CRYPTOGRAPHIE ET MATHEMATIQUES POUR DES ELEVES INGENIEURS EN APPRENTISSAGE

Leïla Reille[1], Anne Exertier[1]

[1] *ESIEE Paris, Noisy-le-Grand, France*

l.reille@esiee.fr

Résumé

L'article présente la mise en place et l'analyse d'un enseignement interdisciplinaire entre mathématiques et technique réalisé sous forme d'apprentissage par problème. Le module s'adresse à des élèves ingénieurs en formation par alternance, qui sont globalement peu réceptifs aux cours théoriques. L'analyse du dispositif montre une augmentation de la motivation et de la participation en séances. Elle propose des pistes d'améliorations concernant l'évaluation individuelle et le travail personnel des étudiants en dehors des séances encadrées.

Mots-clés

Interdisciplinarité ; Apprentissage par problème ; Alternance ; Mathématiques

I. CONTEXTE ET PROBLEMATIQUE

En deuxième année (du cycle ingénieur) de la filière réseaux par apprentissage, les étudiants d'ESIEE Engineering suivent une unité d'initiation à la sécurité des systèmes d'information. Ils y découvrent la cryptographie et le chiffrement (méthode pour sécuriser des données). Les algorithmes de chiffrement reposent sur des concepts mathématiques "avancés" telle que la théorie des corps de Galois. Pour comprendre ces algorithmes et les utiliser sans introduire de failles de sécurité, il est indispensable de maîtriser, un minimum, certaines notions mathématiques.

Or les étudiants de filière par apprentissage sont recrutés après obtention d'un DUT ou BTS dont la formation développe peu la conceptualisation mathématique. Le public auquel s'adresse cette unité dispose d'un bagage mathématique peu adapté à la cryptographie. D'autre part, les étudiants ont pour la plupart développé une certaine réticence ou appréhension vis-à-vis des mathématiques et un manque de confiance dans leurs capacités dans cette discipline. "Comment peut-on entrevoir des satisfactions futures quand personne dans votre entourage ne les incarne, quand

on vous les a désignées depuis longtemps comme inaccessibles" [Meirieu, 1995]. Ils sont vite découragés face à une équation. Comment développer un enseignement de cryptographie nécessitant des mathématiques à des étudiants ayant peu de pré-requis théoriques ?

II. ORIGINES DU DISPOSITIF

La première version proposée aux étudiants consistait en une approche pluridisciplinaire. Tout d'abord une enseignante technique présentait lors de cours magistraux les concepts généraux de cryptographie avant de détailler quelques algorithmes de chiffrement. Ensuite une enseignante de mathématique explicitait les mathématiques en jeu : arithmétique modulaire, théorie des corps de Galois. L'objectif était d'exposer en premier lieu les applications pour intéresser les étudiants à la théorie sous-jacente. Cependant, les étudiants ont éprouvé des difficultés à faire le lien entre ces deux parties a priori complémentaires. L'enseignement bien que préparé collégialement était vu comme cloisonné voire décousu. Les enseignantes ont ressenti une certaine frustration devant le peu d'intérêt manifesté par les étudiants en séance.

Face à ce constat, nous avons cherché à mieux entrelacer les deux disciplines. C'est tout naturellement que la transition de la pluridisciplinarité à l'interdisciplinarité s'est effectuée. Des discussions ont été menées pour clarifier et expliciter les objectifs et attendus. "La frontière disciplinaire, son langage et ses concepts propres vont isoler la discipline par rapport aux autres et par rapport aux problèmes qui chevauchent les disciplines." [Morin, 1990]. Il est effectivement apparu que des termes avaient des significations différentes suivant les disciplines, et que des représentations différentes étaient utilisées pour parler d'un même thème ou objet. Ce n'est pas dérangeant en soi mais ajoute une difficulté supplémentaire, non recherchée, pour l'apprenant. Et cela peut le dérouter voire le bloquer. Nous avons donc été amenées à homogénéiser le vocabulaire et les notations. De plus, il a été envisagé d'aborder un concept mathématique uniquement au travers de son application en cryptographie, l'objectif étant de donner un sens (immédiat) à ce qui est enseigné. D'autre part, la forme pédagogique a été repensée. Comme la population est peu réceptive aux cours magistraux théoriques, nous avons opté pour un type de pédagogie active.

III. PRINCIPALES CARACTERISTIQUES

L'enseignement, d'une durée de 16 heures, est destiné à des élèves ingénieurs réseaux en apprentissage. Il est proposé sous sa forme actuelle à une population de 24 étudiants depuis deux ans. Un document de référence a été conçu en étroite collaboration par les deux enseignantes, il regroupe les principales notions à étudier. Le document de référence doit être suffisamment précis et complet pour être

compréhensible, mais également synthétique pour ne pas rebuter les apprenants, d'autant que l'enseignement ne comporte pas de cours magistraux.

Durant les séances conjointement encadrées par les deux professeurs, les étudiants sont amenés à résoudre des problèmes par équipe de quatre. Ce sont des problèmes concrets qui ont été choisis pour illustrer ou faire ressortir les points clés à acquérir. Il n'y a plus de démarcation franche entre les disciplines : un exercice de mathématiques ne succède plus à un exercice d'informatique. Un problème va nécessiter bien souvent le recours à des compétences mathématiques, informatiques, électroniques. Entre chaque séance, les étudiants sont invités à travailler un chapitre du document de référence, voire également de terminer un problème.

L'évaluation se fait principalement au travers de deux devoirs réalisés en dehors des séances, par équipe de quatre. Les données sont différenciées par équipe. Le premier devoir consiste par exemple à "casser" l'algorithme de chiffrement RSA en trouvant la clé privée à partir de la clé publique (pour des tailles de clés réduites) par attaque par factorisation, puis à déchiffrer un message et enfin à résoudre une énigme. Ces aspects ludique et "challenge" ont été introduits dans le but d'augmenter l'intérêt et la motivation des étudiants. Cette évaluation collective des deux devoirs est complétée, avec un coefficient moindre, par une évaluation individuelle basée sur l'analyse subjective du comportement et de l'investissement de l'étudiant lors des séances.

IV. ANALYSE DU FONCTIONNEMENT

Un questionnaire d'évaluation de cet enseignement a été proposé aux étudiants, en 2009 et 2010. Il comportait des questions fermées et des commentaires libres. Les étudiants ont apprécié de pouvoir donner, pour une fois, un avis critique et détaillé sur leur formation (vu les remerciements dans leurs commentaires), ce qui introduit certainement un biais positif dans leurs réponses au sondage.

Quelle comparaison peut-on faire entre une méthode d'apprentissage par problèmes et une méthode classique ? Lors des séances encadrées, les enseignantes ont constaté que les étudiants étaient globalement actifs et intéressés, bien davantage que lors de l'enseignement classique. L'ambiance dans la salle était nettement plus studieuse que lors des TD ou cours. Ils étaient suffisamment concentrés sur leur sujet qu'ils en oubliaient de réclamer les traditionnelles pauses.

Au début de l'enseignement, certains ont été déstabilisés (36% en 2009, 43% en 2010) par l'approche pédagogique nouvelle pour eux, mais ce sentiment n'a pas perduré. Pendant les séances, un à deux étudiants ont été peu actifs voire totalement passifs. Est-ce lié à des explications insuffisantes sur ce type de méthode d'apprentissage ou à la forme pédagogique peu adaptée à certains types d'apprenants ? Ou encore "cette résistance tient à ce que personne ne peut agir à la place d'un autre, décider d'apprendre ou d'écrire pour lui, …, personne ne peut décider de la liberté de l'autre." [Meirieu, 1991]. Habituellement dans un TD, la plupart de ces étudiants attendent la correction des exercices pour les relire juste

avant les examens. En APP, la proportion d'étudiants passifs a été moindre. Les étudiants éprouvaient le besoin de lever leurs doutes éventuels sur leurs raisonnements et appelaient souvent les enseignantes pour des questions de compréhensions ou des vérifications. Ils ne se contentaient pas d'avoir un résultat aussi peu probable soit-il.

En opposition à l'activité en séance, le travail en dehors était léger comme lors d'enseignements classiques. En général, le chapitre à étudier était davantage survolé que travaillé. Nous n'avons pas réussi à susciter du travail personnel sur le document de référence alors qu'ils se sont investis en dehors des heures programmées à l'occasion des devoirs. Le travail préparatoire pour une séance est superficiel peut-être en raison de la difficulté pour un apprenant à déceler une incompréhension ou un apprentissage peu approfondi. Cette difficulté existe également dans un cours magistral. La lecture attentive d'un document clair et adapté peut donner l'illusion à l'apprenant qu'il a compris alors qu'il a simplement détecté que le cours ne comportait pas d'erreurs. Mais l'apprentissage n'est que superficiel et le lecteur ne le réalisera qu'au moment de la résolution de problèmes. La motivation soulevée pendant les séances ne pousse pas non plus les étudiants à asseoir leurs connaissances en revoyant le document de référence et en retravaillant ce qui a été vu. Pour le travail personnel peu de différences constatées entre les deux approches pédagogiques.

Ce choix de pédagogie active a restreint le contenu scientifique traité au travers des problèmes. Un éventail plus large de connaissances était présenté lors des cours magistraux, mais ces connaissances étaient-elles assimilées ? Si le document de référence a atteint un niveau de synthèse et de clarté satisfaisant, on peut, cependant, lui reprocher l'absence d'ouverture vers un approfondissement et de ne pas insister sur les autres contextes dans lesquels s'appliquent les nouveaux acquis. N'est-ce pas davantage une frustration d'enseignant qu'une nécessité pour l'apprenant ?

"Obtenir la participation ne signifie pas nécessairement susciter un apprentissage positif" [Landsheere, 1975]. Comment déterminer les acquis des apprenants ? L'évaluation retenue, faite au travers de devoirs réalisés par équipe a montré qu'un apprentissage a eu lieu. Par exemple nous avons pu constater que l'analyse des critères de factorisation utilisés a été correctement traitée pour une grande majorité d'entre eux.

L'évaluation par devoirs collectifs a été appréciée, en particulier parce qu'elle retire "l'épée de Damoclès" de l'examen écrit comme l'indique un étudiant. De plus, déchiffrer un message crypté a été perçu comme un jeu et toutes les équipes ont développé un programme informatique pour relever rapidement le défi. L'aspect ludique était une invitation à comprendre qu'ils pouvaient travailler les mathématiques en s'amusant. Les réponses au questionnaire montrent la satisfaction des étudiants d'avoir fait ce devoir et donc que cet objectif a été atteint. Le devoir est le fruit d'un travail collaboratif (a-t-il bien lieu ?), on peut supposer que c'est le partage de la responsabilité et le soutien mutuel qui sont appréciés au travers de l'évaluation. C'est peut-être également l'aspect stressant d'un examen écrit en temps limité qui est rejeté. Néanmoins, certains étudiants s'interrogent sur leurs acquis

individuels. La question se pose également côté enseignant. Une analyse en séances du comportement des étudiants donne des indications sur la participation et leur investissement mais peu d'informations sur leurs apprentissages. Au travers de réponses pertinentes, il est possible de détecter des acquis chez certains, mais très difficile chez les étudiants d'un naturel réservé qui s'expriment peu face à un enseignant.

Le travail en équipe quant à lui favorise l'apprentissage, il initie la discussion au sein de l'équipe mais aussi avec les enseignants. Il diminue la crainte de poser des questions qui sembleraient bêtes, ce que confirme le questionnaire 2010 où 86 % des étudiants ont osé poser toutes les questions utiles à leur compréhension. Un commentaire libre du questionnaire 2009 met en évidence l'intérêt du travail collaboratif : "Cette idée de créer des petits groupes a été une très bonne idée, car on a pu échanger nos questions et nos connaissances entre nous…en étant en petit groupe et non alignés comme du bétail on se repose moins ainsi sur les autres, on se penche plus sur le sujet et on hésite surtout moins à prendre la parole". Le rôle des membres d'une équipe évolue lors des séances : des étudiants réservés ont pris de l'assurance et sont devenus des leaders positifs. Les éléments moteurs dépendent aussi des thèmes abordés, ceux qui ont des facilités sur un sujet aident naturellement leurs coéquipiers.

Outre son intérêt pédagogique, le travail en équipe reproduisant la réalité du métier d'ingénieur constitue une approche professionnalisante. L'attitude de l'enseignant veillant à ce que les équipes avancent et les aidant dans ce sens se rapproche de celle du chef de projet en entreprise. Au-delà de la transformation d'éducateur à accompagnateur, les enseignants n'étant plus isolés face au tableau, sont considérés comme un conseiller, comme le soulignent des commentaires d'étudiants : "enseignant plus accessible", "enseignant plus à l'écoute, plus facile à aborder, plus d'échanges".

L'élaboration d'un enseignement interdisciplinaire diminue fortement l'implicite de chaque enseignant dans sa matière et clarifie les objectifs à atteindre. L'enseignant est amené par les questions de son collègue à expliciter tout ce qui lui aurait semblé "évident" dans sa matière provenant de tous les réflexes acquis. La confrontation du regard de l'autre remet en question les pré-requis supposés et souvent non dits nécessaires pour aborder de nouvelles notions. Les questions du "maître ignorant" sont-elles toujours une aide pour comprendre les difficultés des étudiants ? Parfois, en raison de sa spécialité, le maître ignorant pose des questions qui n'ont pas lieu d'être pour les apprenants. En tenir compte est un risque de perturbations inutiles pour ces derniers. L'encadrement de séances par des enseignants de disciplines différentes permet aux étudiants d'avoir des explications moins formelles et/ou moins rigoureuses quand ils s'adressent au non spécialiste.

L'aspect interdisciplinaire et la forme pédagogique ont contribué à susciter l'intérêt des étudiants pour cet enseignement. 100% le jugent utile pour leur formation d'ingénieurs réseaux.

V. BILAN ET PERSPECTIVES

L'interdisciplinarité et l'évolution vers une pédagogie active ont permis d'augmenter l'intérêt et la motivation des étudiants pour la cryptographie. "Au-delà du désir éphémère et de l'effort ingrat, il faut trouver l'intéressant, qui suscite de lui-même l'effort en profondeur et la joie véritable" [Reboul, 2001]. Il semble que cet objectif soit presque atteint et le sera totalement lorsque nous arriverons à obtenir un travail personnel approfondi et régulier hors séances. Nous avons décidé d'engager cette année une réflexion conjointe avec les étudiants sur le comment développer leur regard critique et analytique face à de nouvelles connaissances et leur faire prendre conscience du profit d'un travail individuel efficace.

L'évaluation est également à améliorer. Elle doit permettre aux étudiants de se rendre compte, à titre individuel, de leurs acquis et de leurs progrès. Une évaluation individuelle doit être proposée, mais sous quelle forme ? Un examen écrit est un mode d'évaluation individuelle, mais est-ce une réponse adaptée ? Il est en tout cas redouté par les apprenants pour qui la majorité des évaluations scolaires a lieu sous cette forme. Un de nos objectifs est de co-construire un mode d'évaluation adéquat à nos attentes mutuelles. Une suggestion peut être d'utiliser un journal de bord pour chaque étudiant où seraient inscrites leurs progressions dans l'acquisition de capacités et de compétences. Reste à savoir s'ils seront intéressés par cette proposition.

L'interdisciplinarité offre aux enseignants la possibilité de changer de regard à la fois sur son domaine de spécialité et sur l'autre. Les étudiants sont également amenés à changer de regard, en particulier, sur une discipline qui leur paraît être déconnectée de la réalité. Ce changement de posture produit un certain enthousiasme et une envie de réussir. Les mathématiques ne sont plus alors perçues uniquement comme une contrainte incontournable dans leurs études d'ingénieurs. Cultiver l'envie commence peut-être par apprendre à changer de regard ?

REFERENCES

Meirieu, P. (1991). Apprendre…oui mais comment. Paris : ESF.

Meirieu, P. (1995). La pédagogie entre le dire et le faire : De l'impuissance et du pouvoir de l'éducateur. Paris : ESF.

Cousinet, R. (1959). Pédagogie de l'apprentissage. Paris : PUF.

Morin, E. (1990). Sur l'interdisciplinarité. Carrefour des sciences, Actes du Colloque du Comité National de la Recherche Scientifique "Interdisciplinarité", Paris : Editions du CNRS.

Reboul, O. (2001). La Philosophie de l'éducation. Paris : PUF 9ème édition.

De Landsheere, G. (1975). Définir les objectifs de l'éducation. Paris, P.U.F.