Rapport sur l'épreuve écrite de culture scientifique
Informatique

L'épreuve comportait trois exercices composés de questions de niveaux gradués afin de mesurer la compréhension, les connaissances et les capacités d'initiative et de créativité des candidats.

Le premier exercice était de loin le plus classique des trois, et fut plutôt bien traité dans l'ensemble, même si la rédaction n'était pas parfaite. Il était composé de quatre questions visant à tester la culture générale en algorithmique : la première portait sur l'algorithme de Horner, la seconde sur l'inversion de plusieurs éléments, la troisième sur le pgcd binaire, et enfin la quatrième sur la racine carrée. Tout candidat ayant lu l'ouvrage de Cormen/Leiserson/Rivest sur l'algorithmique était en mesure de traiter convenablement le premier exercice.

Le deuxième exercice portait sur la recherche de cycle, et il ne fut malheureusement pas bien traité du tout par les candidats. On y présentait l'algorithme de Floyd, qu'il fallait analyser rigoureusement. Le but de la dernière question était de retrouver un algorithme alternatif découvert par Brent. La recherche de cycle est notamment utilisée pour résoudre deux problèmes chers à la cryptographie : la factorisation d'entiers et le logarithme discret.

Le troisième exercice, proposé à la sagacité des candidats dont la discipline secondaire est l'informatique, était le plus mathématique des trois : il n'a pas du tout été traité par l'unique candidat de discipline secondaire. L'exercice portait sur des suites engendrées par ce que l'on appelle un registre à décalage avec rétroaction linéaire. Ce sujet est en rapport avec la théorie des codes correcteurs d'erreurs, et a par exemple des applications en chiffrement par flot. Le but de cet exercice était de decouvrir des algorithmes de reconstructions distincts de l'algorithme de Berlekamp-Massey.

Phong Nguyen