CS 127/CSCI E-127: Introduction to Cryptography

Problem Set 2

Assigned: Sep. 13, 2013 Due: Sep. 20, 2013 (5:00 PM)

Problem 1. (Statistical security) Recall that $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ has *statistically ε-indistinguishable encryptions* if for every two $m_0, m_1 \in \mathcal{M}$ and every $T \subseteq \mathcal{C}$,

$$|\Pr[\mathsf{Enc}_K(m_0) \in T] - \Pr[\mathsf{Enc}_K(m_1) \in T]| \leq \varepsilon$$

where the probabilities are taken over $K \xleftarrow{R} \mathsf{Gen}$ and the coin tosses of Enc.

$$|\Pr[\mathsf{Enc}_K(m_0) \in T] - \Pr[\mathsf{Enc}_K(m_1) \in T]| \leq \varepsilon$$