Задание 9.

CR24. 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.

CR16 а) Покажите, что если случайные величины α_n и β_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. б) Покажите, что существуют такие величины α_n и β_n, которые вычислительно неразличимые, но различимы схемами полиномиального размера.

CR23 Пусть G — это $2n$-генератор. G_0 и G_1 — это первая и вторая половина выхода. Пусть $s \in \{0,1\}^n$, определим $f_s(x) = G_{s_1}(G_{s_2}(\dots G_{s_n}(x))$, где $x \in \{0,1\}^n$, а $s = s_1 s_2 \dots s_n$. Покажите, что f_s вовсе необязательно является семейством псевдослучайных функций.