Jean-Marie Urfer
Membre de la CRM, christian.aebi@edu.ge.ch

Cryptologie

Colloque annuel de la CRM organisé à Champéry du 10 au 13 septembre 2024

La CRM a organisé son traditionnel cours de formation continue pour les enseignant·e·s du secondaire II réunissant quatre conférenciers, une conférencière et plus de cinquante participant·e·s à l'Hôtel Suisse à Champéry. Grâce à une salle parfaitement équipée, les conférences se sont déroulées dans d'excellentes conditions.

Ce cours, riche et varié, proposait des contenus directement exploitables en classe, ainsi que des présentations plus avancées pour offrir aux participant·e·s une meilleure compréhension de certains aspects de la recherche actuelle et de ses applications pratiques.

Pour débuter, Didier Müller (Lycée cantonal de Porrentruy) a présenté les bases de la cryptologie par le biais de quelques livres où le décryptement d'un message secret joue un rôle important et a indiqué quelques pistes pour utiliser en classe son propre livre[1]. Il a également expliqué comment des méthodes métaheuristiques (méthodes stochastiques et itératives utilisées pour résoudre des problèmes d'optimisation) telles que le recuit simulé et la recherche sans tabous pouvaient être appliquées pour casser un code sans en connaître la clé.

Alain Roubaty (HEG-Arc) a ensuite présenté l'art de la stéganographie, c'est-à-dire la dissimulation d'un message dans un autre contenu, comme une image. Dans un deuxième cours, il a rappelé les concepts de clé publique, la notion de « one-way function » et les problèmes permettant la création d'un système à clés publiques, le logarithme discret ou la factorisation des nombres entiers permettant au final la présentation du RSA.

Alessio Caminata (Università di Genova) a exposé les enjeux actuels de la cryptographie post-quantique. Les protocoles actuels de clé publique reposant sur le problème du logarithme discret et la factorisation des entiers peuvent être facilement résolus par un ordinateur quantique grâce à l'algorithme de Shor. La cryptographie post-quantique vise donc à développer de nouvelles primitives cryptographiques à partir de problèmes mathématiques que les ordinateurs quantiques ne pourraient résoudre plus rapidement que les ordinateurs classiques, comme ceux provenant de la théorie des codes, des réseaux ou des polynômes.

Un pas de côté a été proposé par Cristina Landolina (Höhere Fachschule für Technik Mittelland) qui a parlé de la théorie des codes. Après une introduction générale sur les codes correcteurs d'erreurs et sur la théorie du codage classique, à savoir les codes dotés de la métrique de Hamming, elle a exposé une généralisation naturelle de cette théorie : les codes dans la métrique de rang. Les méthodes utilisées dans la théorie du codage sont dans la plupart des cas des applications des concepts de base de l'algèbre linéaire.

Pour terminer, François Weissbaum (DDPS) a abordé l'algorithme de signature numérique à clé publique ECDSA (Elliptic Curve Digital Signature Algorithm). Après une présentation succincte des types de courbes elliptiques permettant de définir un groupe fini utilisé par ECDSA et la simulation du principe du protocole avec le logiciel Sagemath, la deuxième partie s'est concentrée sur la faiblesse de ce protocole qui doit utiliser un nombre aléatoire. Si le générateur ne fonctionne pas correctement, l'attaquant peut alors reconstruire la clé privée de la personne qui a signé un document avec une attaque basée simplement sur l'identité de Bézout.

[1] D. Müller, Les 9 Couronnes, Ed. Société Jurassienne d'Émulation