Зачетные задачи по теме "Сложностная криптография"

1. Пусть f — сильно односторонняя функция. Докажите, что для любого вероятностного полиномиального по времени алгоритма A и любого положительного полинома p множество $B_{A,p} = \left\{x \mid \Pr[A(f(x)) \in f^{-1}(f(x))] \geq \frac{1}{p(|x|)}\right\}$ имеет пренебрежимо малую плотность (т.е. последовательность $\frac{|B_{A,p} \cap \{0,1\}^n|}{2^n}$ пренебрежимо мала).

2*. Постройте функцию, которая будет сильно односторонней, если односторонние функции существуют.

3. Полиномимально вычислимая функция $f : \{0,1\}^* \to \{0,1\}^*$ называется распределенной односторонней, если существует такой полином p и для всех полиномиальных по времени вероятностных алгоритмов A и для всех достаточно больших n статистическое расстояние между распределениями $(U_n, f(U_n))$ и $(A(1^n, f(U_n)), f(U_n))$ больше, чем $1/p(n)$. а) Докажите, что f — слабая односторонняя, то она распределенная односторонняя. б) Докажите, что если существуют распределенные односторонние функции, то существуют и односторонние.

!4. а) Пусть X_n и Y_n — два семейства распределений (X_n — распределение на строках длины n). C_n — семейство полиномиальных вероятностных схем. Докажите, что существует такое семейство полиномиальных детерминированных схем D_n, что $\Delta_D(n) \geq \Delta_C(n)$, где $\Delta_F = |\Pr[F_n(X_n) = 1] - \Pr[F_n(Y_n) = 1]|$. б) Покажите, что если случайные величины X_n и Y_n неразличимы полиномиальными схемами (т.е. для любой схемы C полиномиального размера вероятности $C(\alpha_n) = 1$ и $C(\beta_n) = 1$ отличаются пренебрежимо мало), то они и вычислительно неразличимые.

5*. Пусть $G(x)$ — это $(n+1)$-генератор. Докажите, что $G^{(p(n))}$ (многократная композиция) — то $p(n)$-генератор.

!6. Докажите, что если существует схема кодирования с открытым ключом для однобитового сообщения, то существует и схема кодирования с открытым ключом для произвольных сообщений полиномиальной длины.

Правила

- Задачи 4 и 6 обязательны для всех.
- Диме достаточно для зачета решить 4 и 6.
- Грише достаточно для зачета решить 2,4,5,6.
- Всем достаточно для зачета решить 4,6 и три из оставшихся.