**Задание 5.**

**CR14.** Докажите, что если $f$ — односторонняя перестановка, то $f^{(n^c)}$ (многократная композиция) тоже односторонняя перестановка.

**CR15.** Докажите, что если существует одностороннии функции, то и существует такая односторонняя функция $f$, что для некоторого $c$ функция $f^{(n^c)}$ не является односторонней.

---

**CR11** Пусть $\alpha_n$ и $\beta(n)$ — случайные величины со значениями в $\{0,1\}^{p(n)}$, где $p$ — это полином. Получится ли доказать, что $\alpha_n$ и $\beta_n$ вычислительно неразличимы то последовательность $\sum_{x\in\{0,1\}^{p(n)}} |\Pr[\alpha_n = x] - \Pr[\beta_n = x]|$ пренебрежимо мала?

**CR12** Пусть $\alpha_n$ — это случайная величина со значениями в $\{0,1\}^{p(n)}$, где $p$ — это полином. Говорят, что $\alpha_n$ псевдослучайна по Яо, если для всех $0 \le i \le p(n)-1$ бит $(\alpha_n)_{i+1}$ нельзя предсказать по префиксу $(\alpha_n)_{\le i}$ (т.е. для любого полиномиального вероятностного алгоритма $A$ для любого полинома $q(n)$ выполняется $\Pr[A((\alpha_n)_{\le i}) = (\alpha_n)_{i+1}] \le \frac{1}{2} + \frac{1}{q(n)}$). а) Докажите, что $\alpha_n$ псевдослучайно по Яо величина вычислительно неотличима от $U_{p(n)}$. б) Докажите, что если случайная $\alpha_n$ величина вычислимо неотличима от $U_{p(n)}$, то она псевдослучайна.

**CR13** Докажите, что если существует $(n+1)$-псевдослучайный генератор, то существуют односторонние функции.

**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.