaux de communication, il existe des panneaux de routage tout au long des routes. On peut penser aux panneaux de circulation sur les routes et aux tables de routage des routeurs sur Internet. Ces panneaux sont utiles dès lors que le réseau évolue dans le temps : des routes se font et se défont, des machines se connectent et se déconnectent. De manière générale, le problème du routage revient à chercher le plus court chemin dans un graphe : le graphe représente le réseau, chaque nœud représentant un îlot, et chaque arc un lien de communication entre les îlots. ■

Notions sur le routage

LE ROUTAGE

Le routage, dans lequel on entend le terme « route », est l'action de choisir/suivre, sur une carte routière par exemple (réseau routier), telle ou telle route pour aller d'un point à un autre. En réseau informatique cela se traduit par le choix de certains chemins pour la transmission de données d'un expéditeur à un ou plusieurs destinataires. Le terme routage est souvent lié à celui de réseau, et on les retrouve dans plusieurs domaines : réseaux de transports, réseaux électroniques (internet), réseaux téléphoniques.



*Comme on peut le voir sur cette figure, plusieurs chemins sont possibles pour relayer un message entre **a** et **b**, en passant par différents routeurs (les petits ronds rouges, représentés par les îlots dans l'activité). En fonction de la disponibilité de ces routeurs, le chemin est constamment adapté (de la même façon qu'un GPS adapterait le chemin le plus court en fonction des embouteillages ou des travaux).*

Quelques réseaux informatiques :

- **Réseau personnel (Personal Area Network, PAN) :** réseau s'étendant sur un petit espace (habitation),
- **Réseau local (Local Area Network, LAN) :** réseau s'étendant sur un espace local (entreprise, école),
- **Réseau étendu (Wide Area Network, WAN) :** réseau s'étendant sur une grande zone géographique (le monde, comme pour le réseau Internet).

LES TABLES DE ROUTAGE

Comme vu plus haut, le routage permet de donner des indications sur le chemin à suivre.
Ces indications sont enregistrées dans des tables de routage et contiennent des informations très importantes et utiles : les points de passage. En informatique, ces derniers sont appelés routeurs.
Lorsqu'une trame arrive à un routeur, celui-ci consulte sa table de routage pour déterminer le routeur suivant à partir de la destination de la trame.

Précisions :

Les routeurs s'organisent souvent hiérarchiquement. Ainsi, un routeur peut à la fois appartenir à un réseau et être une passerelle pour un sous-réseau. Lorsqu'il reçoit un message, il détermine à partir de la destination s'il le transmet à un routeur voisin du réseau ou à un routeur du sous-réseau : il joue alors le rôle de passerelle. Cette architecture hiérarchique permet de simplifier les décisions de routage : un routeur doit connaître les routes dans son réseau et dans un seul sous-réseau au lieu de tous les sous-réseaux.

GLOSSAIRE

Table de routage

Exemple de solution : une carte sur une trame

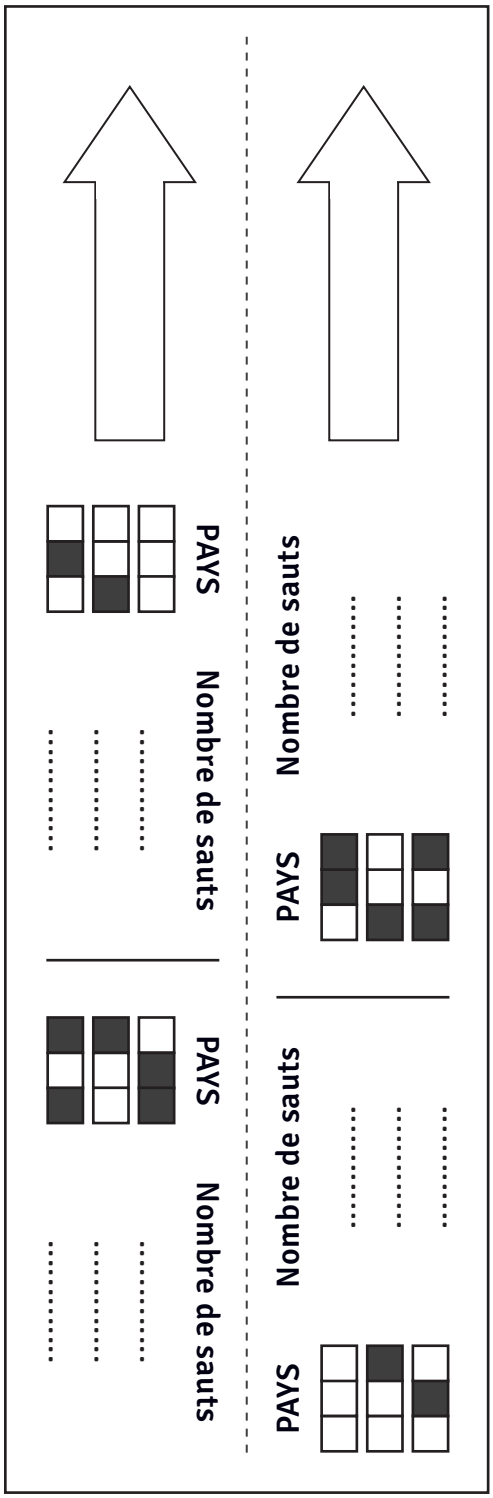
Dans le cadre de l'élaboration de la carte du réseau, les solutions pour fixer une règle pour retourner la trame ne sont pas évidentes. Chaque îlot intermédiaire doit modifier l'état de la trame. Les îlots initial et final doivent pouvoir déterminer le retour à l'envoyeur. Voici une solution, qui repose sur le principe suivant : l'écriture du pays se fait toujours après la dernière case noire utilisée comme séparateur.

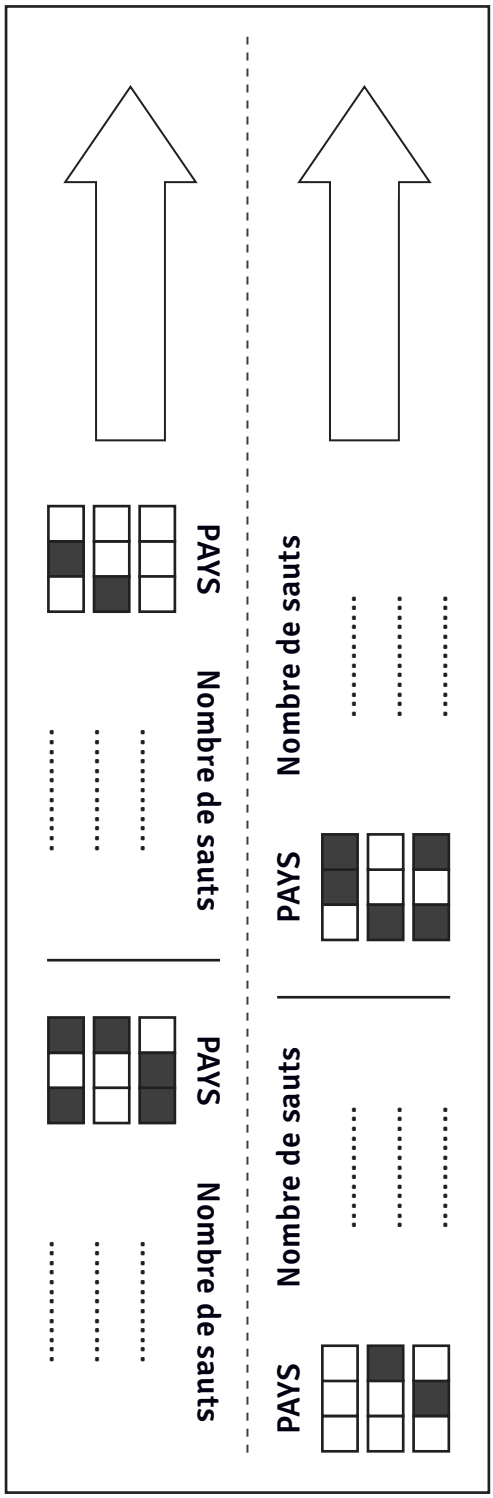
îlot 1	extérieur de la trame	repère · îlot 1 · césure
	intérieur de la trame	
îlot 2	extérieur de la trame	repère · îlot 1 · césure · îlot 2 · césure
	intérieur de la trame	
îlot 3	extérieur de la trame ⚠	repère · îlot 1 · césure · îlot 2 · césure · îlot 3
	intérieur de la trame	césure
îlot 4	extérieur de la trame	repère · îlot 1 · césure · îlot 2 · césure · îlot 3
	intérieur de la trame	césure · îlot 4 · césure
îlot 5	extérieur de la trame	repère · îlot 1 · césure · îlot 2 · césure · îlot 3
	intérieur de la trame	césure · îlot 4 · césure · îlot 5 · césure
îlot 6	extérieur de la trame	repère · îlot 1 · césure · îlot 2 · césure · îlot 3
	intérieur de la trame	césure · îlot 4 · césure · îlot 5 · césure · îlot 6 · césure
retour à l'îlot 1	extérieur de la trame	repère · îlot 1 · césure · îlot 2 · césure · îlot 3
	intérieur de la trame	césure · îlot 4 · césure · îlot 5 · césure · îlot 6 · césure

⚠ ***Pour préserver l'orientation, la dernière case doit être blanche, si le repère initial est noir.***

Panneaux de routage

Ces deux panneaux sont à découper, remplir, puis à plier au niveau des pointillés pour pouvoir les poser sur la table.





SÉANCE 3

Transmettre un message long

Objectifs

Lever une des contraintes sur les messages, à savoir que la longueur ne doit pas dépasser la taille de la trame, à savoir 13 cases.
Introduire la notion de paquets : découpage des messages longs afin de les adapter à la taille de la trame.

Matériel

Pour l'ensemble de la classe :

- **6 kits de communication** [1]
  constitués d'une paire de pinces à linge reliées par un cordon sur lequel est enfilée une petite pince métallique
- **cartes *Consignes* (15 cases)** [5]
  1 par élève ou binôme (peuvent aussi être générées grâce aux ressources disponibles sur www.projetmerite.fr)
- **trames papier** [nf]
  13 cases recto-verso, prévoir un nombre suffisant, à imprimer depuis la clé USB ou www.projetmerite.fr
- **3 boîtes** [nf]
  pour comptabiliser les succès, échecs et pertes en fin de séance
- **FICHE** Tableau de conversion décimal-binaire
  1 photocopie par élève
- **FICHE** S'envoyer des messages
  fiche de la séance 1

[nf] Matériel non fourni
[0] Référence dans le catalogue du matériel

Déroulement pédagogique

1h

Dans un premier temps, il faut identifier les problèmes qui peuvent survenir à cause de contraintes imposées dans ce type de communication (utilisation de la trame).

Contraintes :

- celle imposée par le fait que la trame (face interne ou externe) doit absolument être **orientée** par un couple de cases (blanche/noire) aux extrémités, afin de pouvoir bien lire et exploiter le contenu (voir **FICHE** Interprétations possibles des trames, séance 1).
- celle liée **au message** : son contenu ne figure que sur la face interne de la trame. Des informations administratives peuvent apparaître sur les deux faces.
- une nouvelle contrainte liée à la **taille de la trame** qui est de 13, alors que celle du message est de 15 (et dépasse donc les capacités d'une seule trame).

Immersion

L'enseignant distribue les trames et les cartes *Consignes* (15 cases) aux élèves. Il prend le temps de réexpliquer le contenu de ces documents. Il fait constater aux élèves que les messages à envoyer font maintenant 15 cases, mais que la trame est toujours de 13 cases. Ils vont donc utiliser plusieurs trames.

EXPLICATION DES CONSIGNES

L'objectif est de faire circuler des messages qui ne rentrent pas en intégralité sur une seule trame. On impose donc que la charge utile soit limitée aux 13 cases de la trame interne. La trame externe sert à la partie administrative de la communication : adresse et toute autre information.

GLOSSAIRE
Charge utile

Le but de l'activité est double :

- réussir à envoyer son ou ses messages de 15 cases aux bons destinataires, en utilisant les trames de 13 cases,
- réussir à reconstituer les messages à partir des trames reçues.

Les élèves doivent appliquer les mêmes consignes que lors des précédentes activités :

- utiliser pour communiquer les seuls fils de connexion et les trames papier,
- le temps pour l'échange de messages est limité,
- les trames doivent être pliées, l'adresse à l'extérieur et le contenu à l'intérieur,
- si un élève décide d'ouvrir une trame qui lui est adressée et lit son contenu, cette trame doit absolument être gardée par lui, et associée par la suite à l'autre trame afin de reconstituer le message envoyé,
- à l'issue du temps imparti pour l'activité, les trames n'ayant pas été ouvertes (et donc non traitées) sont placées dans la boîte « Perte » : on dira que le paquet associé à ces trames n'a pas été distribué.

Points de passage

ACTIVITÉ 1

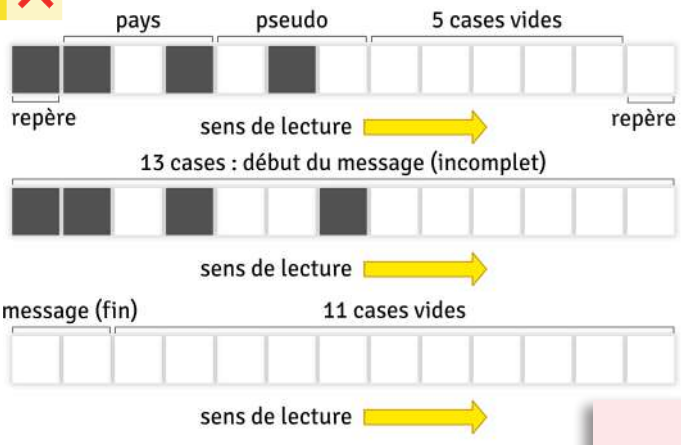
Règles :

- Longueur du message : **connue**, fixée à 15 cases
- Réception par un destinataire d'**un** seul message

L'enseignant précise aux élèves que :

- chaque élève aura son propre message à envoyer,
- l'élève continuera à jouer les 3 rôles déjà vus dans les séances précédentes : expéditeur, routeur, et destinataire,
- pour traiter les messages qui transitent par leur îlot, les élèves travailleront en binôme afin de faciliter et d'accélérer la circulation des messages.

Exemple de solution incorrecte ✗



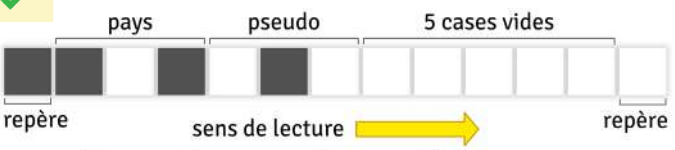
Problème : comment identifier le premier paquet du second ?
Solution : il faut numéroter les paquets (paquet 0 = case blanche ; paquet 1 = case noire).

GLOSSAIRE
Paquet

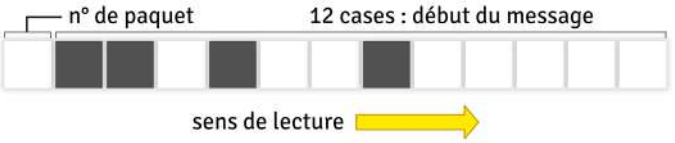
3 Transmettre un message long

Exemple de solution correcte ✓

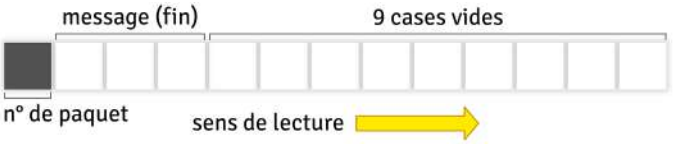
Face externe des trames



Face interne (de la trame 1)
paquet n°0



Face interne (de la trame 2)
paquet n°1



Principe : décomposition en 2 paquets numérotés.

L'enseignant peut commencer, à ce stade, à faire l'analogie entre le fonctionnement en couches d'un îlot et celui d'une machine (voir encadré en bas de page).

Chaque élève n'envoie qu'un seul message et doit :

- le recopier sur deux trames (comme le message dépasse 13 cases),
- envoyer les deux trames, isolément,
- diffuser les trames à un îlot voisin (en respectant les règles de circulation),
- faire circuler les messages reçus des autres îlots qui ne lui sont pas destinés (rôle de routeur),
- recomposer le message reçu s'il lui est destiné.

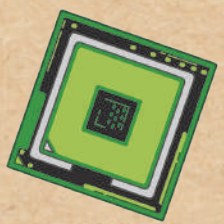
POINTS D'ATTENTION

Pour l'étape d'envoi des deux trames, les élèves pourraient proposer de les coller ou les plier l'une dans l'autre. S'ils ne donnent pas d'indication sur l'ordre de découpage du message, la reconstruction par le destinataire restera difficile.

Pour l'étape de recomposition du message, certains élèves peuvent rencontrer des difficultés si les trames n'ont pas été numérotées ou si le bon découpage du message est difficile à identifier.

LIEN AVEC LA COMMUNICATION ENTRE MACHINES

Chaque îlot fonctionne comme une machine dans un réseau de communication. L'îlot fournit un empilement de couches protocolaires. Un élève joue le rôle d'un utilisateur dans la couche applicative lorsqu'il envoie un message, mais aussi d'un programme dans la couche de transport lorsqu'il décompose en paquets ou recompose les paquets.



Bilan : l'enseignant fait le bilan avec la classe de ce qui a fonctionné et ce qui n'a pas fonctionné. Il propose aux élèves d'établir un protocole pour numéroter les paquets et les identifier précisément. Il est aussi important de préserver les règles déjà rencontrées, concernant l'orientation du recto et celle du verso. L'objectif pour l'enseignant n'est pas seulement d'aboutir à un protocole correct mais aussi de montrer le processus qui y mène, par une succession d'essais-erreurs.

POINTS D'ATTENTION

Suite à cette première activité, le protocole est maintenant établi. Il est conseillé de l'afficher au tableau avant de démarrer les activités suivantes.

Les activités suivantes (2, 3 et 4) ne sont pas obligatoires mais fortement conseillées car elles permettent aux élèves de réinvestir les acquis de l'activité 1.

ACTIVITÉ 2

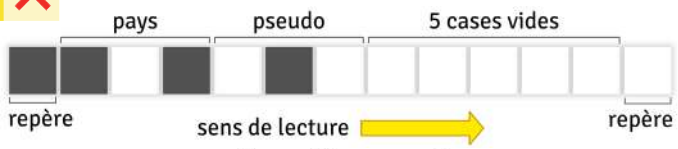
Règles :

- Longueur du message : variable et **inconnue** du destinataire (doit être inférieure à 32)
- Réception par un destinataire d'**un** seul message

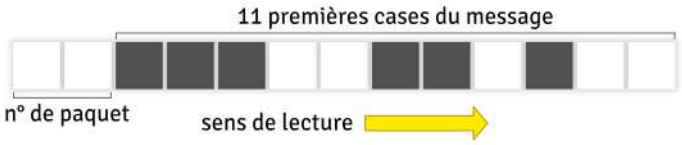
Exemple : envoi d'un message de longueur 27 (la longueur n'est pas connue par le destinataire)

Exemple de solution incorrecte ✗

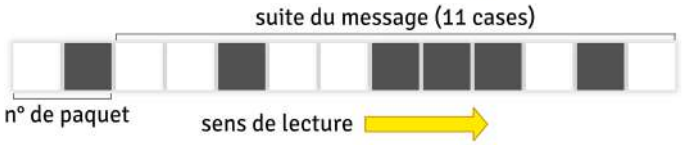
Face externe des trames



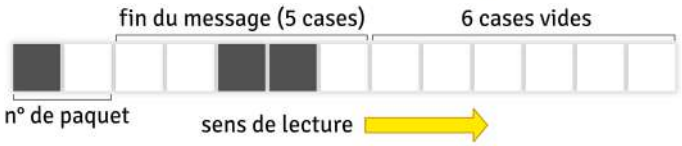
Face interne (de la trame 1)
paquet n°0



Face interne (de la trame 2)
paquet n°1



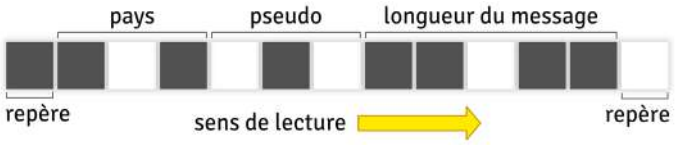
Face interne (de la trame 3)
paquet n°2



Problème : le destinataire ne sait pas quand finit le message puisqu'il ne connait pas sa longueur.
Solution : il faut ajouter une information sur la longueur du message sur la face externe.

Exemple de solution correcte ✓

Face externe des trames



Faces internes (trames 1, 2 et 3) : les mêmes que dans l'encart « Exemple de solution incorrecte »

Principe : décomposition en 3 paquets numérotés + information sur la longueur du message. Avec 5 cases, on ne peut communiquer que des longueurs de message allant jusqu'à 31 (voir **FICHE** Tableau de conversion décimal-binaire).

ACTIVITÉ 3

Règles :

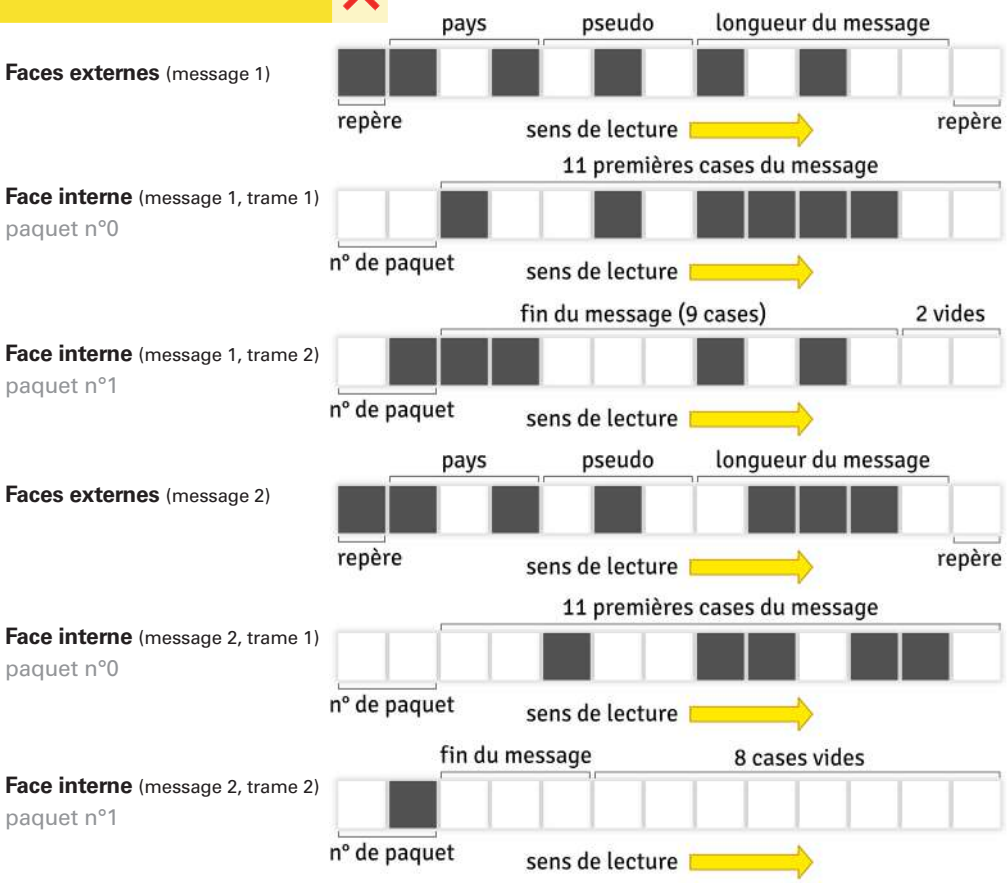
- Longueur du message : variable et **inconnue** du destinataire (doit être inférieure à 32)
- Réception par un destinataire de **2** messages provenant d'**expéditeurs distincts**

Exemple : un 1er expéditeur envoie un message de longueur 20 à un destinataire et un second expéditeur envoie un message de longueur 14 au même destinataire.

Message 1 (expéditeur 1)

Message 2 (expéditeur 2)

Exemple de solution incorrecte ✗

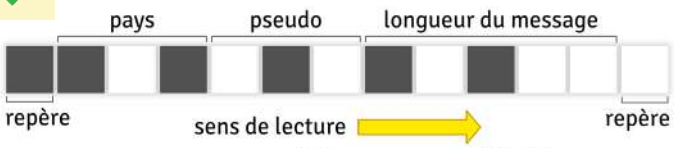


Problème : dans ce cas, le destinataire est incapable de distinguer les paquets du message 1 de ceux du message 2 (il pourrait mélanger les paquets).
Solution : il faut ajouter une information sur l'expéditeur sur la face interne de la trame.

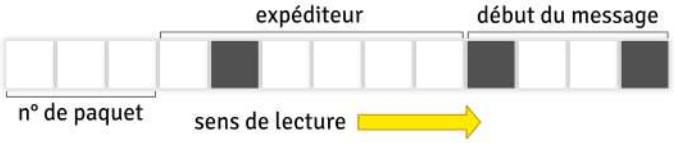
Le code pays et le pseudo (6 cases en tout) sont donc à ajouter sur la face interne des trames, juste après le numéro de paquet. Ainsi, le destinataire est capable d'identifier l'expéditeur et ne mélange pas les paquets. La charge utile de la trame n'est alors plus que de 4 cases (13 - 3 cases pour le n° de paquet - 6 cases pour l'expéditeur = 4 cases) ; on doit donc découper le message en un nombre de paquets plus grand (voir exemple).

Exemple de solution correcte

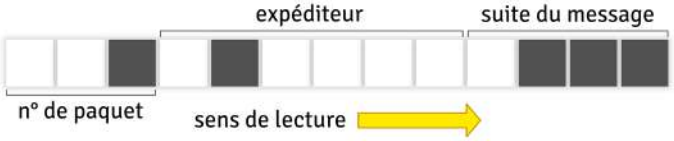
Faces externes (message 1)



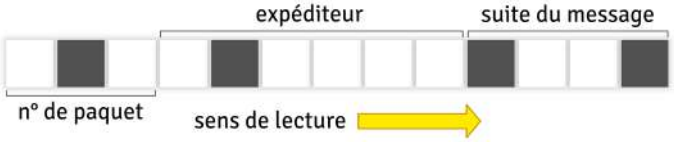
Face interne (message 1, trame 1)
paquet n°0



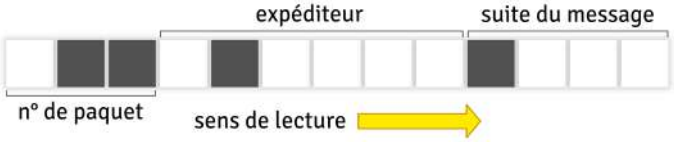
Face interne (message 1, trame 2)
paquet n°1



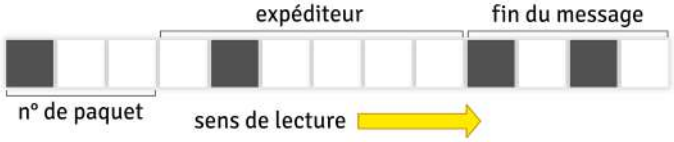
Face interne (message 1, trame 3)
paquet n°2



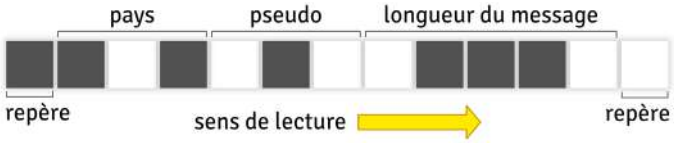
Face interne (message 1, trame 4)
paquet n°3



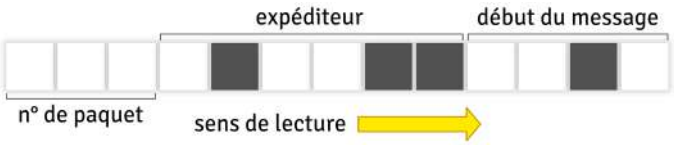
Face interne (message 1, trame 5)
paquet n°4



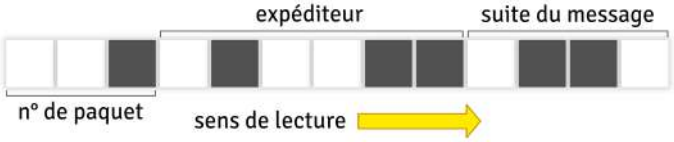
Faces externes (message 2)



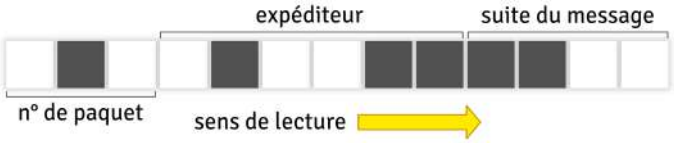
Face interne (message 2, trame 1)
paquet n°0



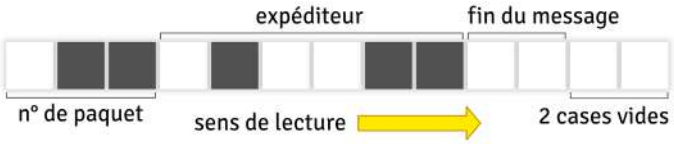
Face interne (message 2, trame 2)
paquet n°1



Face interne (message 2, trame 3)
paquet n°2



Face interne (message 2, trame 4)
paquet n°3



Attention : il faut garder 3 cases pour la numérotation des paquets puisque le découpage du message peut amener jusqu'à la création de 8 paquets (pour un message d'au moins 29 cases).

ACTIVITÉ 4

Règles :

- Longueur du message : variable et **inconnue** du destinataire (doit être inférieure à 16)
- Réception par un destinataire de **2** messages provenant d'**expéditeurs distincts ou non**

Exemple : Un expéditeur envoie deux messages, de longueur 15 et 14 respectivement, au même destinataire.

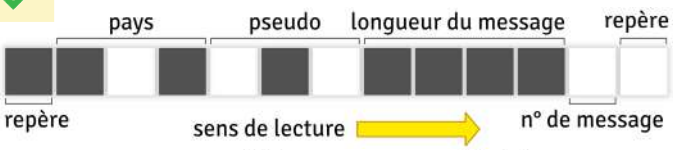
Message 1 (expéditeur 1)

Message 2 (expéditeur 1)

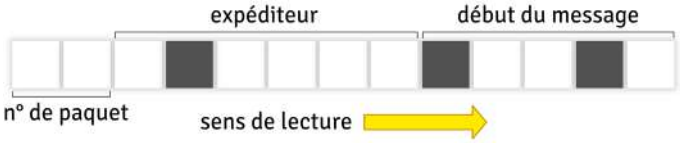
Si on utilise la même solution que précédemment, comment distinguer les paquets des deux messages du même expéditeur ?

Exemple de solution correcte ✓

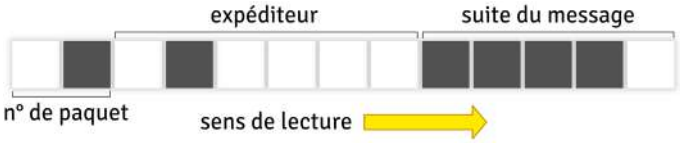
Faces externes (message 1)



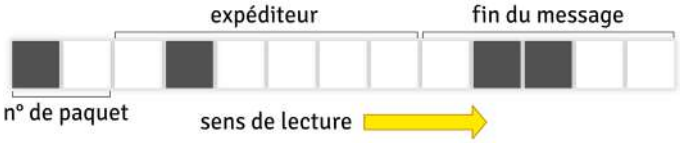
Face interne (message 1, trame 1)
paquet n°0



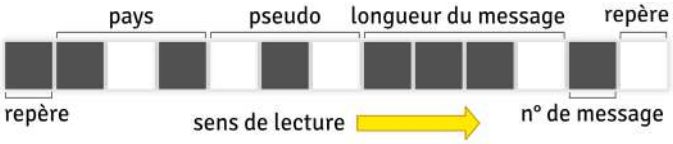
Face interne (message 1, trame 2)
paquet n°1



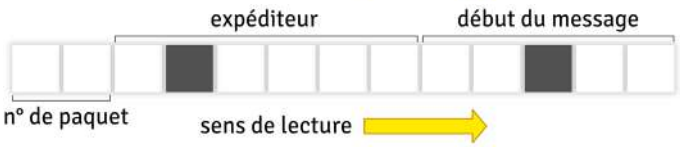
Face interne (message 1, trame 3)
paquet n°2



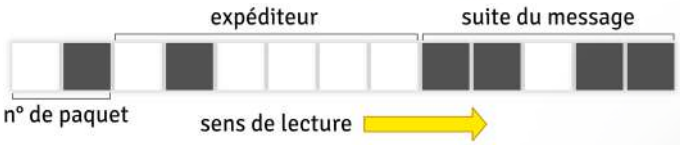
Faces externes (message 2)



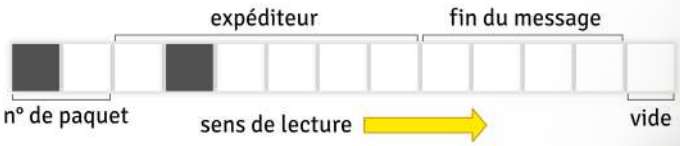
Face interne (message 2, trame 1)
paquet n°0



Face interne (message 2, trame 2)
paquet n°1



Face interne (message 2, trame 3)
paquet n°2



Comme il est possible de le voir sur l'exemple ci-avant, la solution consiste à utiliser la dernière case de la trame extérieure pour y renseigner le numéro du message. Cela a pour conséquence de ne laisser disponibles plus que 4 cases pour la longueur du message. Ainsi, il est impossible d'effectuer cet exercice avec des messages dont la longueur dépasse 15 cases (il manquerait alors une 5e case pour l'écriture de la longueur du message).

Découvertes réalisées

L'enseignant fait le bilan des activités de la séance et des deux précédentes.

L'objectif ici est que les élèves constatent qu'une machine effectue, en une fraction de seconde, beaucoup d'opérations, et que ces opérations peuvent être assimilées à 3 couches différentes : adressage, routage, découpage. Cette action de découpage est réalisée dans la couche du protocole Internet. Les messages sont découpés en paquets appelés datagrammes. Chaque paquet peut suivre une route différente. À réception, le message est recomposé à partir des paquets. Un paquet contient un en-tête avec des informations rappelant celles du protocole réalisé en classe.

L'enseignant attire aussi l'attention des élèves sur leur participation à améliorer le réseau de communication de la classe. En effet, chaque activité a obligé les élèves à mettre au point un nouveau service qui n'existait pas au départ :

Activité 1 : on peut maintenant échanger un message **de plus de 13 cases**,

Activité 2 : on peut maintenant échanger un message **de longueur variable et inconnue**,

Activité 3 : on peut maintenant échanger **deux** messages de longueur variable et inconnue,

Activité 4 : ces messages peuvent provenir **du même expéditeur**. ■

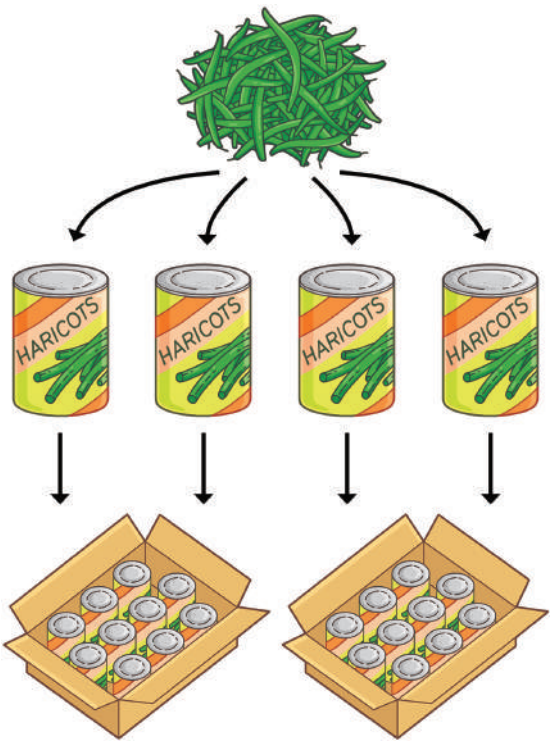
LIEN AVEC LES RÉSEAUX INFORMATIQUES

L'amélioration du réseau de communication de la classe renvoie aux activités du module 2 (communication informatique) au cours desquelles les élèves vont également devoir développer de nouveaux services mais, cette fois, pour améliorer une application de communication numérique. Si l'enseignant le souhaite, il peut commencer dès maintenant à faire des liens avec la suite de la progression.

Les paquets

Il est possible de vulgariser la notion de paquets en s'aidant d'une comparaison :

Imaginons qu'on doive envoyer 100 kg de haricots verts en conserve. Il ne viendrait à l'idée de personne de les mettre dans un bocal géant. Il serait difficile de le manipuler et s'il cassait en cours de route, toute la cargaison serait perdue. La solution privilégiée est de mettre tous ces haricots dans des pots plus petits (par exemple 500 g) et conditionner les 200 pots dans 20 cartons de 10.



Dans cet exemple, le message est représenté par les 100 kg de haricots et l'équivalent d'une trame est représenté par une boîte.

On opère exactement de la même manière pour la transmission de données sur un réseau.

Au cours d'une transaction (envoi ou réception d'un message, chargement d'une page de la toile, transfert d'un fichier *etc.*) la quantité de données à véhiculer est extrêmement variable et peut aller de quelques ko (kilo-octets) à plusieurs Go (Giga-octets). Pour éviter de tout perdre en cas d'incident et surtout pour faciliter l'écoulement sur le réseau (plusieurs petites voitures circulent mieux sur les routes qu'un convoi exceptionnel) on découpe l'ensemble à transmettre en fragments de taille réduite et uniforme (typiquement de l'ordre de 1,5 ko).

Chacun de ces fragments dûment identifié et pourvu de l'adresse du destinataire est envoyé séparément sur le réseau, lequel gère son acheminement jusqu'à bon port. On parle, d'une manière générale, de transmission par paquets.

La comparaison proposée permet de comprendre la notion de paquets mais n'aborde pas la question de la distinction des messages et de leur ordre.

Tableau de conversion décimal-binaire

Dans les activités de la séance, des valeurs décimales (comme la longueur d'un message) sont à exprimer en code binaire (les cases de la trame, pouvant prendre deux valeurs : blanc / 0 ou noir / 1). Le tableau ci-dessous permet de convertir une valeur décimale en binaire (et inversement). Il ne fournit ces éléments que pour les cas où on utilise 5 cases ou moins pour écrire une valeur. La nature même du code binaire (le nombre de combinaisons possibles : $2^5 = 32$) implique qu'on ne peut alors écrire que des valeurs allant de 0 à 31 avec seulement 5 cases.

0	0	0	0	0	0
1	0	0	0	0	1
2	0	0	0	1	0
3	0	0	0	1	1
4	0	0	1	0	0
5	0	0	1	0	1
6	0	0	1	1	0
7	0	0	1	1	1
8	0	1	0	0	0
9	0	1	0	0	1
10	0	1	0	1	0
11	0	1	0	1	1
12	0	1	1	0	0
13	0	1	1	0	1
14	0	1	1	1	0
15	0	1	1	1	1

16	1	0	0	0	0
17	1	0	0	0	1
18	1	0	0	1	0
19	1	0	0	1	1
20	1	0	1	0	0
21	1	0	1	0	1
22	1	0	1	1	0
23	1	0	1	1	1
24	1	1	0	0	0
25	1	1	0	0	1
26	1	1	0	1	0
27	1	1	0	1	1
28	1	1	1	0	0
29	1	1	1	0	1
30	1	1	1	1	0
31	1	1	1	1	1

Code couleur

X	Valeurs décimales qu'il est possible de convertir en binaire en n'utilisant **qu'une seule case** : 0 et 1
X	Valeurs décimales qu'il est possible de convertir en binaire en utilisant **2 cases** : de 0 à 3*
X	Valeurs décimales qu'il est possible de convertir en binaire en utilisant **3 cases** : de 0 à 7*
X	Valeurs décimales qu'il est possible de convertir en binaire en utilisant **4 cases** : de 0 à 15*
X	Valeurs décimales qu'il est possible de convertir en binaire en utilisant **5 cases** : de 0 à 31*

** les valeurs qui peuvent s'écrire avec une case peuvent être écrites avec 2 cases également, en rajoutant un 0 (case blanche) devant, et ainsi de suite... (ex : 0 = 00 ; 101 = 0101...).*

SÉANCE 4

Sécuriser un message

Objectifs

Initier les élèves à la sécurité informatique.
Découvrir la notion de confidentialité des données (les données ne sont lues que par les personnes autorisées).

Matériel

Pour l'ensemble de la classe :

- **6 kits de communication** [1]
  constitués d'une paire de pinces à linge reliées par un cordon sur lequel est enfilée une petite pince métallique
- **tirelires en bois** [2]
  en forme de maison, 1 par îlot
- **cadenas à code** [3]
  1 par îlot
- **trames papier** [nf]
  13 cases recto-verso, plusieurs par élève ou binôme

[nf] Matériel non fourni
[0] Référence dans le catalogue du matériel

Déroulement pédagogique

Dans cette séance, la classe va s'intéresser à la notion de confidentialité.
La classe est organisée en îlots.
Les élèves d'un îlot forment un ensemble et jouent ensemble les rôles de : expéditeur, routeur, destinataire. Il n'y a qu'un message par îlot (et non par élève comme pour les séances précédente).

Immersion

L'enseignant explique que dans cette activité il s'agit d'échanger un message entre expéditeur et destinataire, dont le contenu doit rester secret. Cependant, un îlot intermédiaire peut théoriquement accéder au contenu du message.

L'enseignant questionne la classe :

Comment procéder pour assurer la confidentialité d'un message ?

Une réponse attendue est : en chiffrant les messages. C'est une solution efficace si l'attaquant interceptant le message est incapable de le décrypter (elle sera utilisée lors des activités numériques du second module). Dans cette activité, le chiffrement est matérialisé par l'usage de tirelires avec cadenas. Cette analogie va permettre de saisir les concepts importants de la cryptologie.

Points de passage

ACTIVITÉ 1 : UTILISATION DE TIRELIRES CADENASSÉES, AVEC PARTAGE DE CODE ENTRE 2 ÎLOTS

L'enseignant interroge la classe :

Comment procéder avec les tirelires munies de cadenas ?

En partageant le code de la tirelire entre l'expéditeur et le destinataire. Un parallèle peut être fait avec la notion de chiffrement symétrique (voir **FICHE** Sécurité informatique).

Protocole

L'îlot expéditeur :

- rédige le message,
- le place dans la tirelire et verrouille celle-ci avec le cadenas,
- envoie le message.

L'îlot routeur :

- intercepte le message,
- n'a qu'une seule solution pour lire le message : essayer de trouver le code (puisqu'on exclut toute autre approche, notamment destructrice),
- y réussit, très probablement après un temps long,
- route le message.

L'îlot destinataire :

- à réception du message, déverrouille la tirelire avec le code,
- lit le message.

Que retenir ?

L'intercepteur peut ouvrir la tirelire au bout d'un temps (probablement) très long.

C'est un exemple d'attaque par force brute : toutes les combinaisons possibles sont essayées jusqu'au succès. C'est une attaque classique en informatique : l'attaquant essaie toutes les clés possibles de chiffrement dans l'espoir de décrypter le message. À mesure que les capacités de calcul augmentent, la longueur des clés augmente, de manière à garantir que le temps pour tous ces essais demeure très long.

L'expéditeur peut se rendre compte de l'interception si un accusé de réception est imposé par le protocole :
si au bout d'un certain temps, aucun accusé n'est arrivé, c'est qu'il y a sans doute une attaque.

Cependant, il n'est pas exclu qu'un attaquant puisse envoyer un faux accusé de réception dans les délais.

Comment l'expéditeur peut-il déterminer qu'il s'agit d'un faux accusé de réception ?

Le message contient une information secrète à envoyer avec l'accusé de réception : l'attaquant ne peut envoyer un accusé qu'après avoir décrypté le message.

Bilan de l'activité : la solution proposée est sûre mais suppose donc de partager le code avant de communiquer. Cela représente une limitation dans la communication entre machines, et notamment dans le cas (fréquent) où elles sont distantes.

LIEN AVEC LA SÉCURITÉ INFORMATIQUE

Il est utile, au moment de débuter l'activité, de faire le lien entre celle-ci et ce qui se passe dans un réseau informatique.

L'enseignant peut utiliser l'analogie suivante :

***Code du cadenas** = clé de chiffrement*

***Mettre le message dans la tirelire et verrouiller celle-ci** = chiffrer le message*

***Message dans la tirelire fermée** = message chiffré*

***Déverrouiller la tirelire avec le code et récupérer le message** = déchiffrer le message*

***Ouvrir la tirelire sans connaître au préalable le code et récupérer le message** = décrypter le message*

GLOSSAIRE

Chiffrement

ACTIVITÉ 2 : UTILISATION DE TIRELIRES CADENASSÉES, SANS PARTAGE DE CODE ENTRE ÎLOTS

L'enseignant lance l'activité avec une question :

Comment procéder sans le partage de code ?

Chaque îlot possède une tirelire à code, et ne connait que le code de sa propre tirelire. Les tirelires ont la particularité d'être munies d'une fente. On suppose que malgré cette ouverture, les tirelires sont inviolables : le seul moyen d'avoir accès au contenu d'une tirelire verrouillée est de la déverrouiller.

La solution à ce problème est simple, sans être évidente à trouver : même verrouillée (donc cadenassée), la tirelire peut accepter un nouveau message grâce à la fente.

POINT D'ATTENTION

Cette solution est décrite dans un article célèbre : New directions in cryptography *(Diffie & Hellman, 1976) – « We stand today on the brink of a revolution in cryptography ». Cet article pose les bases de la cryptographie asymétrique. Cette dernière repose sur l'existence d'une clé publique (accessible à tous et permettant le contact entre l'expéditeur et le destinataire) et d'une clé privée (permettant de déchiffrer le message et, par définition, pas accessible à tous). Pour en savoir plus sur la notion de cryptographie asymétrique, consulter la* **FICHE** Sécurité informatique *).*

Protocole :

L'expéditeur envoie un premier message au destinataire pour signifier son intention de communiquer.

Le destinataire envoie à l'expéditeur sa tirelire verrouillée vide.

À réception de la tirelire, l'expéditeur met son message dans la tirelire grâce à l'ouverture, et renvoie le coffre au destinataire.

À réception de sa tirelire, le destinataire le déverrouille et lit le message.

Bilan de l'activité : l'intercepteur ne peut ouvrir la tirelire, le message reste donc confidentiel.

ACTIVITÉ 3 : FIABILITÉ DU PROTOCOLE PRÉCÉDENT

L'enseignant lance l'activité suivante :

Est-il possible d'attaquer le protocole vu en activité 2 ?

L'intercepteur (l'attaquant) est dans une position intermédiaire entre les deux îlots qui communiquent. On suppose qu'il dispose aussi d'une tirelire. Il peut ainsi exploiter sa position d'intermédiaire et essayer de lire le message.

Protocole :

L'expéditeur envoie un message pour signifier son intention de communiquer.

À réception du message, le destinataire envoie à l'expéditeur sa tirelire verrouillée vide.

L'attaquant intercepte, conserve la tirelire du destinataire et envoie sa propre tirelire verrouillée à l'expéditeur à la place.

À réception de la tirelire, l'expéditeur y glisse son message par la fente et la renvoie.

L'attaquant intercepte la tirelire, la déverrouille et lit le message. Il remet ensuite le message dans la tirelire du destinataire et la lui transmet.

À réception de sa tirelire, le destinataire la déverrouille et lit le message.

Bilan de l'activité : l'attaquant a pu lire le message sans que ni l'expéditeur, ni le destinataire ne s'en rendent compte. C'est l'attaque de l'intercepteur, dite de l'homme du milieu (« man in the middle »).

ACTIVITÉ 4 : DÉFENSE CONTRE L'ATTAQUE DE L'INTERCEPTEUR

L'enseignant amorce cette dernière activité en posant la question :

Peut-on se défendre contre l'attaque décrite en activité 3 ?

Pour empêcher l'attaque, il suffit de pouvoir attribuer une tirelire à son propriétaire, par exemple en les numérotant. Un répertoire de ces numéros est constitué et fourni à chaque îlot. Ainsi, lorsque l'expéditeur reçoit la tirelire de l'attaquant, il la compare au répertoire et il ne peut l'attribuer au destinataire : il renonce ainsi à envoyer un message.

Bilan de l'activité : la solution repose sur une information partagée, le répertoire permettant l'identification de la tirelire.

Découvertes réalisées

Contrairement au cas initial où un code secret est partagé (activité 1), dans les activités 2-3-4 c'est une information publique qui est ici diffusée par le propriétaire de la tirelire. Aucune information secrète n'est partagée. C'est le protocole, simple mais subtil, qui permet un échange confidentiel. ■

GLOSSAIRE

Clé de chiffrement

LIEN AVEC LES INFRASTRUCTURES DE GESTION DE CLÉS PUBLIQUES

Ce répertoire pour les tirelires a un analogue pour les clés publiques. Il existe différents systèmes de gestion des clés qui permettent de déterminer si une clé publique appartient bien au propriétaire présumé.
Par exemple, un site Web utilisant le protocole sécurisé https envoie au client une clé publique.
Cette clé publique fait partie d'un certificat que le navigateur client peut vérifier auprès d'une autorité de certification (il vérifie si elle est répertoriée). Cette autorité de certification est pré-installée avec le navigateur.

Sécurité informatique

La sécurité informatique traite, en général, de 3 trois grands problèmes :

Confidentialité des données

Un système sécurisé garantit que les données ne sont lues que par les personnes autorisées.

Intégrité des données

Un système sécurisé garantit que les données ne sont modifiées que par les personnes autorisées.

Disponibilité des données

Un système sécurisé garantit que les personnes autorisées peuvent accéder aux données qui les intéressent.

Pour garantir la confidentialité et l'intégrité des données, un système cherche à éviter toute interception de données.

Pour garantir la disponibilité, un système cherche à éviter tout accès intempestif, qui empêcherait l'accès à des personnes autorisées.

La séance 4 s'intéresse particulièrement à la notion de confidentialité.

La science qui s'intéresse au chiffrement est nommée cryptologie. L'écriture de messages secrets est appelée cryptographie. Les méthodes et les techniques utilisées pour décrypter un message dont on ignore la clé de déchiffrement est appelée cryptanalyse (la force brute en est un exemple).

Qu'est-ce qu'un algorithme de chiffrement et quels sont ses avantages en termes de sécurité ?

La cryptographie à clé publique, ou cryptographie asymétrique, est une méthode de chiffrement qui utilise deux clés distinctes : une clé publique et une clé privée. À l'inverse des algorithmes de cryptographie symétrique - qui dépendent d'une seule clé pour le chiffrement et le déchiffrement - les clés de la cryptographie asymétrique ont chacune une fonction bien spécifique : la clé publique sert à chiffrer et la clé privée sert à déchiffrer.

Il est impossible de deviner la clé privée à partir de la clé publique. C'est pourquoi les clés publiques peuvent être partagées sans danger, permettant ainsi aux utilisateurs de bénéficier d'une méthode facile et pratique de chiffrement de contenu et de vérification de signature numérique. Les clés privées restent secrètes, ce qui garantit que seul leur propriétaire peut déchiffrer du contenu et créer des signatures numériques.

La cryptographie asymétrique permet de résoudre un problème de partage de secret : comment échanger un message secret sans partager un secret initialement ? C'est un problème difficile dont la résolution date d'une cinquantaine d'années (les années 70).

La cryptographie symétrique permet de résoudre un problème de chiffrement : comment échanger un message secret en ayant partagé initialement un secret, la clé de chiffrement ? C'est un problème plus simple, pour lequel il existe des solutions très anciennes, comme le chiffre de César.

GLOSSAIRE

Cryptographie

Cryptologie

MODULE 2

LA COMMUNICATION INFORMATIQUE

Présentation générale

Après avoir étudié les contraintes d'une communication en réseau, sur un support papier et en utilisant des pseudos, les élèves vont s'intéresser à la communication entre machines et au support numérique. Des applications Web, comme par exemple l'application Tchat, permettent aux ordinateurs, tablettes, smartphones, de communiquer en réseau.

Les élèves découvrent que les services (couches) offerts par l'application peuvent répondre à des contraintes déjà abordées au module 1, telles que l'adressage et le routage. Ils ne sont cependant pas toujours suffisants pour satisfaire de nouveaux besoins, comme, par exemple une communication entre utilisateurs via leurs identités réelles ou bien encore une communication sécurisée qui fait appel aux clés de chiffrement et déchiffrement privée et publique. Les élèves, invités à imaginer et à produire les services manquants, sont en mesure de comprendre le mécanisme de création d'un protocole de communication informatique, et de percevoir les différences avec celui de la communication humaine.

Apprentissages visés

Pratiquer des démarches scientifiques et technologiques

Imaginer, synthétiser, formaliser et respecter une procédure, un protocole

Rechercher des solutions techniques à un problème posé, expliciter ses choix et les communiquer en argumentant

Participer à l'organisation et au déroulement de projets

Concevoir, créer, réaliser

S'approprier un cahier des charges

Associer des solutions techniques à des fonctions

Imaginer des solutions en réponse au besoin

Réaliser, de manière collaborative, le prototype de tout ou partie d'un objet pour valider une solution

Imaginer, concevoir et programmer des applications informatiques pour des appareils nomades

S'approprier des outils et des méthodes

Exprimer sa pensée à l'aide d'outils de description adaptés : croquis, schémas, graphes, diagrammes, tableaux (représentations non normées)

Traduire, à l'aide d'outils de représentation numérique, des choix de solutions sous forme de croquis, de dessins ou de schémas

Présenter à l'oral et à l'aide de supports numériques multimédia des solutions techniques au moment des revues de projet

Pratiquer des langages

Décrire, en utilisant les outils et langages de descriptions adaptés, la structure et le comportement des objets

Appliquer les principes élémentaires de l'algorithmique et du codage à la résolution d'un problème simple

Mobiliser des outils numériques

Simuler numériquement la structure et/ou le comportement d'un objet

Lire, utiliser et produire des représentations numériques d'objets

Piloter un système connecté localement ou à distance

Modifier ou paramétrer le fonctionnement d'un objet communicant

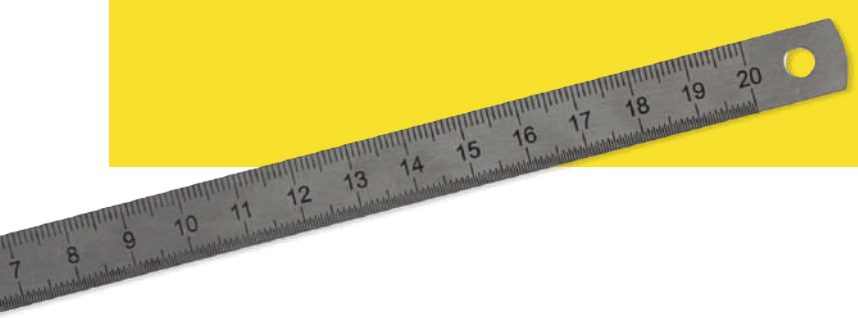
Adopter un comportement éthique et responsable

Développer les bonnes pratiques de l'usage des objets communicants

Analyser l'impact environnemental d'un objet et de ses constituants

Se situer dans l'espace et dans le temps

Relier les évolutions technologiques aux inventions et innovations qui marquent des ruptures dans les solutions techniques



3 séances

Séances du module

SÉANCE 1 — **Discuter avec l'application Tchat**

SÉANCE 2 — **Échanger des messages numériques**

SÉANCE 3 — **Sécuriser les messages de l'application Tchat**

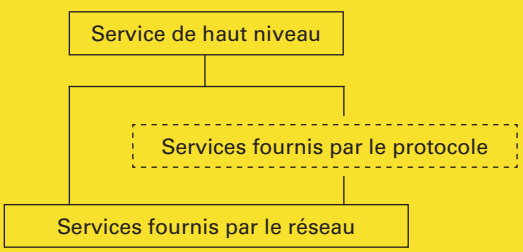
Références

Socle commun de connaissances de compétences et de culture BO N°17 du 23 avril 2015
Programmes scolaires B0 N° 11 du 26 nov 2015 et B0 N°48 du 24 déc 2015

Attendus Fin de Cycle (AFC)	Compétences et Connaissances Associées (CCA)
• **Technologie :** **Design, innovation et créativité** Imaginer des solutions en réponse aux besoins, matérialiser des idées en intégrant une dimension design	Identifier un besoin et énoncer un problème technique ; identifier les conditions, contraintes (normes et règlements) et ressources correspondantes, qualifier et quantifier simplement les performances d'un objet technique existant ou à créer Imaginer, synthétiser et formaliser une procédure, un protocole
L'informatique et la programmation Comprendre le fonctionnement d'un réseau informatique Écrire, mettre au point et exécuter un programme	Composants d'un réseau, architecture d'un réseau local, moyens de connexion d'un moyen informatique Notion de protocole, d'organisation de protocoles en couche, d'algorithme de routage Internet

Conseils pour la mise en œuvre

À chaque réseau rencontré par la suite correspondent une ou plusieurs activités. Chaque activité a pour but de fournir (développer) un service que le réseau n'offre pas. Pour réaliser ce service de haut niveau (voir schéma ci-contre), un ou plusieurs services plus élémentaires, de plus bas niveau, sont requis. S'ils ne sont pas fournis par le réseau, ils doivent être fournis par le protocole : c'est la solution que les élèves doivent développer. Elle apparaît en pointillés dans le schéma ci-contre : pour réaliser le service de haut niveau, on utilise des services existants fournis par le réseau et des services à développer, fournis par le nouveau protocole.



SÉANCE 1

Discuter avec l'application Tchat

Objectifs

Échanger des messages via un réseau informatique, en utilisant l'application Tchat.

Utiliser deux types de réseaux - en étoile et en anneau - et découvrir que le réseau en étoile offre plus de services que le réseau en anneau.

Découvrir que la communication informatique se fait à travers des fonctions qu'on appelle couches (qui fournissent des services).

Comprendre que l'application Tchat est une couche, dite applicative, car elle fait appel à d'autres couches.

Se familiariser avec la création de nouvelles couches, en passant du réseau en étoile à celui en anneau.

Matériel

Par élève ou par binôme :

- **1 ordinateur** nf connecté à Internet
- **application Tchat** disponible via www.projetmerite.fr

nf Matériel non fourni

Déroulement pédagogique

1h10

Chaque élève est installé devant un ordinateur, soit seul, soit en binôme (un seul pseudo par binôme). L'élève (ou binôme) est relié aux membres de son réseau virtuel, et ne peut communiquer qu'avec eux. Les membres d'un réseau peuvent s'échanger des messages textuels, sans contraintes particulières.

Immersion

L'enseignant introduit l'activité par quelques questions générales introductives :

Les postes informatiques de la classe peuvent-ils communiquer entre eux ?

Réponse attendue : oui, grâce au réseau (filaire Ethernet ou le WiFi).

Que faut-il connaître pour pouvoir communiquer ?

Réponse attendue : l'adresse du destinataire et le chemin (route).

Quelle est la forme du réseau des postes de la classe ?

Réponse attendue : en étoile, c'est-à-dire que tous les postes sont reliés les uns aux autres par un équipement central (comme un concentrateur ou un routeur).

Quelle est la forme du réseau internet ?

Réponse attendue : en étoiles, anneaux et ponts (une organisation compliquée mais hiérarchisée).

GLOSSAIRE

Application

Application Web

Couche (protocolaire)

Points de passage

ACTIVITÉ 1 : APPLICATION TCHAT – RÉSEAU EN ÉTOILE

L'enseignant fournit toutes les explications nécessaires pour que les élèves puissent se connecter.

Par défaut, il y a 5 élèves en réseau par espace virtuel. Les élèves sont identifiés par des pseudos (*dede*, *fifi*, *jojo*, *lulu*, *zaza*) qui sont inscrits au tableau. Les messages circulent dans un réseau en étoile (voir **FICHE** Tchat (réseau en étoile ou en anneau)).

L'enseignant annonce l'objectif aux élèves :

Vous devez créer un service qui vous permet de communiquer entre vous en utilisant vos identités réelles et non des pseudos.

Pour l'instant, les services fournis par le réseau sont les suivants :

- communication entre un utilisateur identifié par son pseudo avec un autre utilisateur identifié lui aussi par son pseudo,
- diffusion des messages d'un utilisateur identifié par son pseudo à tous les autres utilisateurs identifiés par leur pseudo.

L'objectif pour les élèves est donc le suivant : élaborer une table de correspondance qui permet de faire le lien entre pseudo et identité réelle de chaque élève.

POINT D'ATTENTION

Il existe au moins deux solutions pour remplir cet objectif. L'enseignant présente ces solutions sans dire aux élèves laquelle est optimale.

Solution 1

Chaque élève diffuse un message aux 4 autres pour leur demander de lui fournir leur identité.

Le nombre de messages envoyés dans ce cas est de 20 (4x5) : cette solution n'est pas optimale.

Solution 2

Les élèves choisissent un responsable réseau (par exemple zaza) à qui envoyer l'information : leur pseudo et leur identité. Ce responsable réseau se charge ensuite d'envoyer à tous les autres utilisateurs les correspondances pseudo-identité.

Le nombre total de messages envoyé est de 8 (4 messages envoyés au responsable réseau puis 4 messages par le responsable réseau aux autres utilisateurs). Cette solution est donc plus efficace que la première, car elle nécessite moins de messages envoyés.

Chaque groupe d'élèves propose une solution et choisit ensuite celle qui lui convient le mieux pour réaliser l'activité.

Bilan de l'activité 1

Les deux solutions permettent d'obtenir une table de correspondance, mais la solution 2 permet de l'obtenir avec un minimum de messages envoyés. C'est la solution optimale.

L'obtention d'une table de correspondance pseudo-identité a permis de réaliser un protocole qui fournit un service qui n'existait pas initialement dans l'application.

Grâce à ce protocole fournissant le service de résolution des noms (pseudos), il est dorénavant possible pour les élèves d'un espace virtuel de communiquer en utilisant directement leurs identités et non leurs pseudos.

Un service manquant dans une application peut être créé et ajouté (par les utilisateurs) aux services existants de celle-ci. Il constituerait une nouvelle couche de l'application.

GLOSSAIRE

Protocole

Résolution des noms

ACTIVITÉ 2 : APPLICATION TCHAT – RÉSEAU EN ANNEAU

Les consignes sont les mêmes que pour l'activité précédente, à la seule différence que les messages ne circulent plus en étoile, mais en anneau : un élève ne peut communiquer qu'avec ses deux voisins (qui lui sont attribués par l'application) et ne peut pas envoyer son message à tous les élèves de son espace virtuel.
Les équipes de 5 élèves par espace virtuel restent inchangées et les élèves sont, de nouveau, identifiés par des pseudos.

L'enseignant annonce l'objectif aux élèves :

Vous devez obtenir un service qui permet à deux utilisateurs non-voisins de communiquer.

Pour l'instant, le service fourni par le réseau est le suivant :

- communication d'un utilisateur identifié par son pseudo à un utilisateur voisin identifié lui aussi par son pseudo.

L'objectif pour les élèves est donc le suivant : déterminer un protocole d'adressage et de routage qui permet à tous les élèves d'un réseau virtuel de communiquer entre eux (et surmonter ainsi la limitation d'une communication entre voisins).

POINT D'ATTENTION

Il est important de :

- *demander à chaque élève qui se connecte de bien identifier ses deux voisins (leurs pseudos),*
- *bien indiquer que la consigne est d'envoyer un message à un élève non voisin,*
- *rappeler que le message envoyé passe par un des deux voisins,*
- *rappeler que si l'élève n'est pas le destinataire, il faut absolument qu'il fasse circuler le message.*

Exemples de messages : *l'expéditeur demande au destinataire son identité.*

- *dede à jojo : qui se cache réellement derrière le pseudo jojo ?*
- *jojo à zaza : qui se cache réellement derrière le pseudo zaza ?*
- *...*

Solution possible :

- *pour l'adressage : commencer par « de expéditeur (un pseudo) à destinataire (un pseudo non voisin) », la mention de l'expéditeur servant à obtenir la réponse,*
- *pour le routage : la consigne de transmettre un message arrivé d'un voisin à l'autre voisin.*

L'activité se déroule en deux temps.

Dans un premier temps, les élèves :

- appliquent les consignes et font un premier essai,
- s'aperçoivent qu'ils doivent faire circuler les messages qui ne leur sont pas destinés,
- réalisent qu'ils doivent mettre en place un protocole : comment rédiger le message (adressage) ? Comment doit-il circuler (routage) ?
- font plusieurs essais-erreurs,
- aboutissent à un premier protocole incluant adressage et routage.

Dans un second temps, les élèves :

- utilisent leur premier protocole,
- l'améliorent au besoin,
- choisissent leur protocole final.

Bilan de l'activité 2

Les élèves se rendent vite compte qu'ils doivent faire circuler des messages qui ne leur sont pas adressés, que cette circulation doit se faire avec des règles d'adressage et de routage et que l'application de ces règles (protocole) rend possibles les communications entre élèves non voisins.

Dans cette activité, les élèves ont utilisé un réseau en anneau dont les services fournis (au départ) limitent la communication à deux élèves voisins.

En mettant en place un protocole incluant adressage et routage, ils ont rendu possible la communication entre élèves non voisins.

Ce protocole a permis ainsi d'étendre les services proposés par le réseau en anneau.

Découvertes réalisées

La classe prend en note les acquis de la séance :

- lorsqu'on fait appel à une application telle que Tchat, celle-ci utilise des couches pour nous proposer un certain nombre de services,
- si les services fournis sont suffisants et répondent à nos besoins, on peut considérer cette application comme une couche applicative haute,
- si par contre nous avons besoin d'un service non fourni, il est possible de le créer. On dit dans ce cas qu'une couche supplémentaire a été ajoutée à notre application de départ.

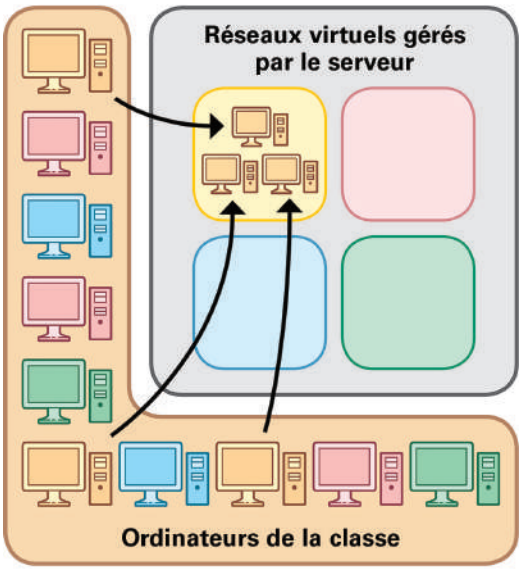
Exemples vus en séance

- dans le cas du **réseau en étoile**, il a été possible de développer une communication entre identités réelles (donc une couche supplémentaire) alors que seule la communication entre pseudos était possible,
- dans le cas du **réseau en anneau**, il a été possible de développer une communication entre utilisateurs non-voisins, alors que l'application ne permettait que des communications entre voisins. ■

Tchat (réseau en étoile ou en anneau)

Organisation de la classe

Contrairement aux activités du premier module, les activités de ce module ne nécessitent pas une organisation de la classe en îlots de tables. L'application Tchat est organisée en des espaces virtuels de 5 utilisateurs maximum, par défaut. Chaque élève (ou binôme) fait donc partie (via son ordinateur) d'un réseau de 5 élèves.



Comment lancer l'application Tchat ?

L'application est disponible en ligne (sur www.projetmerite.fr), mais peut être aussi installée en local si le réseau local interdit les communications par un protocole utilisée par l'application (WebSocket).

L'élève se connecte à l'application (via une adresse externe ou locale) en lançant le navigateur web de son poste informatique.

L'application attribue un pseudo à l'élève connecté.

Les élèves suivants se connectent jusqu'à la constitution du premier réseau virtuel de 5 élèves (les ordinateurs ne sont pas forcément adjacents).

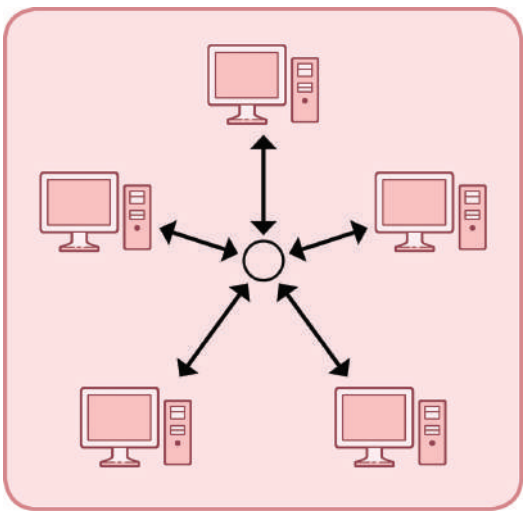
L'activité peut démarrer une fois tous les réseaux constitués (3, 4 ou 5 selon le nombre d'élèves dans la classe), donc une fois que tous les élèves de la classe sont connectés à l'application.

Fonctionnement de Tchat

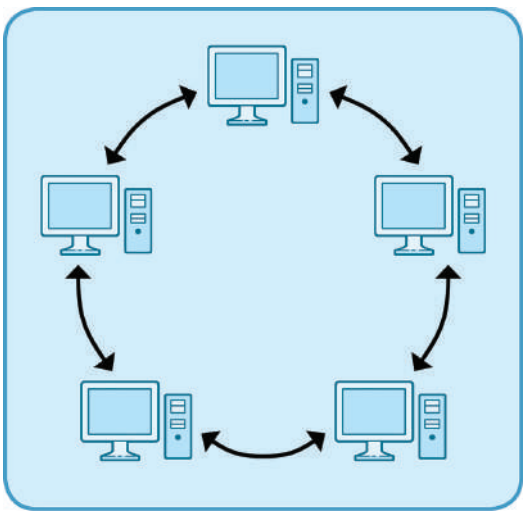
Il y a 5 utilisateurs en ligne, identifiés par des pseudos : ***dede***, ***fifi***, ***jojo***, ***lulu***, ***zaza***.
Les utilisateurs peuvent faire circuler, à l'intérieur de l'espace virtuel, des messages sous forme de texte de taille quelconque.

Il existe 2 sortes de réseaux pour la circulation des messages :

- **réseau en étoile** : permettant à un élève de s'adresser à tous les autres

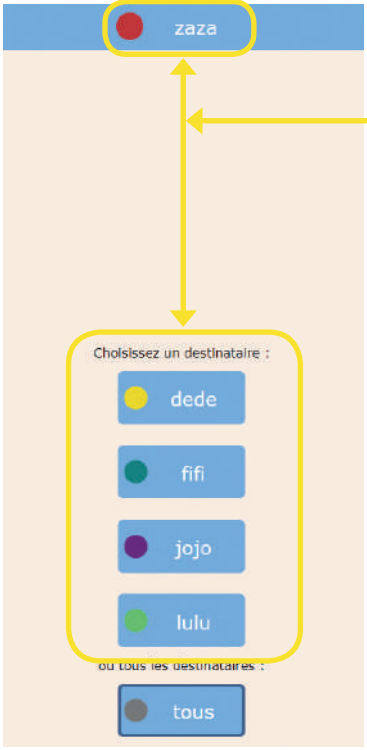


- **réseau en anneau** : ne permettant de s'adresser qu'aux 2 voisins



Tchat - le réseau en étoile

Au premier lancement de l'application, la fenêtre suivante (exemple : pseudo ***zaza***) apparaît :



POINT D'ATTENTION

*L'utilisateur **zaza** peut communiquer avec les 4 autres utilisateurs de son réseau.*

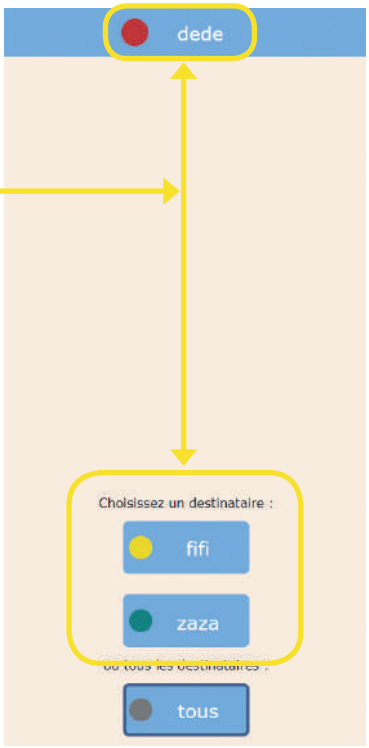
Au 2e lancement (par un autre utilisateur), on obtient un autre pseudo (par exemple ***jojo***). Ainsi de suite, jusqu'à avoir les 5 pseudos.

Un sixième lancement donnera un message d'erreur :

Dans ce cas, il faut se connecter à l'application avec une autre adresse. En effet, l'application est accessible par une suite d'adresses, par exemple, se terminant par « etoile0 », « etoile1 », etc. : il suffit donc d'incrémenter le numéro final pour obtenir une nouvelle adresse.

Tchat – le réseau en anneau

Au premier lancement de l'application, la fenêtre suivante (exemple : pseudo ***dede***) apparait :



POINT D'ATTENTION

*L'utilisateur **dede** ne peut communiquer qu'avec 2 voisins du réseau.*

Au 2e lancement (par un autre utilisateur), on obtient un autre pseudo (par exemple ***lulu***). Ainsi de suite, jusqu'à avoir les 5 pseudos.

Comme précisé plus haut, un sixième lancement donnera un message d'erreur :

Dans ce cas, comme précédemment, il faut se connecter à l'application avec une autre adresse.

SÉANCE **2**

Échanger des messages numériques

Objectifs

Utiliser un réseau mixte : étoile et anneau.
Échanger des messages en utilisant une nouvelle application.
Rédiger ces messages en binaire.
Réinvestir la notion d'adressage et routage.
Établir un protocole pour l'adressage et le routage adapté à la situation et valider ce protocole de communication.

Matériel

Par élève ou par binôme :

- **1 ordinateur** nf connecté à Internet
- **application numérique** disponible via www.projetmerite.fr

nf Matériel non fourni

Déroulement pédagogique

1h15

Pour bien organiser la séance, il est nécessaire que l'enseignant consulte la **FICHE** Application (réseau mixte).

Immersion

L'enseignant rappelle aux élèves que l'informatique exploite le code binaire, qui n'utilise que le 0 et le 1.

Il interroge la classe sur les trames de 13 cases utilisées dans le module 1 :

Comment faisiez-vous pour rédiger votre message ?

Par des cases noircies ou laissées vides.

Quel lien peut-on faire avec les deux chiffres 0 et 1 ?

Les cases blanches valent 0 et les cases noircies valent 1 (l'inverse aurait été possible).

Points de passage

L'enseignant organise la classe en consultant la fiche **FICHE** Application (réseau mixte).

Chaque poste informatique peut être occupé par un seul élève, mais il est tout à fait envisageable d'y placer un binôme d'élèves (considéré comme un seul et unique utilisateur).

Les messages circulent dans un réseau mixte qui relie en anneau des sous-réseaux en étoile appelés domaines. Les élèves sont identifiés par un nom : ***utilisateur@domaine*** (voir **FICHE** Application (réseau mixte)). La communication se fait d'un utilisateur d'un domaine à tous les utilisateurs d'un des deux domaines voisins. Le but de l'activité est qu'un utilisateur puisse envoyer son message à un autre utilisateur appartenant à un domaine non voisin. Les messages sont cette fois-ci numériques et non textuels. L'activité est l'analogue numérique de celle du module 1 dédiée à l'adressage et au routage : les îlots sont les domaines et les trames en papier les messages informatiques codés en binaire.

La **FICHE** Codage en base binaire présente la traduction du décimal au binaire.

L'enseignant annonce l'objectif à la classe :

Vous devez obtenir un service qui permet à deux utilisateurs n'appartenant pas à des domaines voisins, de s'échanger des messages. En d'autres termes, un service de communication entre deux utilisateurs distants.

Pour l'instant, les services fournis par le réseau sont les suivants :

- diffusion du message d'un utilisateur à un sous-réseau (domaine) voisin,
- verrouillage et déverrouillage d'un message pour réaliser son traitement, en excluant les autres utilisateurs du domaine,
- interprétation d'un message (pour déterminer le contenu),
- transmission d'un message à un domaine voisin.

Objectif : établir un protocole d'adressage et de routage qui permet à chaque utilisateur d'interpréter correctement son message, c'est-à-dire extraire l'information utile du message reçu. Une fois l'activité lancée, tous les élèves se connectent : chaque utilisateur prend connaissance de son identité, du message à envoyer, et de l'identité du destinataire.

Les élèves découvrent :

- que le contenu du message est un nombre binaire composé de 7 chiffres : 0 ou 1,
- que le message est composé de 13 chiffres binaires (0 et 1), et qu'il doit contenir le nombre binaire et l'identité du destinataire,
- qu'ils doivent par conséquent établir un protocole d'adressage et de routage, compris et utilisé par tous,
- que le message transite forcément par un des deux domaines voisins.

Ce travail de recherche de protocole se fait avec l'aide de l'enseignant.
Différentes solutions peuvent émerger, dont celle donnée en exemple.
Pour l'adressage, l'ordre des informations peut évidemment varier.
Pour le routage, si la carte du réseau n'est pas préalablement faite, la solution donnée s'impose : l'alternative vue dand le module 1, un sens de rotation horaire ou anti-horaire, n'a pas de sens dans le réseau virtuel.

Bilan de l'activité : les élèves s'aperçoivent de la difficulté d'établir une règle qui soit commune à tous, de la difficulté de l'appliquer correctement et de leur capacité à obtenir, au final, un protocole correct et efficace.

EXEMPLE DE SOLUTION

Opter pour le format de message suivant :
identité suivie du mot binaire

On sait que l'identité est :
utilisateur@domaine

Réserver :
- 3 cases pour l'utilisateur
- 3 cases pour le domaine
- 7 cases pour le nombre binaire
On arrive bien à 13.

Routage : *un message venant d'un domaine et qui n'est pas arrivé à destination doit être transmis à l'autre domaine.*

Découvertes réalisées

L'enseignant rappelle aux élèves les différents acquis de la séance :

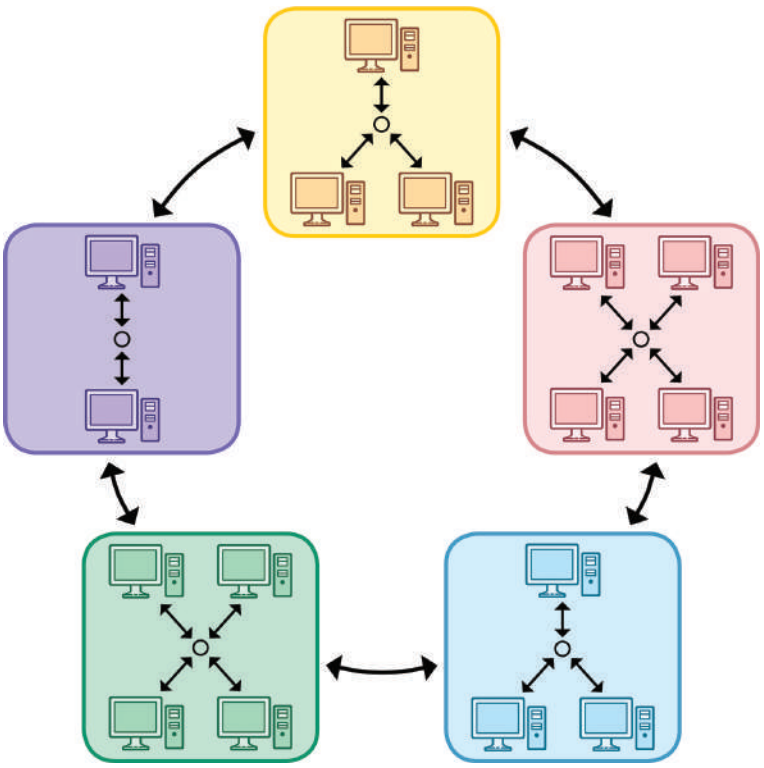
- ils ont utilisé pour la première fois un réseau mixte anneau-étoile,
- ils ont pu faire le lien avec le module 1, à travers l'utilisation d'une trame de 13 chiffres,
- ils ont réinvesti les notions d'adressage et de routage, dans un contexte purement informatique et compris l'importance, dans une communication informatique, d'associer à chaque action une commande dédiée (exemple de la commande « déverrouiller »),
- ils ont établi un protocole d'adressage (comment remplir les 13 cases de la trame) et de routage (quel domaine voisin choisir pour envoyer le message),
- ils ont de nouveau été confrontés à un défi dont le but est de développer un nouveau service non fourni par l'application utilisée,
- ils ont échangé des messages codés en binaire. ■

Application (réseau mixte)

L'application

Dans cette activité, les élèves communiquent en utilisant un réseau mixte reliant en anneau plusieurs sous-réseaux (de 4 à 6 en général) en étoile, appelés domaines : chaque domaine possède de 2 à 5 utilisateurs.

Exemple de réseau :



Comment lancer l'application ?

L'application est disponible en ligne mais elle peut être aussi installée localement : l'installation locale peut être nécessaire si le réseau local interdit les communications par un protocole utilisé par l'application (WebSocket). Pour plus d'informations, consulter www.projetmerite.fr.

Comment circulent les messages ?

Chaque utilisateur d'un domaine peut envoyer un message à un domaine voisin, dans le réseau en anneau.

Une fois arrivé au domaine destinataire, le message est diffusé à tous les utilisateurs du domaine, un sous-réseau en étoile.

L'identité des pseudos et des domaines est exprimée par des nombres binaires.
Les messages qui circulent sont sous la forme de trames binaires de taille fixe (une dizaine de chiffres).

Déroulement

Dans l'exemple ci-dessous, le réseau est organisé de la façon suivante :

- il y a 5 domaines : [0] ; [1] ; [1,0] ; [1,1] ; [1,0,0]
- chaque domaine comprend 3 (mêmes) utilisateurs : [0] ; [1] ; [1,0]
- un utilisateur est identifié de la manière suivante : utilisateur@domaine

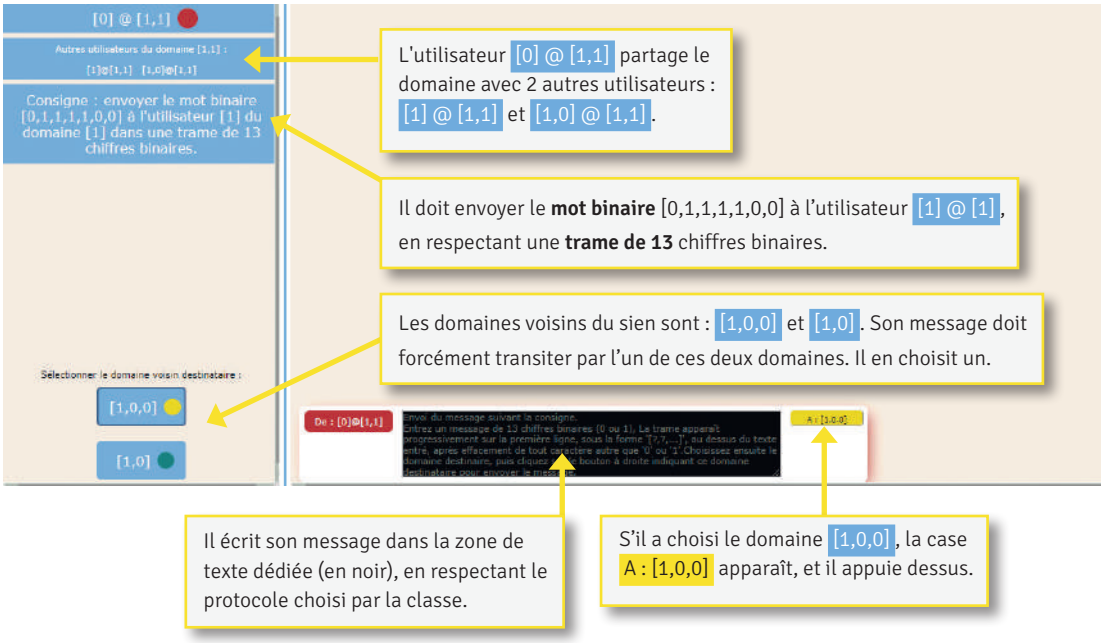
par exemple : [1,0]@ [0] ; [0]@ [1,1] ; *etc.*

POINT D'ATTENTION

Les nombres identifiant les domaines et les pseudos omettent les 0 inutiles à gauche. Ils sont donc égaux aux nombres suivants : [0,0,0] ; [0,0,1] ; [0,1,0] ; [0,1,1] ; [1,0,0], comme le montre la **FICHE** Codage en base binaire .

Cette omission est volontaire : c'est aux élèves de convenir que ces nombres occupent une taille fixe de 3 chiffres dans la trame. C'est une des difficultés à surmonter pour établir un protocole correct.

1 **Connexion -** Le premier utilisateur qui se connecte obtient la page web suivante (cela peut varier selon les utilisations, mais la logique reste la même) :



Les identités ***utilisateur@domaine*** sont attribuées au fur et à mesure des connexions.
Lorsque le nombre maximal de connexions est atteint, on obtient le message suivant :

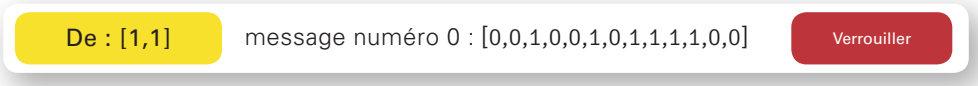
Fin de l'application après l'erreur suivante :
[14:22:45, le 03/02/2020 : Tchat - Réseau complet ! Il est impossible de se connecter : le réseau est complet.]

Dans ce cas, il faut se connecter à l'application avec une autre adresse. En effet, l'application est accessible par une suite d'adresses, se terminant, par exemple, par « distribution0 », « distribution1 », etc. : il suffit donc d'incrémenter le numéro final pour obtenir une nouvelle adresse.

2 **Entrée d'un message -** Lorsque l'élève entre son message, il peut le compléter par des espaces ou des caractères : seuls les 0 et les 1 sont finalement retenus. La suite de 0 et 1 retenue est écrite au-dessus du texte en train d'être tapé. Il est ainsi possible d'entrer « pour 001 @ 001 : 01 111 00 », pour obtenir la trame [0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0]. Le nombre de chiffres qu'il reste à écrire est aussi indiqué, tout comme le nombre de chiffres en trop en cas de dépassement.

2 Échanger des messages numériques

3 **Communication -** L'utilisateur a finalement choisi le domaine [1,0]. Le message envoyé est reçu par les trois utilisateurs du domaine [1,0]. L'image ci-dessous montre le message reçu par l'utilisateur [0]@[1,0] (les deux autres utilisateurs - [1]@[1,0] et [1,0]@[1,0] - ont le même type de fenêtre) :



4 **Traitement -** Un des trois utilisateurs décide de traiter le message.
Pour cela il doit appuyer sur la touche ***Verrouiller***. Il obtient la fenêtre suivante :

POINT D'ATTENTION

*Le fait d'appuyer sur la touche **Verrouiller**, permet à l'utilisateur de signaler aux deux autres que c'est lui qui va traiter le message. Si on fait le parallèle avec la communication papier du module 1, le traitement d'un message par un des utilisateurs de l'îlot était directement visible par les autres. C'est là une différence majeure entre la communication papier et la communication numérique. Les ressources matérielles ne sont pas partageables, alors que les ressources informatiques le sont. Pour interdire le partage, il est nécessaire de verrouiller les ressources informatiques, par des contrôles à l'intérieur des programmes.*

L'utilisateur a 3 possibilités :

- **Interpréter :** si le message lui est adressé,
- **Transmettre :** si le message est destiné à un autre domaine,
- **Déverrouiller :** si le message est pour un utilisateur de son domaine.

5 L'utilisateur a choisi de transmettre le message au domaine [1]. L'utilisateur [1]@[1], le reçoit et doit l'interpréter, c'est-à-dire extraire le mot binaire qui lui a été adressé. Si l'interprétation est correcte, voici la page qui s'affiche :

Sinon, c'est une notification « Perdu par l'utilisateur » qui apparaît sur l'écran.

Codage en base binaire

Rappels

2^x signifie : 2 à la puissance x

$2^0 = 1$; $2^1 = 2$; $2^2 = 4$

Binaire : utilise les deux chiffres 0 et 1 (base 2)

Bit : chiffre en binaire, qui peut prendre 2 valeurs : 0 ou 1

Astuce pour calculer de tête :

$2^{10} = 1024 \approx 1000 = 10^3$

Exemple :
$2^{32} = 2^{(2 + 10*3)} = 2^2 * 2^{(10*3)} = 4*(2^{10})^3$
$= 4*1024^3 \approx 4*1000^3 = 4*(10^3)^3 = 4*10^9$

Cas d'un codage sur trois bits

Les valeurs possibles de chaque bit sont :

- **1er bit :** (0 ou 1) x 2^0 → si on a 0 dans le bit, alors la valeur est : 0 x 2^0 = 0
  → si on a 1 dans le bit, alors la valeur est : 1 x 2^0 = 1
- **2e bit :** (0 ou 1) x 2^1 → si on a 0 dans le bit, alors la valeur est : 0 x 2^1 = 0
  → si on a 1 dans le bit, alors la valeur est : 1 x 2^1 = 2
- **3e bit :** (0 ou 1) x 2^2 → si on a 0 dans le bit, alors la valeur est : 0 x 2^2 = 0
  → si on a 1 dans le bit, alors la valeur est : 1 x 2^2 = 4

Exemples :

Le chiffre 0 s'écrit : 000 → 0 x 2^2 + 0 x 2^1 + 0 x 2^0 = 0

Le chiffre 1 s'écrit : 001 → 0 x 2^2 + 0 x 2^1 + 1 x 2^0 = 1

Le chiffre 2 s'écrit : 010 → 0 x 2^2 + 1 x 2^1 + 0 x 2^0 = 2

…

Le chiffre 7 s'écrit : 111 → 1 x 2^2 + 1 x 2^1 + 1 x 2^0 = 7

7 est le chiffre maximal qu'on peut coder avec 3 bits : $2^3 - 1$

Chiffre en décimal	Codage binaire sur 3 bits
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

***Remarque** : Si l'on souhaite coder le chiffre 8 (et les suivants), il faudrait passer à 4 bits.*

SÉANCE 3

Sécuriser les messages de l'application Tchat

Objectifs

Réfléchir à une manière de chiffrer les messages.
Définir un algorithme de chiffrement.
Échanger des messages chiffrés en utilisant l'application Tchat.

Matériel

Par élève ou par binôme :

- **1 ordinateur** nf connecté à Internet
- **application Tchat** disponible via www.projetmerite.fr

nf Matériel non fourni

Déroulement pédagogique

1h

Immersion

L'enseignant introduit la séance en interrogeant les élèves :

Peut-on envoyer un message confidentiel en utilisant un réseau qui n'est pas sûr ?

Réponse attendue : en chiffrant le message à l'expédition et en le déchiffrant à la destination.

Quel algorithme de chiffrement choisir ?

Les réponses possibles sont variées :

PREMIER CAS : LE MESSAGE EST TEXTUEL

Il est possible de réaliser une substitution des lettres, par exemple en les décalant. Pour déchiffrer, il suffit de les recaler. Il est aussi possible de réaliser une permutation des lettres, en modifiant leur ordre. Pour déchiffrer, il sufit de remettre en ordre.

SECOND CAS : LE MESSAGE EST NUMÉRIQUE

Les techniques applicables aux textes s'appliquent toujours. Mais il existe aussi des techniques fondées sur des calculs. Comme le message forme un nombre, pour chiffrer, il suffit d'appliquer une fonction numérique et, pour déchiffrer, appliquer la fonction inverse. Par exemple : ajouter 7 pour chiffrer, retirer 7 pour déchiffrer, le nombre 7 étant la clé de chiffrement. De manière générale, une clé de chiffrement est le paramètre d'une famille de fonctions de chiffrement et de déchiffrement.

Points de passage

L'enseignant fournit toutes les explications nécessaires pour que les élèves puissent se connecter à l'application Tchat, avec un réseau en anneau (voir la première séance pour les détails). Chaque réseau contient 5 utilisateurs de pseudos : *dede*, *fifi*, *jojo*, *lulu* et *zaza*. Il est organisé en anneau : un utilisateur ne peut communiquer qu'avec ses deux voisins.

L'enseignant annonce l'objectif à la classe :

Vous devez développer un service qui permet à deux utilisateurs non voisins de s'échanger des messages confidentiellement, en les chiffrant et en les déchiffrant.

Pour simplifier, on peut se limiter à un contenu numérique des messages : par exemple des nombres entiers compris entre 0 et 999.

Enfin, une contrainte est imposée : il est interdit de communiquer autrement que par l'envoi de messages en utilisant l'application Tchat. Une exception cependant : il est possible de partager de vive voix une information avec le destinataire, qui aura été identifié à partir de son pseudo.

Initialement, le réseau fournit le service suivant :

- communication d'un utilisateur identifié par son pseudo aux deux utilisateurs voisins, identifiés aussi par leur pseudo.

Pour parvenir à l'objectif, les élèves doivent résoudre une succession de problèmes :

- l'adressage et le routage dans un réseau en anneau (activité 2 - séance 1),
- la résolution des pseudos, c'est-à-dire la détermination de l'identité réelle derrière un pseudo (une adaptation à un réseau en anneau de l'activité 1 - séance 1),
- le partage d'une clé entre l'expéditeur et le destinataire, lors d'une communication orale, après la résolution des pseudos,
- la conception d'une famille de fonctions de chiffrement et de fonctions de déchiffrement, inverses des précédentes, familles paramétrées par la clé.

Les élèves découvrent :

- que le protocole de l'activité 2 (séance 1) pour l'adressage et le routage dans un réseau en anneau peut être repris,
- que le protocole de résolution des pseudos peut être adapté à un réseau en anneau,
- qu'il existe de nombreuses familles de fonctions paramétrées par des clés pour le chiffrement et le déchiffrement.

Un exemple de protocole pour la résolution des pseudos est donné, ainsi que quelques familles pour le chiffrement et le déchiffrement.

Les élèves élaborent ainsi leur protocole, avec l'aide de l'enseignant et l'activité peut être lancée dans chaque anneau.

Les élèves commencent par déterminer les identités réelles, en utilisant le protocole de routage et celui de résolution des pseudos.

EXEMPLES DE PROTOCOLES

Résolution de pseudos

- Chaque élève envoie un message contenant une association de son pseudo avec son prénom.

- Chaque élève transmet un message reçu incomplet après lui avoir ajouté l'association pseudo-prénom.

- Chaque élève conserve un message complet, c'est-à-dire contenant 5 associations, une par pseudo. Il donne la table de correspondance permettant de résoudre les pseudos en des identités réelles.

Chiffrement - Déchiffrement

Les fonctions cryptographiques viennent en couple : une fonction de chiffrement et son inverse, la fonction de déchiffrement associée. Lorsqu'on définit un protocole cryptographique, on utilise une classe de tels couples, paramétrée par une clé.

Voici quelques classes possibles pour notre cas, le chiffrement et le déchiffrement d'un nombre entier entre 0 et 999 :

***1.** On décale pour chiffrer, on recale pour déchiffrer :*

- le chiffre des centaines de 3 pas, et inversement,
- le chiffre des dizaines de 4 pas, et inversement,
- le chiffre des unités de 5 pas, et inversement.

***2.** On ajoute la clé (un nombre entier) pour chiffrer, on la retire pour déchiffrer. Les calculs se font modulo 1000 pour éviter le dépassement de 1000 (voir* **FICHE** Notions sur le chiffrement *).*

***3.** On remplace chaque chiffre par un autre pour chiffrer, on fait le remplacement inverse pour déchiffrer. Par exemple, on remplace 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 par 3, 1, 4, 5, 9, 2, 7, 0, 8, 6 respectivement.*

***4.** On met dans le désordre les chiffres pour chiffrer, on les remet en ordre pour déchiffrer. Par exemple, le chiffre de tête est mis en fin pour chiffrer, et inversement pour déchiffrer.*

Chaque expéditeur partage de vive voix une clé secrète avec le destinataire, déterminée ainsi :

- pour *dede* : destinataire *jojo*,
- pour *fifi* : destinataire *lulu*,
- pour *jojo* : destinataire *zaza*,
- pour *lulu* : destinataire *dede*,
- pour *zaza* : destinataire *fifi*.

L'enseignant attribue 5 nombres entre 0 et 999 à *dede*, *fifi*, *jojo*, *lulu* et *zaza* identifiés respectivement par D, F, J, L et Z.

Chaque expéditeur envoie au destinataire le nombre qui lui a été attribué après l'avoir chiffré en utilisant la clé partagée.

Lorsque le message parvient au destinataire après un routage, celui-ci déchiffre le nombre.

L'enseignant vérifie que le déchiffrement a donné :

- pour *dede* : L,
- pour *fifi* : Z,
- pour *jojo* : D,
- pour *lulu* : F,
- pour *zaza* : J.

L'enseignant interroge la classe :

Peut-on décrypter un message (le déchiffrer sans connaître la clé) ?

Les élèves analysent les algorithmes de chiffrement proposés et essaient d'évaluer leur robustesse. Pour ce faire, l'enseignant peut les aiguiller en posant deux questions supplémentaires :

À partir d'un texte chiffré, peut-on obtenir des informations sur le texte original ?
À partir d'exemples de chiffrement, peut-on obtenir des informations sur la clé ?

Une cryptanalyse sommaire des algorithmes donnés comme possibles solutions est présentée dans la **FICHE** Notions sur le chiffrement (pour les enseignants qui souhaiteraient aller plus loin).

Bilan de l'activité : les élèves doivent combiner plusieurs protocoles pour réaliser une communication confidentielle de messages (résolution des pseudos, adressage et routage, chiffrement).

Découvertes réalisées

L'enseignant rappelle aux élèves les différents acquis de la séance :

- un protocole pour l'échange de messages confidentiels,
- des techniques de chiffrement symétrique, requérant le partage d'une clé secrète, privée. ■

POUR ALLER PLUS LOIN...

Chiffrement asymétrique

Le chiffrement symétrique a pour inconvénient de supposer le partage d'une clé privée, secrète, entre l'expéditeur et le destinataire. En se passant de cette hypothèse, le chiffrement asymétrique révolutionne la cryptographie. Il suffit désormais de partager une clé publique. Dans la **FICHE** Chiffrement asymétrique*, est présentée la première solution de chiffrement asymétrique, donnée par Diffie et Hellman dans leur célèbre article de 1976 « New directions in cryptography ».*

Impact environnemental

Dans le cadre des apprentissages concernant l'analyse de l'impact environnemental d'un objet et de ses constituants, l'enseignant peut faire réfléchir et travailler les élèves sur l'aspect énergivore (consommation d'électricité) de l'outil informatique, et sa conséquence directe : utilisation importante des énergies fossiles (pétrole, charbon, gaz naturel) très polluantes et génératrices de dioxyde de carbone (CO_2) dans l'atmosphère, responsable en partie du réchauffement climatique. On parle dans ce cas de l'empreinte carbone du numérique.

L'enseignant fait réfléchir les élèves sur le lien entre l'envoi d'un message avec l'application Tchat et la pollution de l'environnement.

Pour aider les élèves, l'enseignant peut réorienter le débat en les faisant travailler sur le coût d'un SMS en termes d'émission de gaz à effet de serre. Il peut les accompagner dans leur investigation documentaire et s'appuyer sur quelques éléments :

- *le SMS a une longueur maximale de 140 octets, soit 1120 bit,*
- *données d'un opérateur de téléphonie : 2600 GWh ont été consommés pour le transport de 60000 Térabits de données, ce qui correspondant à 53000 milliards de sms,*
- *l'envoi d'un sms consommerait donc 0,05 Wh (50 mWh, consommation d'une ampoule de 12 W pendant 15 secondes), ce qui correspond à l'émission de* ***2,15 mg*** *équivalent CO_2 par message.*

Les élèves retiennent que l'envoi d'un SMS a un coup énergétique et un impact écologique puisqu'il génère du CO_2 qui est un gaz à effet de serre. Même si la quantité produite par SMS est très petite, la multiplication des SMS peut augmenter cette quantité jusqu'à devenir non négligeable et avec effet direct sur l'environnement.

Notions sur le chiffrement

ARITHMÉTIQUE MODULAIRE

Très souvent, en informatique, et notamment en cryptographie, on recourt à l'arithmétique modulaire : les calculs se font modulo un certain entier. Cette particularité vient de la taille fixée des entiers, représentés en utilisant un nombre fixe de chiffres. Si la taille est p, on peut représenter au total 10^p nombre décimaux, de 0 à 10^{p-1}, et 2^p nombres binaires, de 0 à 2^{p-1}.

Exemple, avec p = 3 :

- *base 10 : 000, 001, ..., 998, 999 (au total : 1000 nombres)*
- *base 2 : 000, 001, ..., 110, 111 (au total : 8 nombres)*

On note M la borne supérieure de l'intervalle, 1000 en base 10 comme en base 2, soit les nombres 1000 et 8 (en base 10). Lorsqu'on fait des calculs et qu'on dépasse la valeur maximale M, se pose un problème : comment représenter le résultat ? La solution la plus simple est de revenir à 0. Autrement dit, on prend pour résultat le reste de la division euclidienne par M du résultat dépassant M.

Notation pour le reste de la division euclidienne par M : n mod M (n modulo M)
n mod M = r si n = M∗q + r, avec $0 \leq r < M$

Exemple, pour p = 3, M = 1000 (base 10) :

- *1002 mod 1000 = 2 car 1002 = 1000 ∗ 1 + 2*
- *4985 mod 1000 = 985 car 4985 = 1000 ∗ 4 + 985*

Les calculs modulo ont toutes les bonnes propriétés arithmétiques et se font naturellement.

Voici un calcul réalisé de deux manières, montrant que le reste final peut être calculé à partir de restes intermédiaires :

- ((997 + 5) ∗ (995 + 6)) mod 1000 = (1002 ∗ 1001) mod 1000 = 1003002 mod 1000 = 2
- ((997 + 5) ∗ (995 + 6)) mod 1000 = ((1002 mod 1000) * (1001 mod 1000)) mod 1000 = (2 ∗ 1) mod 1000 = 2

En cryptographie, on utilise plutôt un nombre premier comme module : en effet, l'ensemble des entiers modulo un nombre premier forme un corps, ce qui peut être utile dans les calculs.

CRYPTANALYSE

La cryptanalyse, ou l'art de décrypter, est difficile à maîtriser et requiert des efforts importants pour obtenir le moindre succès. Un « jeu » s'instaure entre les chiffreurs et les décrypteurs :

- le chiffreur conçoit un algorithme,
- le décrypteur trouve un moyen d'attaquer,
- le chiffreur améliore son algorithme contre cette attaque,
- et ainsi de suite.

La robustesse d'un algorithme de chiffrement peut s'évaluer suivant différents critères.
En voici deux significatifs :

- À partir d'un texte chiffré, peut-on obtenir des informations sur le texte original ?
  Parmi les quatre techniques proposées, seules deux ne donnent aucune information :
  - (1) **décalage** et (2) **addition** : aucune information,
  - (3) **substitution** : les répétitions de chiffres sont préservées,
  - (4) **permutation** : l'ensemble des chiffres est préservé.
- À partir d'exemples de chiffrement, peut-on déduire la clé ? Pour les quatre techniques proposées, il suffit d'un exemple pour déterminer la clé, à condition évidemment de connaître l'algorithme utilisé.

GLOSSAIRE

Module

PRÉSENTATION FORMELLE DES ALGORITHMES DE CHIFFREMENT

Une formalisation mathématique des algorithmes est possible et évidemment utile lorsqu'on programme les calculs : elle ne doit cependant pas faire oublier l'intuition derrière ces calculs.
Si un nombre a pour centaines x, dizaines y et unités z, il est égal à x∗100 + y∗10 + z, et est aussi noté x.y.z, pour mettre en avant les positions : x en position 2, y en positon 1 et z en position 0.

*Par exemple : 789, noté aussi 7.8.9, est égal à 7*100 + 8*10 + 9*

Possibilités de chiffrement et de déchiffrement

1. Le **décalage** de chiffres modulo 10 (de c pour les centaines, d pour les dizaines, u pour les unités, avec c, d et u entre 0 et 9) et le décalage inverse, avec la clé *c.d.u*.

- **Chiffrement par décalage :** x.y.z → ((x + c) mod 10).((y + d) mod 10).((z + u) mod 10)

  Exemple (clé k = 3.4.5) : 7.8.9 → ((7 + 3) mod 10).((8 + 4) mod 10).((9 + 5) mod 10) = 0.2.4

- **Déchiffrement par décalage inverse :** x.y.z → ((x - c) mod 10).((y - d) mod 10).((z - u) mod 10)

  Exemple (clé k = 3.4.5) : 0.2.4 → ((0 - 3) mod 10).((2 - 4) mod 10).((4 - 5) mod 10) = 7.8.9

2. L'**addition** de k modulo 1000 et la soustraction de k modulo 1000 - clé : entier k.

- **Chiffrement par addition :** x → (x + k) mod 1000

  Exemple (clé k = 345) : 789 → (789 + 345) mod 1000 = 1134 mod 1000 = 134

- **Déchiffrement par soustraction :** x → (x - k) mod 1000

  Exemple (clé k = 345) : 134 → (134 - 345) mod 1000 = - 211 mod 1000 = 789

3. La **substitution** des chiffres (par une bijection S de {0, ..., 9} dans lui-même), la substitution inverse (notée S^{-1}), avec la clé : S(0). ... .S(9).

- **Chiffrement par substitution :** x.y.z → S(x).S(y).S(z)

  Exemple (clé k = 3.1.4.5.9.2.7.0.8.6) : 7.8.9 → 0.8.6

- **Déchiffrement par substitution inverse :** x.y.z → S^{-1} (x).S^{-1} (y).S^{-1} (z)

  Exemple (clé k = 3.1.4.5.9.2.7.0.8.6, substitution inverse 0 → 7, ..., 6 → 9, ...) : 0.8.6 → 7.8.9

4. La **permutation** des trois chiffres (positions : 2 → p2, 1 → p1, 0 → p0), la permutation inverse (p2 → 2, p1 → 1, p0 → 0), notée (2 → q2, 1 → q1, 0 → q0), avec la clé : p2.p1.p0.

- **Chiffrement par permutation :** x.y.z → $x*10^{p2} + y*10^{p1} + z*10^{p0}$

  Exemple (clé k = 0.2.1, décrivant la permutation (2 → 0, 1 → 2, 0 → 1)) :

  *7.8.9 → 7*1 + 8*100 + 9*10 = 8.9.7*

- **Déchiffrement par permutation inverse :** x.y.z → $x*10^{q2} + y*10^{q1} + z*10^{q0}$

  Exemple (clé k = 0.2.1, permutation inverse (2 → 1, 1 → 0, 0 → 2)) :

  *8.9.7 → 8*10 + 9*1 + 7*100 = 7.8.9*

Chiffrement asymétrique

Le chiffrement asymétrique suppose qu'une information est partagée entre l'expéditeur et le destinataire mais, contrairement au chiffrement symétrique, cette information n'a pas besoin d'être secrète.
Cette information sert à déterminer une clé secrète de chiffrement après un premier échange d'informations. Les modalités précises dépendent de l'algorithme. Est présenté ci-dessous l'algorithme de Diffie-Hellman, en montrant qu'il s'agit de l'analogue numérique du protocole décrit avec les tirelires cadenassées rappelé en gris entre guillemets.

Algorithme de Diffie-Hellman - Protocole d'échange de clé secrète

1. « L'expéditeur envoie un premier message au destinataire pour signifier son intention de communiquer. »

L'expéditeur envoie une clé qui peut être publique et un premier message chiffré :

- **clé publique :**
  - M (module, les calculs se faisant modulo M),
  - g (générateur entre 0 et M-1.
- **message chiffré :** le nombre entier g^a modulo M, où a est un secret choisi au hasard par l'expéditeur.

2. « En réponse, Le destinataire envoie à l'expéditeur sa tirelire verrouillée vide. »

En réponse, le destinataire envoie le nombre entier g^b modulo M, où b est un secret choisi au hasard par le destinataire.

3. « À réception de la tirelire, l'expéditeur met son message dans la tirelire grâce à l'ouverture, et renvoie la tirelire au destinataire. »

À réception de g^b modulo M, l'expéditeur calcule la clé $((g^b) \bmod M)^a \bmod M$ et chiffre son message en utilisant cette clé.

4. « À réception de sa tirelire, le destinataire le déverrouille et lit le message. »

À réception du message chiffré, le destinataire calcule la clé $((g^a) \bmod M)^b \bmod M$ et déchiffre le message en utilisant cette clé. C'est possible car $(g^a)^b = g^{(a*b)} = g^{(b*a)} = (g^b)^a$.

La robustesse de l'algorithme provient de l'impossibilité pour l'attaquant de déterminer a ou b, connaissant g^a modulo M et g^b modulo M. Il n'existe pas d'algorithme efficace permettant de calculer le logarithme discret : il suffit donc de choisir une valeur de M suffisamment grande pour empêcher pratiquement l'attaquant de déterminer a ou b. Comme pour le protocole des tirelires, l'attaque de l'intercepteur est possible. La même défense est envisageable : il suffit d'authentifier la première réponse du destinataire. En pratique, plutôt qu'un répertoire, ce sont des solutions d'authentification fondées sur des signatures cryptographiques qui sont utilisées. Comme nous n'avons pas traité le problème de l'authentification, nous n'entrons pas dans les détails.

Protocole de Diffie-Hellman étendu pour contrer l'attaque de l'intercepteur

Un préambule est ajouté au protocole.

0. « Chaque îlot reçoit un répertoire donnant pour tout îlot le numéro de sa tirelire. »

Chaque utilisateur reçoit un répertoire donnant une information permettant d'authentifier une signature.

Les étapes 2 et 3 du protocole sont modifiées.

2. « En réponse, Le destinataire envoie à l'expéditeur sa tirelire verrouillée vide. »

En réponse, le destinataire envoie le nombre entier g^b modulo M, où b est choisi au hasard par le destinataire, et signe le message.

3. « À réception de la tirelire, l'expéditeur vérifie son numéro dans le répertoire, met son message dans la tirelire grâce à l'ouverture, et renvoie la tirelire au destinataire. »

À réception du message signé contenant g^b modulo M, l'expéditeur vérifie la signature grâce à son répertoire, calcule la clé $((g^b) \bmod M)^a \bmod M$ et chiffre son message en utilisant cette clé.

Exemple (clé définie par M = 17 et g = 6 ; E = expéditeur ; D = destinataire) :

- *E → D : envoi de la clé (M = 17, g = 6) et de $6^5 \bmod 17$, soit 7*
- *D → E : envoi de $6^{11} \bmod 17$ soit 5*
- *E → D : envoi du message chiffré par E avec la clé $5^5 \bmod 17$ (soit 14) puis déchiffré par D avec la clé $7^{11} \bmod 17$ (soit 14) (en utilisant un chiffrement symétrique)*

Glossaire

Glossaire

Adressage

Opération par laquelle une adresse est ajoutée au contenu d'un message afin d'identifier le destinataire.
Il existe des normes pour les adresses, par exemple celle des URL pour les ressources du Web.

Application

Programme qui réalise une certaine fonctionnalité en utilisant un environnement (système d'exploitation, bibliothèque de sous-programmes) - le programme réalise donc une application de l'environnement pour parvenir à une fin particulière, la fonctionnalité attendue.

Application Web

Application utilisant la technologie du Web (protocole http, serveur web, navigateur).

L'application utilisée au cours de la progression (Tchat) présente un type d'architecture dite client-serveur, dans laquelle le programme est décomposé en deux parties :

- un serveur, qui répond aux clients,
- des clients, qui font des requêtes au serveur.

Les termes « serveur » et « client » désignent des rôles qui s'appliquent aussi bien aux machines qu'aux programmes. Ainsi, un serveur peut être une machine serveur ou un programme serveur : le contexte permet de distinguer le sens.

Précautions pour les applications web côté client :

- pour lancer une application web, on utilise son navigateur : on rentre l'adresse du programme serveur dans la barre des adresses,
- l'application côté client se ferme si on ferme l'onglet ou si on recharge la page.

Boutisme

Convention de lecture. En informatique, les mots, composés d'octets (ensemble de 8 bits), sont lus - tout comme pour les langues - soit de droite à gauche, soit de gauche à droite. Le boutisme définit le sens de la lecture.

Charge utile

La partie de la trame qui reste (réellement) exploitable pour écrire le texte du message à envoyer.

Chiffrement

Procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

Clé de chiffrement

Paramètre permettant de chiffrer et déchiffrer. Les fonctions de chiffrement et de déchiffrement sont paramétrées par des clés. Les clés peuvent être secrètes ou non.

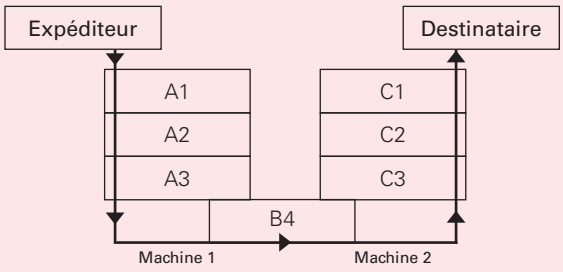
Couche (protocolaire)

Elément d'une pile protocolaire fournissant un service à la partie haute de la pile et le réalisant en utilisant les services fournis par la partie basse de la pile. Les protocoles de communication s'organisent en piles protocolaires formées de différentes couches.

Une architecture en couches a plusieurs avantages :

- la spécialisation, puisque chaque couche réalise une fonctionnalité bien identifiée,
- l'abstraction, puisque de l'extérieur, seul le service fourni importe,
- l'interchangeabilité, puisqu'une couche peut être remplacée par une autre fournissant le même service.

Le protocole établi pour la communication dans le module 1 met en évidence quatre couches, que nous détaillons. Le principe est que chaque couche, à l'exception de la plus basse, fournit des services en appelant des services fournis par une couche de niveau inférieur.



A1 - Couche applicative (émission)

- Entrée : trois nombres décimaux désignant le pays, le pseudo et le message
- Conversion des nombres décimaux en nombres binaires
- Appel de la couche de transport (émission) en passant trois nombres binaires pour le pays, le pseudo et le message

A2 - Couche de transport (émission)

- Entrée : trois nombres binaires, pour le pays, le pseudo et le message
- Décomposition du message en paquets
- Pour chaque paquet, appel de la couche d'adressage en passant quatre nombres binaires pour le pays, le pseudo, le paquet et ses informations administratives.

A3 - Couche d'adressage (émission)

- Entrée : quatre nombres binaires pour le pays, le pseudo, le paquet et ses informations administratives
- Écriture de la trame suivant les règles du protocole
- Appel de la couche de routage (transmission) en passant la trame

B4 - Couche de routage (transmission)

- Entrée : une trame
- Routage de la trame en utilisant le pays extrait de la trame et la table de routage
- Appel de la couche d'adressage (réception) si le message est arrivé à destination ou de la couche de routage (transmission) de l'îlot voisin

C3 - Couche d'adressage (réception)

- Entrée : une trame
- Interprétation de la trame suivant les règles du protocole
- Appel de la couche de transport (réception) en passant quatre nombres binaires pour le pays, le pseudo, le paquet et ses informations administratives

C2 - Couche de transport (réception)

- Entrée : quatre nombres binaires pour le pays, le pseudo, le paquet et ses informations administratives
- Composition de plusieurs paquets en un message
- Appel de la couche applicative (réception) en passant trois nombres binaires, pour le pays, le pseudo et le message

C1 - Couche applicative (réception)

- Entrée : trois nombres binaires, pour le pays, le pseudo et le message
- Conversion des nombres binaires en nombres décimaux
- Résultat : trois nombres décimaux désignant le pays, le pseudo et le message

Cryptographie

Une des disciplines de la cryptologie. Elle s'attache à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés.

Cryptologie

Étymologiquement, la science du secret.
Cette science englobe la cryptographie – l'écriture secrète, la cryptanalyse, l'analyse de cette dernière, et la stéganographie, l'art de la dissimulation.

Émetteur

Acteur initiant une communication. Dans les domaines de la linguistique et de la communication, un émetteur est une personne qui crée un message et le transmet ensuite à un récepteur ou destinataire par un canal, le médium.

Médium

Moyen par lequel est transmise l'information.

Module

Grandeur caractérisant l'opération modulo. Par exemple : dans l'opération 7,5 mod 2 = 1,5, le module est 2.

Paquet

Unité de transmission de la couche réseau. Les messages qui sont transmis sur le réseau sont découpés en paquets transmis séparément.

Protocole

Ensemble de règles qui régissent la communication, dans de nombreux domaines, de la diplomatie à l'informatique. Pour la communication entre machines, ces règles s'organisent en couches - voir *Couche (protocolaire)*.

Récepteur

Acteur terminant une communication. Dans le domaine de la linguistique et de la communication, le récepteur, receveur ou destinataire est la personne ou l'entité qui reçoit un message - souvent formé de signes linguistiques - envoyé par un émetteur par le canal d'un média, et tente de le comprendre. Il peut être humain, informatique, animal... indépendamment de la nature de l'émetteur.

Résolution des noms

Procédé par lequel un nom identifiant une entité est traduit en une valeur directement associée à cette entité, comme sa référence ou son adresse. La résolution des noms intervient en programmation, où le nom d'une variable est résolu en une adresse en mémoire, mais aussi en communication réseau, où un nom logique est résolu en une adresse physique. Par exemple, une adresse Web est un nom logique résolu en une adresse IP d'une machine.

Routage

Procédé permettant de déterminer une route. En informatique et télécommunications, il s'agit d'une opération consistant à diriger des données au sein d'un réseau.

Table de routage

Table associant à toute destination finale la prochaine destination. Elle permet de déterminer le routage de proche en proche. Sur le réseau Internet, les routeurs disposent de tables de routage maintenues à jour en permanence.

Traceroute

Programme utilitaire permettant de suivre le chemin qu'un paquet de données va prendre pour transiter de la machine locale à une autre machine connectée au réseau Internet.

Web

Système d'information mondial utilisant le réseau Internet et ses protocoles pour fournir des pages web, contenant des hypertextes - des textes liés entre eux. Ce système repose sur des applications client-serveur utilisant le protocole http.

- serveur web : serveur http,
- client web ou navigateur : client http permettant de visualiser les pages web et de naviguer entre elles.

Remerciements

Le projet MERITE est le fruit d'un travail collectif qui a rassemblé de nombreux acteurs de l'enseignement supérieur et de la recherche, de l'Éducation nationale et des partenaires institutionnels impliqués pour la promotion de la culture scientifique et technique.

Le Centre de Ressources en Pratiques Expérimentales d'IMT Atlantique, a coordonné l'ensemble du projet : Carl Rauch et Lotfi Lakehal-Ayat (coordination générale), Josiane Hamy (coordination pédagogique et éditoriale), Blanche Cahingt (matériel), et successivement Jean-Félix Picard, Caroline Thoraval, Audrey Guillermic (coordination administrative), successivement Clémentine Jung et Flavy Benoit (communication, diffusion), Arnaud Schmitt (rédactionnel et édition).

L'équipe de coordination adresse ses remerciements :

- aux auteurs du guide pédagogique : Hervé Grall, enseignant-chercheur, Département Automatique Productique Informatique IMT Atlantique ; Lotfi Lakehal-Ayat enseignant-chercheur Centre de Ressources en Pratiques Expérimentales IMT Atlantique, au contributeur Jean-Félix Picard, enseignant de Technologie, qui a participé à la rédaction de ce guide ;

- aux enseignants qui ont co-construit et/ou testé le guide à ses différentes étapes : Christophe Audren, Mickaël Cosnuau, Carole Guinel, Tony Marchand, Fabrice Moreau, Sébastien Müller, Laurent Pérol, et aux enseignants des formations de la Maison pour la science de Rennes ;

- aux acteurs de l'Éducation nationale qui ont contribué : Cristel Izac, IA-IPR Sciences et Techniques Industrielles ;

Philippe Briaud, formateur ; Omer Demiraslan, enseignant et formateur ; Marc Tavera et Philippe Thullier, conseillers pédagogiques départementaux, pour leur participation à la coordination pédagogique ;

- aux acteurs ayant participé à la conception et à la fabrication des mallettes : Sébastien Bluet, designer produit ; les entreprises Condi-Ouest, Cal'Concept, Pankarte PLV, et l'Étape Tournière Services ;

- au comité de pilotage composé de : Paul Friedel, directeur d'IMT Atlantique, président ; Anne Beauval, directrice déléguée d'IMT Atlantique ; Yves Bourdin, délégué académique de l'action éducative et pédagogique, Rectorat de Nantes ; Patrick Bourgeois, correspondant pour le groupe Assystem ; Patricia Carre, responsable du pôle Science et Société, Conseil Régional des Pays de la Loire ; Pierre Le Cloirec et Régis Gautier, successivement directeurs de l'École Nationale Supérieure de Chimie de Rennes ; Arnaud Godevin, directeur de l'École Supérieure du Bois ; David Jasmin, directeur de la Fondation La main à la pâte ; Pascal Jousset, chargé de programme FEDER ; Jean-Louis Kerouanton, vice-président de l'Université de Nantes ; Lionel Luquin, directeur des Formations d'IMT Atlantique ; Caroline Prevot, correspondante académique scientifique et technologique, Rectorat de Nantes ; Ana Poletto, responsable de la mission diffusion de la culture scientifique et technique, Université de Nantes ; Elena Popa, gestionnaire du service FEDER ; René Siret, directeur général de l'École Supérieure d'Agricultures d'Angers ; Pascal Leroux et Jean-François Tassin, successivement directeurs de l'École Nationale Supérieure d'Ingénieurs du Mans ; Sarah Turbeaux, cheffe de projet pôle sciences société, service recherche, Conseil Régional des Pays de la Loire.

Le consortium MERITE est composé de 7 établissements d'enseignement supérieur du Grand Ouest aux expertises scientifiques diverses : matériaux, énergie, environnement, chimie, alimentation, numérique et robotique, mesures et acoustique.

Crédits

Direction artistique : Nathalie Papeil ; **Photographie :** Jean-Charles Queffelec ; **Illustrations :** Marie Ducom ;

Autres crédits : p. 10-11 : *photographie* Lev Dolgachov / Adobe Stock ;

Modèles mains : Clémence et Jules Papeil.

Tous droits de reproduction et de diffusion réservés © MERITE
MERITE est une marque déposée à l'INPI.

Coordination : IMT Atlantique
Conception : MERITE

Édité en août 2020

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Imprimé par Icones www.icones.fr

Communication informatique : tout un protocole

Que se passe-t-il lorsqu'on envoie un mail ou un SMS ? Pour comprendre comment des ordinateurs, des smartphones ou des tablettes communiquent entre eux, mettons-nous à leur place.

Dans le premier module de cette mallette pédagogique, les élèves s'envoient des messages sur papier, mais pas n'importe comment ! À qui le message est-il destiné ? Dans quel sens l'information circule-t-elle ? Comment envoyer un message volumineux et comment le protéger ? Réalisées sans ordinateur et à l'aide de matériel très simple, ces 4 séances permettent de comprendre les notions informatiques d'adressage, de routage, de paquet et de sécurité.

Le second module s'intéresse à la communication via le réseau informatique. Sur ordinateur cette fois-ci, les élèves s'envoient des messages grâce à une application développée spécifiquement et réinvestissent les notions du premier module.

Cette mallette pédagogique a été conçue par IMT Atlantique

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

mallettes MERITE
itinéraires en sciences et techniques : expérimenter et comprendre

Conçues pour les enseignants du CM1 à la classe de 3e, les mallettes MERITE sont des ressources pédagogiques mêlant sciences et technologie, laissant une grande part à l'expérimentation des élèves. Apprendre en faisant par soi-même, investiguer, progresser par essai-erreur, réfléchir en groupe sur des questions concrètes avec du matériel approprié, s'entraîner à raisonner sur des faits et des observations, sont les principes au cœur de cette collection. Chaque mallette MERITE est composée d'un guide pour l'enseignant détaillant la progression pédagogique, et du matériel nécessaire pour réaliser les expériences.

www.projetmerite.fr

14 thématiques variées proches du quotidien des élèves

CM1 - CM2 - 6e - CYCLE 3

Chimie en couleurs
Créez vos objets animés : entre programmation et électronique
Le bois : un matériau issu du vivant
Les aliments : de la matière première aux produits finis
Le sol et son rôle dans la croissance végétale
Le sucre : une matière à explorer
Lutherie sauvage, musique et acoustique
Matériaux et objets quotidiens
Robotique pédagogique : du moteur au mouvement

5e - 4e - 3e - CYCLE 4

Apoll'eau : mesures et analyses avec des fusées à eau
À la table des matières : les sucres
Communication informatique : tout un protocole
Développement d'un objet connecté
Électricité : la produire, la partager

Cette collection est le fruit du projet MERITE (2015-2020) coordonné par IMT Atlantique en partenariat avec 7 établissements d'enseignement supérieur du Grand Ouest et le Rectorat de l'Académie de Nantes. MERITE a été financé au titre du Programme d'Investissements d'Avenir lancé par l'Etat, ainsi que par le Fonds européen de développement régional, la Région des Pays de la Loire et le groupe Assystem.

mallettes MERITE
académie Nantes
RÉGION ACADÉMIQUE PAYS DE LA LOIRE
UNION EUROPÉENNE
Région PAYS de la LOIRE
CE PROJET EST COFINANCÉ PAR LE FONDS EUROPÉEN DE DÉVELOPPEMENT RÉGIONAL
assystem
INVESTIR L'AVENIR