Домашнее задание №5 по курсу „Теоретико-сложностные основы криптографии“

сдать к 3 мая 2018 г.

19. Покажите, что если функция Рабина является сильной односторонней, то трудным битом для нее будет четность x, т.е. функция, которая по строке возвращает ее последний бит.

21 б. Покажите, что существуют такие величины α_n и β_n, которые вычислительно неразличимы полиномиальными вероятностными алгоритмами, но различимы схемами полиномиального размера.

29. Объясните, как из семейства псевдослучайных функций (ПСФ) $\{f_n^s\}$, отображающих слова длины n в слова длины n, построить семейство ПСФ, отображающих слова длины n в слова длины $2n$.

30. Докажите, что любой интерактивный протокол привязки к биту можно перестроить так, чтобы алгоритм посылающего в качестве ключа выдавал свои случайные биты и секретный бит.

31. Пусть Алиса и Боб играют в следующую игру: они запускают протокол подбрасывания монетки, результат подбрасывания 0 и $\perp_B$ интерпретируется как выигрыш Алисы, результат подбрасывания 1 и $\perp_A$ интерпретируется как выигрыш Боба.

    а) Покажите, что в предположении, что игроки используют для игры вероятностные схемы полиномиального размера, то у каждого игрока есть стратегия, которая гарантирует выигрыш с вероятностью как минимум $\frac{1}{2} - \epsilon_n$, где ϵ_n пренебрежимо малая последовательность.

    б) Рассмотрим протокол подбрасывания монетки, основанный на неинтерактивной привязки к биту (построенный по хорошей односторонней перестановке). У какого игрока есть выигрышная стратегия, если не ограничивать игроков схемами полиномиального размера?

    в) Аналогичный вопрос, если использовать интерактивный протокол привязки к биту, основанный на генераторе псевдослучайных чисел.

32. Пусть интерактивный алгоритм $F(x)$ разглашает только $f(x)$, а интерактивный алгоритм $G(x)$ разглашает только $g(x)$. Докажите, что при последовательном применении интерактивных алгоритмов $F(x)G(x)$, они разглашают только $(f(x), g(x))$ (см. теорему 8.1).

33. Покажите, что если есть протоколы привязки к строке, то два игрока, играющие в покер по телефону, могут честным образом раздать друг другу по пять карт 5.