**Exercises lecture 3 - Part 2 /JL Roch - Provable security**

# 1 Entropy and unconditional security

Let $k$ be a key of length $n$ uniformly chosen in $\{0,1\}^n$ ; let $(E_k, D_k)$ be an encryption scheme for messages of length $m$ :

$$\forall k \in \{0,1\}^n, \forall x \in \{0,1\}^m : \quad D_k(E_k(x)) = x.$$

Besides, let $U_n$ denote the uniform distribution over $\{0,1\}^n$.

1. In this question only, $n = m$ and $E_k = E_k^{OTP}$ : $E_k^{OTP}(x) = x \oplus k$ where $\oplus$ denotes the bitwise XOR. What is $D_k^{OTP}(x)$ ?
   For any $x, x' \in \{0,1\}^m$, show that the distribution $E_{U_n}^{OTP}(x)$ is the same as $E_{U_n}^{OTP}(x')$.
2. For any $(E_k, D_k)$ : if $n < m$, show that there exist two messages $x, x' \in \{0,1\}^m$ such that $E_{U_n}(x)$ is not the same distribution as $E_{U_n}(x')$.
3. If $n \geq m$, we consider $(E_k, D_k)$ such that $\forall x, x'$ : $E_{U_n}(x)$ is the same distribution as $E_{U_n}(x')$. Show that $E$ is then unconditionally secure *(hint : use Bayes theorem)*.

# 2 Levin's universal one-way function

Let $(M_i)_{i \in \mathbb{N}}$ denote the sequence of all deterministic Turing machines (or equivalently all deterministic algorithms). For $x \in \{0,1\}^+$, we define $M_i^t(x)$ by :
- if $M_i$ performs at most $t$ computational steps on input $x$, then $M_i^t(x)$ is the output of $M_i$ on input $x$ ;
- else $M_i^t(x) = 0^{|x|}$ (i.e. the bit O repeated $|x|$ times).

The Levin's universal function $f_U : \{0,1\}^+ \to \{0,1\}^+$ is defined by :
- treat the $n$ input bits as a list $x_1, \ldots, x_{\log n}$ of blocks of $n/\log n$ bits each ;
- output the sequence of $\log n$ results : $M_1^{n^2}(x_1), \ldots, M_{\log n}^{n^2}(x_{\log n})$.

Questions :

1. Justify that $f_U$ can be computed in polynomial time.
2. In this question, we assume that $M_1$ implements a one-way function. Moreover, we assume that, for any input of $n$ bits, $M_1$ uses at most $n^2$ computational steps and outputs exactly $n$ bits. Show that $f_U$ is a one-way function (hint : explicit a reduction).
3. Assume there exists a function $g$ resistant to pre-image such that, for an input $x$ of $n$ bits, $g(x)$ is computed in time at most $n^c$ (and thus has at most $n^c$ bits).
   For $x \in \{0,1\}^n$, let $L_c(x)$ denote the $\lfloor n^{1/c} \rfloor$ first bits of $x$ and $H_c(x)$ the remainder bits : $x = L_c(x) || H_c(x)$. Define $g'(x) = g(L_c(x))$.
   Show that $g'$ is resistant to pre-image and can be computed in time $O(|x|)$.
4. Show that $f_U$ is one-way if and only if there exists a one-way function.