Задание 4. (на 29.02)

Число задач для записи: 2.

CR 18. Покажите, что протокол с открытым ключом и одноразовой надежностью обладает многоразовой надежностью.

CR 19. Пусть (G, E, D) — это протокол с секретным ключом. Противник интересуется результатом функции $f : \{0,1\}^* \to \{0,1\}^*$. Пусть противник применяет к шифру $E(d_n, x)$ семейство схем C_n полиномиального размера. Докажите, что существует такое семейство схем полиномиального размера F_n, что для любой последовательности сообщений x_n вероятность $C_n(E(d_n, x_n)) = f(x_n)$ примерно равна вероятности того, что $F_n(r_n) = f(x_n)$, где случайная величина r_n распределена равномерно.

CR 20. Докажите, что если существует неинтерактивная привязка к биту, то существуют и односторонние функции.

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.

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 $0 \le i \le p(n)-1$ 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 $\Pr[A((\alpha_n)_{\le i}) = (\alpha_n)_{i+1}] \le \frac{1}{2} + \frac{1}{q(n)}$). б) Докажите, что если случайная α_n величина вычислимо неотличима от $U_{p(n)}$, то она псевдослучайна.

CR 15. 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.