Practice Problems-3: Foundations of Cryptography (Course No: CS60088)

Attempt All Questions

1. Let G be a length preserving pseudorandom generator. Prove that:

$$G'(x_1||\ldots||x_n) = (G(x_1)||G(x_2)||\ldots||G(x_n)),$$

   where $|x_1| = |x_2| = \ldots = |x_n| = n$, is a pseudorandom generator.
2. Let $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ be computationally indistinguishable probability distributions.
   (a) Prove that for any probabilistic polynomial time algorithm $\mathcal{A}$ it holds that $\{\mathcal{A}(X_n)\}_{n\in\mathbb{N}}$ and $\{\mathcal{A}(Y_n)\}_{n\in\mathbb{N}}$ are computationally indistinguishable.
   (b) Consider a pseudorandom function G which has a expansion factor $l(n) = n+1$. Answer the following questions in this regard:
      i. Consider the distributions U_n and U_{n+1}, which indicates the uniform distributions from $\{0,1\}^n$ and $\{0,1\}^{n+1}$. Indicate whether $G(U_n)$ and U_{n+1} are computationally indistinguishable. State reasons for your answer.
      ii. Consider an adversary $\mathcal{B}$ which does not run in polynomial time. Frame an efficient distinguisher $\mathcal{B}$ for the distributions $G(U_n)$ and U_{n+1}.

   Thus, justify that the claim of part (a) may not be true if $\mathcal{A}$ does not run in polynomial time.
3. Let G be a pseudorandom generator with expansion factor $l(n) = n+1$. Prove that G is a one-way function.
   [Hint: Note that the domain of the generator is $\{0,1\}^n$, while the range is $\{0,1\}^{n+1}$]