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

# 02/12/2024. Homework for Lecture 11.

**Exercise 1.** Let $m_1$ and $m_2$ be two natural numbers. Prove that if a prime number $p$ divides $n = m_1 \cdot m_2$, then $p$ must divide $m_1$ or $m_2$.

**Exercise 2.** Prove that if $\mathrm{P} = \mathrm{NP}$ then there exists a deterministic algorithm that finds for every input $n$ (an integer numbers given by its binary expansion) the list of all its prime factors in polynomial time.

**Exercise 3.** Let $n = 323 = 17 \cdot 19$.

(a) Find without a computer a number $x$ in the set $\{1, \ldots, n-1\}$ such that $x = 1 \mod 17$ and at the same time $x = -1 \mod 19$.

(b) Find without a computer four different numbers $x$ in the set $\{1, \ldots, n-1\}$ such that $x^2 = 1 \mod n$.

(c) Find without a computer four different numbers $x$ in the set $\{1, \ldots, n-1\}$ such that $x^2 = 16 \mod n$.