Задание 5. (на 14.03)

Число задач для записи: 1.

CR 21. Пусть стратегия F_x разглашает только $f(x)$, а стратегия G_x разглашает только $g(x)$. Докажите, что при последовательном применении стратегия F_xG_x разглашает только $(f(x), g(x))$.

CR 22. Покажите, что если RSA является односторонней функцией, то существует СТОЗ.

CR 15. б) Покажите, что существуют такие величины α_n и β_n, которые вычислительно неразличимые, но различимы схемами полиномиального размера.

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.