CSE 5331 Homework 3
Due: Wednesday, February 11 by class time

1. We do not require EAV-secure encryption schemes to hide message length. This question is to show that no EAV-secure encryption scheme with message space $M = \{0,1\}^*$ can hide message length. Specifically, in the original experiment $\text{PrivK}^{\text{ev}}_{A,\Pi}(n)$, the adversary is required to use messages $(m_0, m_1)$ of the same length. Now we want to show that if an encryption scheme can encrypt arbitrary length messages (i.e., message space $M = \{0,1\}^*$) and the adversary is not restricted to use equal length messages, then the scheme cannot have indistinguishable encryptions against eavesdroppers. (Hint: you need to design an adversary $A$ and show $\Pr[\text{PrivK}^{\text{ev}}_{A,\Pi}(n,0) = 1] - \Pr[\text{PrivK}^{\text{ev}}_{A,\Pi}(n,1) = 1]$ to be not negligible. To this end, let $q(n)$ be a polynomial upper-bound on the length of the ciphertext of a single bit. Then consider an adversary $A$ who outputs $m_0, m_1$ with $m_0 \in \{0,1\}$ and $m_1 \in \{0,1\}^{q(n)+2}$.)

2. Design an encryption scheme which is EAV-secure against eavesdroppers even if the adversary is not restricted to output equal length messages. (Hint: Let the message space $M$ be the set of all binary strings of length less than $n$ with a trailing 1.)

3. Prove or refute that $(A_n)_{n \geq 1}$, $(B_n)_{n \geq 1}$ are polynomially indistinguishable, where $A_n = \{0,1\}^n$ and $B_n = A_n - C_n$, where $C_n = \{s \in \{0,1\}^n : s$ has exactly one 1-bit}. 

4. Show that $(A_n)_{n \geq 1}$ and $(B_n)_{n \geq 1}$ are polynomially distinguishable, where $A_n = \{0,1\}^n$ and $B_n = 0 \| \{0,1\}^{n-1}$. (Hint: design a distinguisher $D$ such that $\Pr[D(r) = 1: r \leftarrow A_n] - \Pr[D(r) = 1: r \leftarrow B_n]$ is not negligible.)