1. In class, we showed how to build an encryption scheme from a pseudo-random bit generator (PRBG): the key for the encryption scheme is a random seed for the PRBG, and encryption works by stretching the seed using the PRBG, and taking the exclusive-or of this with the message. We proved in class that this encryption scheme is secure if the PRBG is secure. Prove the converse: the PRBG is secure if this encryption scheme is secure. Hint: assume there is an algorithm that breaks the PRBG, and show how to use this to construct an adversary that breaks the encryption scheme.

2. Suppose that we have a pseudo-random bit generator $G = (G, \ell, \ell')$, where for all $\lambda \in \mathbb{N}$ and $s \in \{0, 1\}^{\ell(\lambda)}$, we have $G(1^\lambda, s) \in \{0, 1\}^{\ell'(\lambda)}$. Let $t(\lambda)$ be any poly-time-constructable function in the security parameter, and let us define a new pseudo-random bit generator $\hat{G} = (\hat{G}, t\ell, t\ell')$ as follows: for all $\lambda \in \mathbb{N}$, and all $s_1, \ldots, s_{t(\lambda)} \in \{0, 1\}^{\ell(\lambda)}$, we define

$$\hat{G}(1^\lambda, s_1 \| s_2 \| \cdots \| s_{t(\lambda)}) := G(s_1) \| G(s_2) \| \cdots \| G(s_{t(\lambda)}).$$

Show that if $G$ is a secure PRBG, then so is $\hat{G}$.

3. In class, we showed that if one could effectively distinguish a random bit string from a pseudo-random bit string, then one could succeed in predicting the next bit of a pseudo-random bit string with probability significantly greater than $1/2$ (where the position of the “next bit” was chosen at random). Generalize this from bit strings to strings over the alphabet $\{0, \ldots, n-1\}$, for any $n \geq 2$, assuming that $n$ is a poly-time-constructable function in the security parameter. Hint: first generalize the distinguisher/predictor lemma discussed in class.

4. Suppose that we have a pseudo-random bit generator $G = (G, \ell, \ell')$. For any 0/1-valued, probabilistic, poly-time algorithm $A$, we defined the distinguishing advantage of $A$ to be

$$\text{Dist}_{A}(\lambda) := |\text{SDist}_{A}(\lambda)|,$$

where

$$\text{SDist} := \Pr[s \leftarrow_R \{0, 1\}^{\ell(\lambda)}, s' \leftarrow G(s) : A(s') = 1] - \Pr[s' \leftarrow_R \{0, 1\}^{\ell'(\lambda)} : A(s') = 1].$$

Show that we can effectively turn an “unsigned” advantage into a “signed” advantage. More precisely, show that for every poly-time-constructable function $Q(\lambda)$, there exists a 0/1-valued, probabilistic, poly-time algorithm $A'$, such that the following holds for all $\lambda \in \mathbb{N}$:

$$\text{Dist}_{A}(\lambda) \geq 1/Q(\lambda) \quad \text{implies} \quad \text{SDist}_{A}(\lambda) \geq \text{Dist}_{A}(\lambda) - 2^{-\lambda}.$$