MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Alternative definition for semantic security). *The standard notion of semantic security is defined through the following games:*

$$
\begin{array}{ll}
\mathcal{G}_0^{\mathcal{A}} & \mathcal{G}_1^{\mathcal{A}} \\
\left[\begin{array}{l}
\mathsf{sk} \leftarrow \mathsf{Gen} \\
\mathcal{M}_0 \leftarrow \mathcal{A}^{\mathsf{Enc}_{\mathsf{sk}}(\cdot)} \\
m \leftarrow \mathcal{M}_0 \\
c \leftarrow \mathsf{Enc}_{\mathsf{sk}}(m) \\
\textbf{\textit{return}}\ [g(m) \stackrel{?}{=} \mathcal{A}(c)]
\end{array}\right.
&
\left[\begin{array}{l}
\mathsf{sk} \leftarrow \mathsf{Gen} \\
\mathcal{M}_0 \leftarrow \mathcal{A}^{\mathsf{Enc}_{\mathsf{sk}}(\cdot)} \\
m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0 \\
\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{sk}}(\overline{m}) \\
\textbf{\textit{return}}\ [g(m) \stackrel{?}{=} \mathcal{A}(\overline{c})]
\end{array}\right.
\end{array}
$$

where the second game $\mathcal{G}_1$ models a very specific attack in the setting where the adversary does not see the encryption of a challenge message. This does not reflect reality close enough as the adversary can perform other more successful attacks in this setting. To capture that we define a new security game

$$
\begin{array}{l}
\mathcal{G}_2^{\mathcal{A}_*} \\
\left[\begin{array}{l}
\mathsf{sk} \leftarrow \mathsf{Gen} \\
\mathcal{M}_0 \leftarrow \mathcal{A}_*^{\mathsf{Enc}_{\mathsf{sk}}(\cdot)} \\
m \leftarrow \mathcal{M}_0 \\
\textbf{\textit{return}}\ [g(m) \stackrel{?}{=} \mathcal{A}_*]
\end{array}\right.
\end{array}
$$

This allows us to define two advantages

$$
\begin{aligned}
\mathsf{Adv}_g^{\mathsf{sem}}(\mathcal{A}) &= \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] \\
\mathsf{Adv}_g^{\mathsf{sem}*}(\mathcal{A}, \mathcal{A}_*) &= \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_2^{\mathcal{A}_*} = 1\right]
\end{aligned}
$$

The cryptosystem is (t, ε)-weakly semantically secure if for any t-time adversaries $\mathcal{A}$ and $\mathcal{A}_*$ the advantage $\mathsf{Adv}_g^{\mathsf{sem}*}(\mathcal{A}, \mathcal{A}_*) \leq \varepsilon$. Prove that semantic security implies weak semantic security for the same function g. Show that for large enough t it is possible to get $\Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] \ll \Pr\left[\mathcal{G}_2^{\mathcal{A}_*} = 1\right]$ for some adversaries $\mathcal{A}$. Does this mean that weak semantic security does not imply semantic security?

Solution.