COMP 655 Homework 1

This homework is due in class on Monday, October 8, 2018. You are allowed to work in teams of two on this assignment, but a “team” of one is also allowed. Each team should hand in a single solution set, with all team members’ names and ONYENS. Collaboration between teams is prohibited, as is consulting material outside of resources provided by the instructor. Please typeset your solutions neatly, and show why they work. Clarity of your solution will factor into your grade.

1. (15 points) Let \( SE = \langle K, E, D \rangle \) be a symmetric encryption scheme. For a bit \( b \in \{0, 1\} \), let \( R(\cdot, b) \) be defined as follows: \( R(x, 1) = x \), and \( R(x, 0) \) selects and returns a random bit string of same length as \( x \). Now consider the experiment, where \( A \) is an algorithm taking one oracle:

\[
\text{Experiment } \text{Expt}_{SE}^{\text{tor-cpa-}b}(A) \\
K \leftarrow K() \\
b' \leftarrow A^{E_{k}(R(\cdot, b))()} \\
\text{return } b'
\]

Define

\[
\text{Adv}_{SE}^{\text{tor-cpa}}(A) = \Pr \left[ \text{Expt}_{SE}^{\text{tor-cpa-}1}(A) = 1 \right] - \Pr \left[ \text{Expt}_{SE}^{\text{tor-cpa-}0}(A) = 1 \right]
\]

and

\[
\text{Adv}_{SE}^{\text{tor-cpa}}(t, q, \mu) = \max_A \{ \text{Adv}_{SE}^{\text{tor-cpa}}(A) \}
\]

where the maximum is taken over all \( A \) running in total time \( t \), making \( q \) oracle queries of total length \( \mu \) to \( E_{k}(R(\cdot, b)) \).

(a) (6 points) Prove that for any \( SE = \langle K, E, D \rangle \),

\[
\text{Adv}_{SE}^{\text{tor-cpa}}(t, q, \mu) \leq \text{Adv}_{SE}^{\text{ind-cpa}}(t', q, \mu)
\]

for \( t' \approx t \).

(b) (9 points) Prove that for any \( SE = \langle K, E, D \rangle \),

\[
\text{Adv}_{SE}^{\text{ind-cpa}}(t, q, \mu) \leq 2 \cdot \text{Adv}_{SE}^{\text{tor-cpa}}(t', q, \mu)
\]

for \( t' \approx t \).

2. (20 points) Let \( g : \{0, 1\}^k \times \{0, 1\}^{2m} \rightarrow \{0, 1\}^m \) be a secure MAC tagging function. Let \( \ell = 2m \) and define \( f : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell \) as follows, where each of \( a_1 \) and \( a_2 \) are \( m \) bits in length and \( || \) denotes concatenation:

\[
\text{Algorithm } f(k, a_1||a_2) \\
\sigma \leftarrow g(k, a_1||a_2) \\
\text{return } \sigma||a_1
\]

(a) (8 points) Prove that

\[
\text{Adv}_{f}^{\text{uf-cma}}(t, q, \mu) \leq \text{Adv}_{g}^{\text{uf-cma}}(t', q, \mu)
\]

for \( t' \approx t \).
(b) (12 points) Let CBC[$f$](\(k, \cdot\)) be a MAC for \(2\ell\)-bit messages (i.e., for two “blocks”) as defined in class, where \(f\) is as defined previously. Show that CBC[$f$](\(k, \cdot\)) is not a secure MAC.

3. (15 points) Recall that we showed in class that CBC-MAC is a secure MAC for fixed-length messages.

   (a) (7 points) Show that it is not secure for variable-length messages.

   (b) (8 points) Consider a variant of CBC-MAC that first appends to the message an extra block that records the message’s length before computing its CBC-MAC as before. The verification function, then, returns “1” only if the last block indicates a length that is consistent with the actual message length. Show that this is not a secure MAC, either.