Problem Set 2

1. Suppose that $F : \{0, 1\}^k \times \{0, 1\}^m \to \{0, 1\}^m$ is a $(t, \epsilon)$ secure pseudorandom function.

Consider the following randomized MAC scheme (we shall assume for simplicity that $m$ is a multiple of 3 and the scheme is defined only for messages whose length is a multiple of $m/3$ and is at most $\frac{m}{3} \cdot 2^{m/3 - 1}$):

- **Tag** ($K, M$)
  - divide $M$ into blocks $M_1, \ldots, M_\ell$ of length $m/3$
  - pick a random $r \in \{0, 1\}^{m/3}$
  - return $(r, F_K(r, 0, 0, M_1), F_K(r, 0, 2, M_2), \ldots, F_K(r, 1, \ell, M_\ell))$

- **Verify** ($K, M, (r, f_1, \ldots, f_\ell)$)
  - divide $M$ into blocks $M_1, \ldots, M_\ell$ of length $m/3$
  - check that for every $i \in \{1, \ldots, \ell - 1\}$ we have $f_i = F_K(r, 0, i, M_i)$ and that we have $f_\ell = F_K(r, 1, \ell, M_\ell)$.

Show that this scheme is $(t/O(L), \epsilon + t^2 \cdot 2^{-m/3} + 2^{-m})$-secure, where $L$ is an upper bound to the length of the messages that we are going to authenticate.

2. Fix a randomized algorithm $P$ (for “padding”) that on input a string in $\{0, 1\}^m$ runs in time $\leq r$ and outputs another string in $\{0, 1\}^m$. Let $(Enc, Dec)$ be an encryption scheme that encrypts blocks of length $2m$, and consider the modified encryption scheme $(PEnc, PDec)$ defined so that a message $M$ is first padded by appending $P(M)$ and then it is encrypted with $Enc$:

- $PEnc(K, M) := Enc(K, (M, P(M)))'$
- $PDec(K, C)$:
  - $(M_1, M_2) := Dec(K, C)$
  - return $M_1$

Prove that

(a) If $(Enc, Dec)$ is $(t, \epsilon)$-semantically secure, then $(PEnc, PDec)$ is $(t, \epsilon)$-semantically secure.

[Hint: you may find it easier to first argue the case in which $P$ is deterministic.]
(b) If \((Enc, Dec)\) is \((t, \epsilon)\) CPA secure, then \((PEnc, PDec)\) is \((t/r, \epsilon)\) CPA secure.

(c) If \((Enc, Dec)\) is \((t, \epsilon)\) CCA secure, then \((PEnc, PDec)\) is \((t/O(r), \epsilon)\) CCA secure.