Conception et organisation d'une situation didactique en cryptographie

Evmorfia-Iro Bartzia, Simon Modeste, Michael Lodi, Marco Sbaraglia, Viviane Durand-Guerrier

Conception et organisation d'une situation didactique en cryptographie

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

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

Résumé La cryptographie est un domaine propice pour étudier les interactions entre mathématiques et informatique. Nous présentons la conception d'une situation didactique basée sur un système cryptographique asymétrique. Cette situation a été expérimentée dans une formation d'enseignants.

Keywords: Situation didactique · cryptographie · graphes · ensemble dominant parfait.

1 Introduction, contexte et méthodologie

Dans un contexte international où l'informatique se développe comme discipline scolaire, et où l'interdisciplinarité prend une place importante dans les curriculums et la formation des enseignants, nous interrogeons l'interdisciplinarité entre les mathématiques et l'informatique. En particulier, nous proposons d'explorer le potentiel de la cryptographie pour porter des apprentissages en informatique, mathématiques et leurs interactions, dans le cadre de l'enseignement secondaire et de la formation des enseignants de sciences du secondaire.

1.1 Questions de recherche

Ceci nous amène à étudier les questions de recherche suivantes : 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 ? Quelle organisation peut favoriser l'apprentissage des contenus mathématiques, informatiques, et de leur interactions ?

1.2 Méthodologie d'Ingénierie didactique

Pour développer cette recherche, nous nous plaçons dans une méthodologie d'ingénierie didactique [1], qui consiste à concevoir et analyser finement (du point de vue épistémologique et didactique) une situation qui est ensuite proposée à l'expérimentation. La spécificité de l'ingénierie didactique est la confrontation

d'une analyse a priori à une analyse a posteriori de l'expérimentation. La validation des hypothèses résulte de la conformité de l'analyse a posteriori, sur le plan épistémologique, à l'analyse a priori. Les écarts éventuels permettent de retravailler l'analyse a priori en vue de nouvelles expérimentations. Dans la lignée de nombreuses recherches menées en didactique des mathématiques, nous nous avons développé cette ingénierie didactique dans le cadre de la Théorie des Situations Didactiques (TSD) [2].

2 Le cryptosystème et la situation didactique

2.1 Le problème de l'ensemble dominant parfait

Dans [4] N.Koblitz et M.Fellows proposent un cryptosystème asymétrique basé sur un problème difficile (NP-complet) : le problème du *code parfait* ou de l'*ensemble dominant parfait* (en anglais, Perfect Dominating Set).

Soit un graphe $G = (V, E)$ avec V l'ensemble des sommets et E l'ensemble d'arêtes. Un *voisinage (fermé)* d'un sommet $u \in V$ est l'ensemble $N[u] = \{v \in V | uv \in E\} \cup \{u\}$, des sommets de V adjacents à u ainsi que u (autrement dit, les sommets à distance $\leqslant 1$ de u). Un *ensemble dominant* de G est un sous-ensemble de sommets $S \subseteq V$ tel que tout sommet de V est inclus dans le voisinage d'un sommet de S. Si S est un ensemble dominant de $G = (V, E)$, alors chaque sommet de V est voisin d'au moins un sommet de S ou il appartient à S. Si chaque sommet de V est inclus dans exactement un voisinage d'un sommet de S, on dit que S est un *ensemble dominant parfait* ou un *code parfait* (noté PDS dans la suite). La figure 1 (gauche) donne un exemple de graphe avec un PDS.

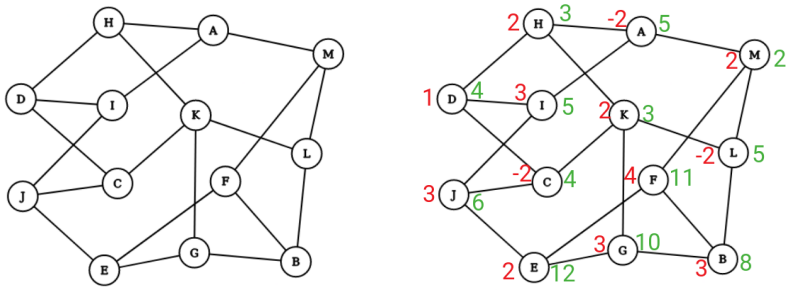

Figure 1. À gauche. Dans le graphe G, $\{I, K, F\}$ est un PDS.
À droite. Exemple d'un message chiffré à partir du graphe G avec les valeurs secrètes en rouge et les valeurs publiques en vert. Le message clair m est la somme des valeurs secrètes (ici $m = 19$).

Ainsi, le problème PDS est le suivant [3,5] :

— Donnée : un graphe $G = (V, E)$

— Question : Déterminer un PDS de G (s'il en existe un)

La sécurité du cryptosystème étudié repose sur la NP-complétude du problème PDS (et du problème de décision associé). Le problème utilisé dans notre situation didactique est une instance du problème PDS, c'est-à-dire basé sur un graphe fixé.

2.2 Le cryptosystème

Sur la base du problème PDS, on peut concevoir un cryptosystème qui exploite les deux faits suivants :

— étant donné un ensemble de sommets, on peut facilement construire un graphe ayant comme PDS cet ensemble de sommets

— étant donné un graphe contenant un PDS, il est difficile de retrouver le PDS si l'on ne connaît que le graphe

Alice et Bobby veulent communiquer confidentiellement. Pour que Bobby puisse envoyer un message m (ici m est un nombre entier) à Alice, ils suivent le protocole de *chiffrement* suivant :

1. Alice construit un graphe $G = (V, E)$ avec un PDS S. Le graphe G est la clé publique de Alice et le PDS S est sa clé privée. Soit $V = \{v_1, v_2, ...v_k\}$.
2. Bobby choisit des entiers $m_1, m_2, ..., m_k$ tels que $m_1 + m_2 + ... + m_k = m$.
3. Bobby attribue à chaque sommet v_i de V un m_i. On appelle m_i la *valeur secrète* du sommet v_i.
4. Pour chaque sommet v_i, Bobby somme sa valeur secrète avec les valeurs secrètes de ses voisins. Cette nouvelle valeur p_i est appelée la *valeur publique* du sommet v_i.
5. Bobby écrit sur chaque sommet sa valeur publique et supprime les valeurs secrètes. Le message chiffré est le graphe G muni des valeurs publiques.

La figure 1 (droite) donne un exemple de graphe avec ses valeurs publiques et secrètes.

Pour *déchiffrer* le message, Alice calcule la somme des valeurs sur les sommets qui appartiennent au PDS (qu'elle connaît).

On voit bien que le graphe G (clé publique) et le message chiffré (graphe G avec valeurs publiques) peuvent circuler sans qu'un observateur puisse connaître m (a priori). Notons aussi que si le graphe a plusieurs PDS, alors tout PDS peut être utilisé pour le déchiffrement.

2.3 La situation didactique : étude du cryptosystème

La situation didactique est organisée comme suit :

Étape 1 : Chiffrement On présente le protocole et l'algorithme de chiffrement avec clé (publique) d'un graphe quelconque G. Nous ne nous référons pas à l'existence d'un PDS (on n'en a pas besoin pour chiffrer un message).

Étape 2 : Cryptanalyse La classe est divisée en trois groupes. On donne aux groupes un message chiffré (le même) et on leur demande de le déchiffrer. Chaque groupe a des informations différentes à sa disposition pour résoudre le défi :

- Le groupe A dispose de (i) la définition d'un PDS et (ii) un PDS pour le graphe G donné. On n'explique pas l'algorithme du déchiffrement.
  Le groupe A se trouve dans la position d'un ingénieur cryptographique qui possède tous les éléments mathématiques et il doit trouver comment les combiner afin de construire un cryptosystème à clé publique.
- Le groupe B dispose de (i) la définition d'un PDS ainsi que (iii) l'algorithme de déchiffrement (qui utilise le PDS). Ils ne connaissent pas le PDS pour le graphe G en question. Le groupe B se trouve dans la position d'un cryptanalyste qui réalise une *attaque de l'homme du milieu* (man-in-the-middle attack) ; i.e. l'attaquant connaît le fonctionnement du cryptosystème asymétrique mais il ne connaît pas la clé privée.
- Le groupe C ne dispose d'aucune information supplémentaire. Il ne connaît pas l'algorithme du déchiffrement. On ne fait pas référence à l'existence d'un PDS. Le groupe C se trouve dans la position d'un cryptanalyste qui cherche à retrouver le message clair sans forcément retrouver la clé privée.

3 Expérimentation

Cette situation didactique a été développée et testée dans le cadre d'une formation de futurs enseignants des sciences, proposée sur plusieurs jours (d'autres activités étaient proposées). À cause des restrictions liée au covid-19, la formation a eu lieu en visio-conférence (ce qui a eu un impact sur la manière dont les étudiants ont pu interagir). Cette première expérimentation a permis de valider nos première hypothèses et de répondre favorablement aux questions de recherches que nous avons posées. Nous ne pouvons pas détailler tout cela ici. Lors de la présentation du poster, nous apporterons des précisions sur les expérimentations et leurs analyses.

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)
5. Haynes, T.W., Hedetniemi, S., Slater, P. : Fundamentals of domination in graphs. CRC press (2013)