Sujets de projets proposés en Arithmétique Modulaire (2020/21)

Les algorithmes implémentés doivent être intéressants, ils doivent reposer sur un concept solide de recherche algorithmique.

Projet 1 : « Tests de Primalité »

L'objectif du projet est de faire un exposé sur les différents tests de primalité existants en arithmétique modulaire et en cryptographie des plus anciens aux plus récents, et d'implémenter au moins deux de ces algorithmes en précisant la complexité de chaque algorithme implémenté.

Projet 2 « Exponentiation modulaire »

L'objectif de ce projet est de faire un exposé sur les différents algorithmes permettant de calculer les puissances et leurs utilités en cryptographie, et implémenter au moins deux méthodes en précisant la complexité de chaque algorithme implémenté.

Projet 3 « Logarithme discret»

L'objectif du projet est de faire un exposé riche sur ce concept et son application en cryptographie, citer les différents algorithmes et en implémenter au moins deux algorithmes en précisant la complexité de chaque algorithme implémenté.

Projet 4. « Calcul du symbole de Legendre et de Jacobi »

L'objectif de ce projet est de faire un exposé sur l'utilité des symboles de Legendre et Jacobi en cryptographie, citer les différents algorithmes dans la littérature pour le calcul de ces symboles, en implémenter au moins deux tout en précisant la complexité ainsi que l'efficacité des algorithmes proposés.

Projet 5. Arithmétique dans $\mathbb{F}_p$

L'objectif de ce projet est d'abord d'expliciter la problématique de l'implémentation des réductions modulaires et d'exposer les différents algorithmes proposés et d'implémenter un algorithme de réduction modulaire généraliste en précisant sa complexité ainsi qu'un algorithme de réduction modulaire spécifique sur le corps $\mathbb{F}_p$ et préciser sa complexité.

Projet 6. Multiplication dans le corps fini $\mathbb{F}_{2^n}$

L'objectif de ce projet est d'abord d'exposer l'importance des corps finis en cryptographie et codage, ensuite d'implémenter deux algorithmes de multiplication modulaire et matrice de structure dans le corps $\mathbb{F}_{2^n}$ et de préciser leurs complexités.