Задание 3.

CR7. Пусть D_n — это распределение на $\{0,1\}^n$. Семейство распределений $\{D_n\}_{n=1}^{\infty}$ является полиномиально моделируемым, т.е. если существует вероятностный алгоритм S, выходы которого на входе 1^n имеют длину n и распределены согласно D_n. Докажите, что если существует полиномиально вычислимая функция $f : \{0,1\}^* \to \{0,1\}^*$, что для любого полинома p для всех вероятностных полниномиальных по времени алгоритмов A для всех достаточно больших n выполняется $\Pr_{x\in D_n}[A(f(x),1^n) \in f^{-1}(f(x))] < \frac{1}{p(n)}$, то существуют и односторонние в обычном смысле функции.

CR8. Полиномиально вычислимая функция $f : \{0,1\}^* \to \{0,1\}^*$ называется неравномерно односторонней, если для любого полинома p для всех полиномиальных по размеру схем для всех достаточно больших n выполняется $\Pr_{x\in D_n}[(f(x),1^n) \in f^{-1}(f(x))] < \frac{1}{p(n)}$. Докажите, что неравномерно односторонняя функция является и односторонней в обычном смысле.

CR9. Покажите, что если существуют односторонние функции, то существует и такая односторонняя функция, что не один из битов x не является для нее трудным битом.

CR10. Докажите, что если у биективной полиномиально-вычислимой функции, которая сохраняет длину есть трудный бит, то она является сильной односторонней.

CR4 Покажите, что функция $f(xy) = prime(x) + prime(y)$, где x и y — бинарные строки равной длины, а $prime(n)$ — это наименьшее простое число, которое больше, чем n, не является односторонней.