Cryptography: Homework 6
(Deadline: Nov 8, 2018)

1. (20 points) Let X_n be a random variable over $\{0,1\}^n$ for every integer $n \geq 1$. Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a PRG. Show that if $\{X_n\} \equiv_{\text{c.i.}} \{U_n\}$, then $\{G(X_n)\} \equiv_{\text{c.i.}} \{U_{l(n)}\}$.

   (hint: show that $\{G(X_n)\} \equiv_{\text{c.i.}} \{G(U_n)\}$)

2. (20 points) Show that if a one-to-one function f has a hard-core predicate, then f is one-way.