Outils et algorithmes pour la protection de l'information (I231)
Session 1 (2022-2023) - Partie 1 (10pts)

La précision et la clarté de votre rédaction sont ***fondamentales***. Chaque réponse doit être ***justifiée***, les programmes doivent être ***commentés*** et les algorithmes ***expliqués***. Le [barême] est donné à titre indicatif et il est susceptible d'être adapté. Les documents sont interdits. Durée à consacrer à cette partie : 1h45.

EXERCICE 1. [2.00] Rappelez la définition d'une transformation polynomiale $\propto_P$ et la définition d'un problème NP-Complet.

EXERCICE 2. [5.00] Démontrez que la fonction $f : \mathbb{N}^2 \to \mathbb{N}$ définie par

$$f(n,m) := \begin{cases} 1 & \text{si } n \geq m, \\ 0 & \text{sinon.} \end{cases}$$

est Turing-calculable. Impératif : décrivez d'abord votre algorithme *en français* avant d'écrire votre code que vous commenterez afin de mettre en évidence le rôle de chaque bloc d'instruction. Indication : utilisez l'alphabet unaire.

EXERCICE 3. [3.00] On considère le problème de décision suivant : soit B un ensemble fini de séquences binaires toutes de même longueur $n \in \mathbb{N}$. Existe-t-il une séquence binaire x de longueur n qui coïncide avec chaque séquence de B sur un bit au moins ?

Formalisez ce problème de décision avec la terminologie employée en cours, puis démontrez qu'il est dans la classe NP.