# Introduction to Cryptography – LMAT2450
# Practical Lesson 2

Clément Hoffmann (clement.hoffmann@uclouvain.be)
Yaobin Shen (yaobin.shen@uclouvain.be)

October 12, 2022

**Exercise 1** (*An attack*)

Let $F$ be a pseudorandom permutation. Consider the mode of operation in which a uniform value $IV \in \{0,1\}^n$ is chosen, and the $i$-th ciphertext block $c_i$ is computed as $c_i := F_k(IV + i + m_i)$, where each $m_i \in \{0,1\}^n$ and the addition is performed modulo $2^n$. Show that this scheme is not EAV-secure.

**Exercise 2** (*Reduction.*)

Let $\Pi = \langle \mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec} \rangle$ be an encryption scheme having indistinguishable multiple encryptions in the presence of an eavesdropper. Suppose we define a new scheme $\Pi' := \langle \mathrm{Gen}', \mathrm{Enc}', \mathrm{Dec}' \rangle$ as follows.

- $\mathrm{Gen}' := \mathrm{Gen}$
- $\mathrm{Enc}'_k(m) := \mathrm{Enc}_k(m) \| 1$ (i.e. a '1' bit is appended to the ciphertext)
- $\mathrm{Dec}'_k(c) := \mathrm{Dec}_k(c_1)$, where $c_1$ is obtained by discarding the last bit of $c$.

1. Is $\Pi'$ also a mult-EAV secure encryption scheme? Provide either an (efficient) attack/adversary or a (polynomial) reduction, depending on your claim.

2. Answer the same question, but considering the CPA security of $\Pi'$, assuming that $\Pi$ is CPA secure.

**Exercise 3** (*PRG.*) Let $G$ be a pseudorandom generator with expansion factor $\ell(n) > 2n$. In each of the following cases, say whether $G'$ is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample.

1. Define $G'(s) = G\left(s_1 \cdots s_{\lceil n/2 \rceil}\right)$, where $s = s_1 \cdots s_n \in \{0,1\}^n$.

2. Define $G'(s) = G\left(0^{|s|} \| s\right)$ where $s \in \{0,1\}^n$, that is, we prepend $|s|$ '0' bits to $s$.