Introduction to Cryptology ENEE459E/CMSC498R: Homework 4

Due by beginning of class on 3/3/2015.

1. Prove the equivalence of Definition 3.8 and Definition 3.9.

2. Let G be a pseudorandom generator with expansion factor $\ell(n) > 2n$. In each of the following cases, say whether G' is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample.

   (a) Define $G'(s) = G(s_1, \ldots, s_{\lceil n/2 \rceil})$, where $s = s_1 \cdots s_n$.

   (b) Define $G'(s) = G(0^{|s|}||s)$.

3. Let G be a pseudorandom generator where $|G(s)| \geq 2 \cdot |s|$.

   (a) Define $G'(s) = G(G(s))$. Is G' necessarily a pseudorandom generator?

   (b) Define $G'(s) = G(s||\overline{s})$, where $\overline{s}$ is the bit-wise negation of s. Is G' necessarily a pseudorandom generator?

   (c) Define $G'(s) = s_1, \ldots, s_{n/2}||G(s_{n/2+1}, \ldots, s_n)$. Is G' necessarily a pseudorandom generator?

   (d) Define $G'(s) = G(s)||G(\overline{s})$, where $\overline{s}$ is the bit-wise negation of s. Is G' necessarily a pseudorandom generator?

4. There are two files on the course webpage rand_1.txt and rand_2.txt. One of these files contains the output (in hexadecimal) of a pseudorandom generator and the other file is not random or pseudorandom. Can you distinguish which file is which? Use the statistical tests provided by NIST here http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html