ACCES – Apprentissages en Cryptographie et CybersÉcurité au Secondaire

Projet CyCLyC – Cybersécurité et Cryptographie au Lycée et Collège

Caroline BARDINI
Nicolas SABY

(IMAG- CNRS/Université de Montpellier)

Contexte et problématique

- **Enjeu:** former les élèves au monde numérique actuel, en leur donnant les clés pour le comprendre, y vivre, et y travailler.

- **But:** former les citoyens aux enjeux de cybersécurité dès le secondaire. Etudier le rôle de l'informatique dans l'enseignement, prendre en compte les enjeux actuels en mathématiques, et questionner les liens possibles entre mathématiques et informatique.

- **Questions:**

  - **Quels éléments de cryptographie et de cybersécurité peuvent être enseignés dans le secondaire en France ?**

  - **Comment des apprentissages mathématiques et informatiques en cryptographie peuvent outiller les élèves faces aux enjeux de cybersécurité ?**

  - **Comment peut-on développer ces apprentissages en cybersécurité et cryptographie ?**

Responsable du projet: Simon MODESTE (Université de Montpellier)

Deux versants du projet

- Identifier les possibilités **d'enseigner cybersécurité et cryptographie dans le contexte scolaire français**, sur base d'analyses didactiques, épistémologiques, sémiotiques, historiques, et qui permettent de soutenir une analyse écologique des curricula. **(ACCES)**

- Former un groupe de travail collaboratif entre 3 chercheur(e)s et 7 enseignant(e)s (de mathématiques et d'informatique, en collège ou lycée) permettant la **co-conception et l'expérimentation d'activités**, en prenant en compte la réalité du terrain et des expériences et du bagage des enseignant(e)s. (**CyCLyC**)

Concevoir, expérimenter et analyser des situations d'apprentissages en mathématiques et informatique. Explorer les obstacles épistémologiques et didactique propres à la cybersécurité et cryptographie. Développer des outils théoriques permettant d'analyser les ressources existantes et proposer des activités adaptées au curriculum français. Contribuer à l'appropriation des enjeux sociétaux et citoyens et outiller les élèves face à ces enjeux par ces apprentissages.

ACCES – contexte

- **Etat des lieux:**
  - De nombreuses ressources en cryptographie et cybersécurité ont été développées pour initier le grand public ou des élèves, mais cela n'a **pas toujours diffusé dans les classes et les pratiques enseignantes. Peu de recherches étayées en didactique sur le sujet.**
  - La **plupart des publications** sur l'enseignement de l'informatique qui explorent l'apprentissage de la cybersécurité, considèrent seulement la cryptographie visent souvent un **point de vue technique et instrumental, plutôt que pour ses principes fondamentaux et ses implications sociales.**

- **But:** Apporter un cadre théorique et une méthodologie de recherche permettant la conception et l'analyse fine des situations d'apprentissages, et le pilotage et l'étude des apprentissages des élèves.

ACCES – Approche (1/2)

- **Analyse des programmes scolaires**

But: Identifier :

- Les éléments de contenus explicites liés à la cybersécurité et la cryptographie.
- Les « niches » dans lesquelles de tels contenus pourraient se développer en lien avec les contenus et les compétences du programme.
- Les objectifs en terme d'interdisciplinarité et de compréhension du monde numérique.

- **Analyse épistémologique et sémiotique du savoir**

Exploration épistémologique sur la base des ressources existantes et du savoir disciplinaire.

But: Identifier:

- Les éléments de mathématiques et d'informatique nécessaires à la cybersécurité et la cryptographie.

- Les contenus spécifiques au champ et prérequis associés.

Basés sur une solide approche didactique, soutenir une analyse écologique des curricula.

ACCES – Approche (2/2)

- **Identification des possibles et mise à l'épreuve en classe**

- Proposer et mettre en œuvre des situations afin d'explorer la transposition didactique (*i.e.* le passage du savoir savant au savoir enseigné).

- Les situations développées seront analysées afin d'étudier le potentiel d'apprentissage des élèves. Des vidéos d'activités des élèves, leurs productions, et résultats d'évaluation fourniront une base d'analyse et qui pourront servir de « preuve de concept ».

- **Expérimentations effectuées et analyses en cours**

Enjeu: Faire comprendre les enjeux de la cryptographie et cybersécurité.

Difficultés identifiées: Glissement d'enjeux sémantiques vers le syntaxique, d'où l'importance de la sémiotique pour cette analyse.

Un exemple: Expérimentations autour du code de César.

CyCLyC

- Le groupe de travail est un **groupe collaboratif** entre des enseignant(e)s du secondaire en mathématiques et en informatique et des chercheur(e)s en didactique des mathématiques et de l'informatique, selon le format classique d'un « groupe IREM ».

- **Buts:**
  - Co-concevoir des situations d'apprentissage en cryptographie et cybersécurité. Les situations conçues seront expérimentées dans les classes des participant(e)s et analysées des situations d'apprentissages prenant appui sur les théories développées et explorées dans le cadre de ACCES.
  - Identifier des contenus et approches pertinentes par rapport au contexte français.
  - Prendre en compte la réalité du terrain et des expériences et formations des enseignants, et faire « monter en compétence » des enseignant(e) s sur ces sujets.

Les productions seront principalement des ressources pour l'enseignement (et la formation – initiale et continue) en cybersécurité et cryptographie, qui pourront être diffusées sous forme d'une brochure ou de documents en ligne.

CyClyC - Constitution du groupe et buts

- **Constitution du groupe**

- 2 enseignants de NSI (lycée), 2 enseignants de mathématiques (lycée), 3 enseignants de mathématiques (collège).
- 3 chercheur(e)s.

- **Buts:**

- Développer des activités interdisciplinaires ancrées dans des questions d'actualité.

- Explorer les potentiels d'apprentissage en mathématiques et informatique de ces sujets relativement aux contenus de cryptographie et cybersécurité.

- Réunir et partager des retours d'analyse réflexifs sur les expérimentations des enseignant(e)s ainsi que sur les apprentissages des élèves.

CyCLyC – Expertises des collègues

Retours d'expériences:

- Consultant en cybersécurité actuellement enseignant de NSI.
- Enseignant de Collège qui mène un projet depuis 8 ans en 3ème en interdisciplinarité sur la figure de Turing et la cryptographie.

CyCLyC – Travaux en cours

- Protocole d'informatique débranchée sur la cryptographie asymétrique en terminale NSI (confidentialité, intégrité, authenticité).
- Escape Game en lycée seconde SNT.
- Parcours en cryptographie au fil de l'année de 4ème .
- Parcours en cryptographie en 4ème en résonnance avec ce qui est développé dans le projet ACCES.

SKXIO

(Codage: I c’est O)