# Introduction to Cryptography – LMAT2450
# Practical Lesson 1

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

**Exercise 1** (*Perfect secrecy.*)

We define the following encryption scheme for messages, keys and ciphertexts in $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n$, where $\mathbb{Z}_n$ is essentially the integers in the interval $[0, n)$ (in fact $(\mathbb{Z}_n, +)$ forms a group):

- Gen outputs a key $k \in \mathcal{K}$ selected uniformly at random.
- $\mathrm{Enc}_k(m) := k + m \mod n$
- $\mathrm{Dec}_k(c) := c - k \mod n$

Suppose messages are drawn from $\mathcal{M}$ according to the binomial distribution. More precisely $M \sim \mathrm{Bi}(n-1, p)$ for some probability $p$ which means that $\forall m \in \mathcal{M} : \Pr[M = m] = \binom{n-1}{m} p^m (1-p)^{n-1-m}$.

1. Show that the encryption scheme above is perfectly secret.
2. Evaluate $\Pr[C = c]$ for every $c \in \mathcal{C}$.
3. Evaluate $\Pr[K = k | C = c]$ for every $k \in \mathcal{K}$ and $c \in \mathcal{C}$.

**Exercise 2** (*Negligible functions.*)

1. Let $f$ be a negligible function in $n$. Show that $g : n \mapsto 1000 \cdot f(n)$ is negligible too.
2. Show that the function $n \mapsto n^{-\log(n)}$ is negligible in $n$.

**Exercise 3** (*Efficiency.*)

Explain why the function that maps $n$ on a sequence of "1" of length $\lfloor \sqrt{n} \rfloor$ cannot be evaluated by any efficient algorithm in the size of the entry.

An example of such algorithm is given in Algorithm 1.

**Algorithm 1** Example of algorithm

**Require:** $n \geq 0$
**Ensure:** A sequence of $\sqrt{n}$ "1"
  **for** $i = 0$ to $\lfloor \sqrt{n} \rfloor$ **do**
    Print '1'
  **end for**

Hint: see $n$ as a power of 2.

**Exercise 4** (*Security model.*)

Let $\epsilon$ denote a negligible function. Remember that $\Pi := \langle \text{Gen}, \text{Enc}, \text{Dec} \rangle$ has *indistinguishable multiple encryption in the presence of eavesdroppers* if $\forall$ PPT $\mathcal{A}$, $\exists\ \epsilon$ :

$$\Pr[\mathsf{PrivK}^{\mathsf{mult}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \epsilon(n)\,,$$

where $\mathsf{PrivK}^{\mathsf{mult}}_{\mathcal{A},\Pi}(n)$ is defined as follows.

1. $\mathcal{A}$ outputs $M_0 = (m_0^1, \ldots, m_0^t), M_1 = (m_1^1, \ldots, m_1^t)$
2. Choose $k \leftarrow \text{Gen}(1^n)$ and $b \leftarrow \{0, 1\}$, and send $(\text{Enc}_k(m_b^1), \ldots, \text{Enc}_k(m_b^t))$ to $\mathcal{A}$
3. $\mathcal{A}$ outputs $b'$
4. Define $\mathsf{PrivK}^{\mathsf{mult}}_{\mathcal{A},\Pi}(n) := 1$ iff $b = b'$

Also remember that $\Pi := \langle \text{Gen}, \text{Enc}, \text{Dec} \rangle$ has *indistinguishable encryption under a chosen-plaintext attack* if $\forall$ PPT $\mathcal{A}$, $\exists\ \epsilon$ :

$$\Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \epsilon(n)\,,$$

where $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$ is defined as follows.

1. Choose $k \leftarrow \text{Gen}(1^n)$
2. $\mathcal{A}$ **is given oracle access to** $\text{Enc}_k(\cdot)$
3. $\mathcal{A}$ outputs $m_0, m_1 \in \mathcal{M}$
4. Choose $b \leftarrow \{0, 1\}$ and send $\text{Enc}_k(m_b)$ to $\mathcal{A}$
5. $\mathcal{A}$ **is again given oracle access to** $\text{Enc}_k(\cdot)$
6. $\mathcal{A}$ outputs $b'$
7. Define $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) := 1$ iff $b = b'$

Define the concept of indistinguishable *multiple* encryption under a chosen-plaintext attack.