Задание 3. (на 22.02)

Число задач для записи: 3.

CR 12. Покажите, что если существуют односторонние функции, то существует и такая односторонняя функция, что не один из битов x не является для нее трудным битом.

CR 13. Пусть α_n и $\beta(n)$ — случайные величины со значениями в $\{0,1\}^{p(n)}$, где p — это полином. Докажите, что если α_n и β_n статистически неразличимы, то они и вычислительно неразличимы.

CR 14. 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.

CR 15. а) Покажите, что если случайные величины α_n и β_n неразличимы схемными противниками, то неразличимы и равномерными противниками. б) Покажите, что существуют такие величины α_n и β_n, которые вычислительно неразличимые, но различимы схемами полиномиального размера.

CR 16. 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 17. а) Докажите, что если f односторонняя перестановка, то $f^{(n^c)}$ (многократная композиция) тоже односторонняя перестановка. б) Докажите, что если существует одностороннии функции, то и существует такая односторонняя функция f, что для некоторого c функция $f^{(n^c)}$ не является односторонней.

CR 7. 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.