Задание 2. (на 15.02)

Число задач для записи: 3.

CR 5. а) Покажите, что если существуют односторонние функции, то существуют односторонние функции $\{0,1\}^{k(n)} \to \{0,1\}^{k(n)}$. б) Покажите, что если существуют односторонние функции, то существуют односторонние функции $\{0,1\}^n \to \{0,1\}^n$.

CR 6. а) Докажите, что если существует односторонние функции, то и существуют односторонние функции $\{0,1\}^n \to \{0,1\}^n$, вычислимые за время $100n^2$ на одноленточной машине Тьюринга. б) Рассмотрим функцию $U_n : (M, x) \mapsto (M, M(x))$, где $M(x)$ — это содержимое первых $100n^2$ ячеек машины M на входе x через $100n^2$ шагов, $|x| = n, |M| = \log n$. Докажите, что если существуют односторонние функции, то U является слабой односторонней. (Детали определения функции U_n предлагается додумать самостоятельно)

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 8. Верно ли, что если f сохраняющая длину односторонняя функция, то $f(x) \oplus x$ тоже односторонняя?

CR 9. Докажите, что односторонняя функция против схемного противника является односторонней и против противника, который является вероятностным алгоритмом.

CR 10. Пусть $cyc_f(x)$ — это минимальное такое число n, что $f^{(n)}(x) = x$. Докажите, что среднее значение cyc_f на строчках длины n не может быть ограничена полиномом от n для слабой односторонней f.

CR 11. Докажите, что если у биективной полиномиально-вычислимой функции, которая сохраняет длину, есть трудный бит, то она является сильной односторонней.