**HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2023**

# 27/11/2023. Homework for Lecture 11.

**Exercise 1.** Show that the function mapping every natural number to is square is not a one-way function.

**Exercise 2.** Let $f : \{0,1\}^* \to \{0,1\}^*$ be a one-way function.

(a) Prive that the function $f'$ defined as $f'(x) := f(x)0$ (a suffix '0' is added) is also a one-way function.

(b) Prive that the function $f''$ defined as $f''(x) := f(x)f(x)$ (the value $f(x)$ repeated twice) is also a one-way function.

**Exercise 3.** (a) Show that if there exists a one-way functions, then there exists a one-way function such that $f(\underbrace{00\ldots0}_{n}) = \underbrace{00\ldots0}_{n}$ for every $n$.

(b) Show that if there exist one-way functions, then some of them are are not pseudo-random generators.

**Exercise 4.** Show that there exists a length-preserving one-way function $f : \{0,1\}^* \to \{0,1\}^*$ such that $g(x) := x \oplus f(x)$ (bitwise XOR of $x$ and $f(x)$) is *not* a one-way function.