Homework 3

1. D

2. Construct an attack that shows G is not a prg.

U_n 2^{n+1} PRU 2^n

D(x)

return 1 if last bit of y is 0

return 0 Otherwise

$$Pr[D(r) = 1] = 1/2$$

$$Pr[D(G(s)) = 1] = 1$$

This holds for all n!

$1/2$ is not negligible

Since $x > N$ $\frac{1}{2} < \frac{1}{f(x)}$ for $f(x) = poly$ is not true

3. Define $G_0(s) = G(s_1 \cdots s_{n/2})$ where $s = s_1 \cdots s_n$.

$|G(s)| = 2|s|$

Counter Example $G_0(s_1 \cdots s_{n/2}) =$

$Out = \underbrace{s_1 \cdots s_{n/2}}_{n/2} \underbrace{s_1 \cdots s_{n/2}}_{n/2} \longmapsto$ length $|G_0(s)| = n$

D:

~~Return 1~~ if ~~$Out[0, n/2] == Out[n/2 + 1$~~

By def $|G_0(s)| > |s|$

So $G_0(s)$ is never a PRG

(#4.) Show $n_1 + n_2$ is negligible

Suppose n_1, n_2 is negligible and $n_1 + n_2$ not.

$\exists f(x)$ s.t. $n_1 + n_2 \not< \frac{1}{f(x)}$ for $x > N$

Let $f(x)$ be a polynomial $\Rightarrow \exists N_1, N_2$ s.t.

$n_1(x) < \frac{1}{f(x)}$ for $x > N_1$

$n_2(x) < \frac{1}{f(x)}$ for $x > N_2$

Define $\bar{N} = \max(N_1, N$

Therefore $\exists \bar{N}$ s.t.

$$n_1(x) + n_2(x) < \frac{1}{2f(x)} + \frac{1}{2f(x)} = \frac{2}{2f(x)} = \frac{1}{f(x)}$$

for $x > \bar{N}$.