

Задание 4.

CR11. Пусть α_n и $\beta(n)$ — случайные величины со значениями в $\{0, 1\}^{p(n)}$, где p — это полином. Докажите, что α_n и β_n вычислительно неразличимы тогда и только тогда, когда последовательность $\sum_{x \in \{0,1\}^{p(n)}} |\Pr[\alpha_n = x] - \Pr[\beta_n = x]|$ пренебрежимо мала.

CR12. Пусть α_n — это случайная величина со значениями в $\{0, 1\}^{p(n)}$, где p — это полином. Говорят, что α_n псевдослучайна по Яо, если для всех $0 \leq i \leq p(n) - 1$ бит $(\alpha_n)_{i+1}$ нельзя предсказать по префиксу $(\alpha_n)_{\leq i}$ (т.е. для любого полиномиального вероятностного алгоритма A для любого полинома $q(n)$ выполняется $\Pr[A((\alpha_n)_{\leq i}) = (\alpha_n)_{i+1}] \leq \frac{1}{2} + \frac{1}{q(n)}$). а) Докажите, что α_n псевдослучайно по Яо величина вычислительно неотличима от $U_{p(n)}$. б) Докажите, что если случайная α_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 $f(xy) = \text{prime}(x) + \text{prime}(y)$, где x и y — бинарные строки равной длины, а $\text{prime}(n)$ — это наименьшее простое число, которое больше, чем n , не является односторонней.

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