HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2024

30/09/2024. Homework for Lecture 4.

Exercise 1. A proper 3-coloring of a graph is a labeling of each vertex of the graph with one of three colors so that every two vertices connected by an edge get different colors. Not all graphs admit a proper 3-coloring. The problem of deciding whether a given graph is 3-colorable is NP-complete.

Assume there exists an efficient (polynomial-time) algorithm $\mathcal{A}_1$ that can decide whether a given graph is 3-colorable. Prove that there exists another efficient (polynomial-time) algorithm $\mathcal{A}_2$ that not only decides whether a given graph is 3-colorable, but also finds for every 3-colorable graph an instance of a proper 3-coloring.

Exercise 2. A function $F\colon \{0,1\}^k \to \{0,1\}^n$ can*not* be a pseudo-random generator (in the sense of the definition discussed in the class) if $k \leq \log n$.

Exercise 3. If $\mathrm{P} = \mathrm{NP}$, then pseudo-random generators do no exist.