CONCEPTION ET ORGANISATION D'UNE SITUATION DIDACTIQUE EN CRYPTOGRAPHIE

Bartzia, Evmorfia-Iro[1] , Modeste, Simon[1] , Lodi, Michael[2,3] , Sbaraglia, Marco[2], Durand-Guerrier, Viviane[1]

[1]Institut Montpelliérain Alexander Grothendieck, Université de Montpellier [2]Département d'Informatique, Université de Bolognia (Italy) [3]INRIA

Contexte

- Développement de l'informatique scolaire
- Interdisciplinarité (mathématique - informatique)
- Cryptographie comme champ à l'interface

Projet **IDENTITIES** – Integrate Disciplines to Elaborate Novel Teaching approaches to InTerdisciplinarity and Innovate pre-service teacher Education for STEM challenges

Questions

1. Peut-on concevoir une situation didactique à l'interface des mathématiques et de l'informatique ? La cryptographie est-elle un contexte adapté pour une telle situation ?

2. Quel type de contenu peut être abordé dans une telle situation didactique ? Quelle organisation peut favoriser l'apprentissage des contenus mathématiques, informatiques, et de leur interactions ?

Cryptographie asymétrique

Bob message clair *m* → chiffrement avec clé publique d'Alice → message chiffré *m'* → déchiffrement avec clé privée d'Alice → **Alice** message déchiffré *m*

Eve

Potentiels didactiques de la cryptographie - hypothèses

- Apprentissages mathématiques et informatique, et interface
- Motivation, et dévolution
- Adidacticité forte : tentatives de chiffrement-déchiffrement, rétroactions...

Choix du problème

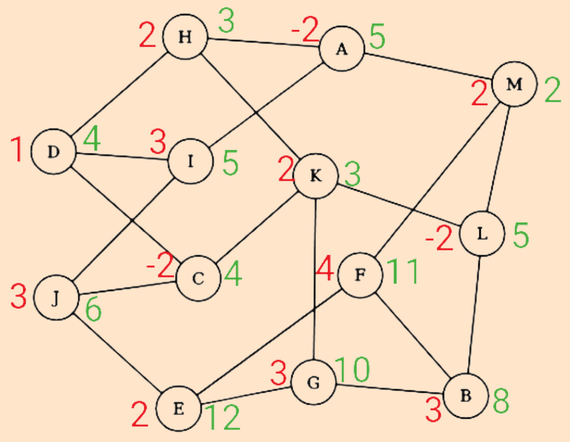
Cryptosystème asymétrique basé sur le problème de l'ensemble dominant parfait (PDS) [3,4].

Un PDS d'un graphe G est un sous-ensemble de sommets tel que tout sommet de G est à distance ≤1 d'exactement un sommet du PDS.

message : un entier m
clé publique : un graphe G ; clé secrète : un PDS de G

Chiffrement :
1. Alice construit un graphe G = (V, E) avec un PDS S
2. Bob attribue à chaque sommet v_i de G un entier m_i , tels que $\Sigma m_i = m$. m_i est appelée la valeur secrète de v_i
3. Pour chaque sommet v, Bob somme sa valeur secrète avec les valeurs secrètes de ses voisins. Cette valeur est appelée la valeur publique du sommet v.
4. Le message chiffré est le graphe G muni des valeurs publiques des sommets.

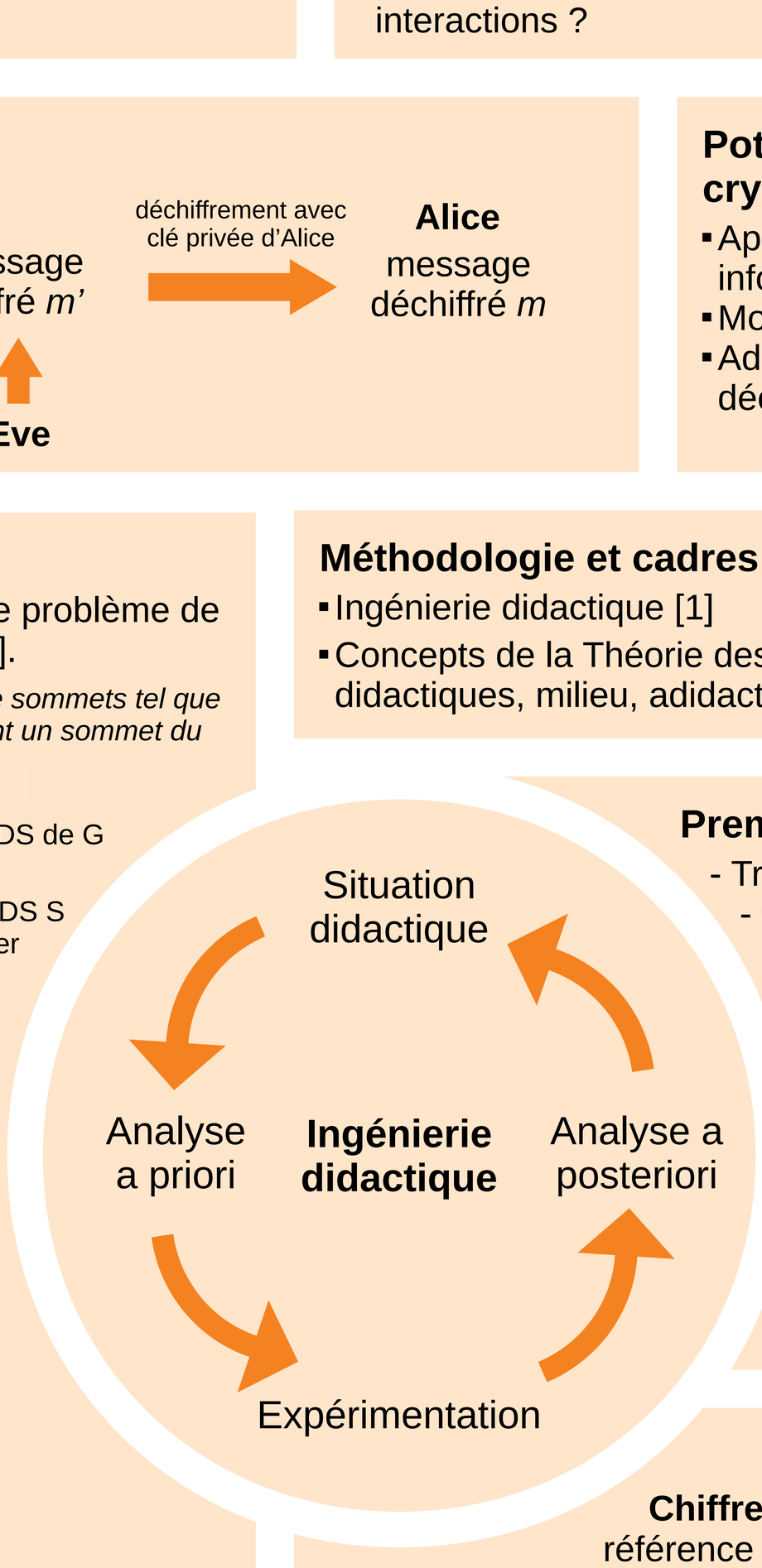
Déchiffrement :
Alice calcule la somme des valeurs sur les sommets qui appartiennent au PDS (qu'elle connaît) et obtient m.



Exemple. Dans ce graphe G, {I, K, F } est un PDS. Message chiffré à partir du graphe G avec les valeurs secrètes en rouge et les valeurs publiques en vert. Le message clair m est la somme des valeurs secrètes (ici m = 19).

Méthodologie et cadres théoriques

- Ingénierie didactique [1]
- Concepts de la Théorie des Situations Didactiques [2] : variables didactiques, milieu, adidacticité, dévolution et institutionnalisation



Premières observations

- Travail cohérent avec les analyses a priori
- Choix des variables didactiques cohérent
- Dévolution rapide du problème
- Validation du potentiel adidactique

Contextes d'expérimentation

- Ateliers internationaux de formation d'enseignants (Mathématiques, Physique-Chimie, Informatique)
- Formation initiale d'enseignants de mathématiques en France

Organisation de la situation

Chiffrement – Présentation du protocole sans référence au PDS

Cryptanalyse – Trois groupes disposant tous d'un même message à déchiffrer, mais d'autres informations différentes :

Groupe A – position « ingénieur cryptographique » :
(i) la définition d'un PDS et (ii) un PDS pour le graphe G donné.

Groupe B – position de cryptanalyste « attaquant »
(i) la définition d'un PDS et (iii) l'algorithme de déchiffrement (qui utilise le PDS)

Groupe C – position de « cryptanalyste testant la robustesse du cryptosystème »
ne dispose d'aucune information supplémentaire

Références

[1] Artigue, M. : Ingénierie didactique : quel rôle dans la recherche didactique aujourd'hui ? Les dossiers des sciences de l'éducation 8(1), 59–72 (2002)
[2] Brousseau, G. : La théorie des situations didactiques en mathématiques. No. 5-1, Presses universitaires de Rennes (2011)
[3] Fellows, M.R., Hoover, M.N. : Perfect domination. Australas. J Comb. 3, 141–150 (1991)
[4] Fellows, M.R., Koblitz, N. : Combinatorially based cryptography for children (and adults). Congressus Numerantium pp. 9–9 (1994)

Co-funded by the Erasmus+ Programme of the European Union

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

This project has been funded with the support of the European Union and the Italian National Agency within the framework of the Erasmus+ Programme (Grant Agreement n°2019-1- IT02-KA203- 063184). The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.