Problem Set #2

CMSC/Math 456
Instructor: Daniel Gottesman

Due on Gradscope, Tuesday, Sep. 20, noon (before start of class)

Problem #1. Composing Pseudorandom Generators (60 points)

For this problem, let $G(y)$ be an efficiently computable pseudorandom generator with $\ell(s) = 2s$. Recall that G takes inputs of arbitrary length s and outputs bit strings of length $\ell(s)$.

a) (5 points) If $\epsilon(s)$ is negligible, show that $\epsilon(2s)$ is negligible as well.

b) (30 points) Let $G^{(2)}(y) = G(G(y))$, so $G^{(2)}$ takes inputs of length s and outputs bit strings of length $4s$. Show that $G^{(2)}(y)$ is a pseudorandom generator as well.

   Hint: Use a reduction similar to the way we proved in class that the pseudo one-time pad is EAV-secure.

c) (5 points) Let $G^{(k)} = G^{(k-1)}(G(y))$ for $k > 2$. If the input to $G^{(k)}$ is a bit string of length s, how long is the output?

d) (20 points) Let $H(y) = G^{(s)}(y)$ when the length of y is s. Is $H(y)$ a pseudorandom generator? If yes, prove this. If no, find an efficient attack that can distinguish its output from that of a true random number generator, showing it is not a pseudorandom generator.