UCLouvain – EPL
LMAT2450: Cryptography
Year 2020-2021

Last Name:

Given Name:

NOMA:

# LMAT2450 – First Homework

**Question 1**: Pseudorandom Generator.

Let $G$ be a pseudorandom generator (PRG) such that, if $s \in \{0,1\}^n$, then $G(s) \in \{0,1\}^{l(n)}$ with $l(n) > n$.

We define, for $s_1, s_2 \in \{0,1\}^n$, $G'(s_1||s_2) := G(s_1)||s_2$ where $G'(s_1||s_2) \in \{0,1\}^{l(n)+n}$.

Show that either $G'$ is a PRG by offering a reduction to the security of $G$, or that $G'$ is not a PRG by exhibiting an attack (building a distinguisher with non negligible advantage).

**Solution:**

Last Name:

Given Name:

NOMA:

**Question 2**: Pseudorandom Function.

Consider $F$ a pseudorandom function (PRF) such that $F : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$.

We define $F' : \{0,1\}^n \times \{0,1\}^{2n} \longrightarrow \{0,1\}^n$ such that $F'(k, x||y) := F(k,x) \oplus F(k,y)$.

Show either that $F'$ is a PRF by providing a reduction to the security of $F$, or that $F'$ is not a PRF by exhibiting an attack (building a distinguisher with non negligible advantage).

**Solution:**

Last Name:

Given Name:

NOMA:

**Question 3**: How not to derive a PRG.

Let $G$ be a PRG such that, if $s \in \{0,1\}^n$, then $G(s) \in \{0,1\}^{l(n)}$ with $l(n) > n$. Define also $G'$ such that $G'(s) := G(s) \oplus (0^{l(n)-n} || s)$.

Show that $G'$ may not be a PRG.

**Solution:**