Задание 6.

CR 16. а) Покажите, что если случайные величины α_n и β_n неразличимы полиномиальными схемами (т.е. для любой схемы C полиномиального размера вероятности $C(\alpha_n) = 1$ и $C(\beta_n) = 1$ отличаются пренебрежимо мало), то они и вычислительно неразличимые. б) Покажите, что существуют такие величины α_n и β_n, которые вычислительно неразличимые, но различимы схемами полиномиального размера.

CR 17. Докажите, что если существует $\ell(n)$-псевдослучайный генератор, то для любого многочлена $p(n)$ для всех достаточно больших n для любой строки $\alpha \in \{0,1\}^{\ell(n)}$ выполняется $\Pr_{x \leftarrow U_n}[G(x) = \alpha] < \frac{1}{p(n)}$.

CR 18. Пусть G — это псевдослучайный генератор, а h — это вычислимая за полиномиальное время перестановка. Докажите, что $h(G)$ и $G(h)$ тоже являются псевдослучайными генераторами.

CR 19. а) Покажите, что если существует псевдослучайный генератор, то существует неинъективный псевдослучайный генератор. б) Покажите, что если существует односторонняя перестановка, то существует инъективный $p(n)$-псевдослучайный генератор для любого полинома $p(n)$.