Дополнительное домашнее задание по курсу „Теоретико-сложностные основы криптографии“

сдать к 1 мая 2018 г.

1. 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.

2. Пусть α_n — это случайная величина со значениями в $\{0,1\}^{p(n)}$, где p — это полином. Говорят, что α_n псевдослучайна по Яо, если для всех $0 \leq i \leq p(n)-1$ бит $(\alpha_n)_{i+1}$ нельзя предсказать по префиксу $(\alpha_n)_{\leq i}$ (т.е. для любого полиномиального вероятностного алгоритма A для любого полинома $q(n)$ выполняется $\Pr[A((\alpha_n)_{\leq i}) = (\alpha_n)_{i+1}] \leq \frac{1}{2} + \frac{1}{q(n)}$). а) Докажите, что α_n псевдослучайно по Яо величина вычислительно неотличима от $U_{p(n)}$.

3. Докажите, что если случайная α_n величина вычислимо неотличима от $U_{p(n)}$, то она псевдослучайна по Яо.

4. Пусть имеются две схемы шифрования с секретным ключом (с многоразовой надежностью). Изготовим из них новую схему шифрования: ключ в новой схеме состоит из пары ключей для исходных схем, первая половина сообщения шифруется алгоритмом из первой схемы с помощью первого ключа, а вторая половина сообщения — алгоритмом из второй схемы в помощью второго ключа. Аналогичным образом шифрограмма расшифровывается. Докажите, что полученная таким образом схема также удовлетворяет определению схемы шифрования с секретным ключом.

5. Докажите, что существует СТОЗ, если функция RSA является сильно односторонней.

6. Покажите, что если существует семейство псевдослучайных функций $\{0,1\}^n \to \{0,1\}^n$, то существует и семейство псевдослучайных функций $\{0,1\}^* \to \{0,1\}^n$.

7. Покажите, что в протоколе многоразовой подписи идентификатор сообщения можно выбирать не случайным образом, а использовать префиксный код подписываемого сообщения. Таким образом подписывающий алгоритм становится детерминированным.

8. Как модифицировать протокол подписи из предыдущей задачи, чтобы длина подписи не зависела бы от длины сообщения, а зависела бы только от параметра безопасности?

9. Докажите, что существует слабо необратимое семейство всюду определённых функций g_n, не являющаяся сильно необратимым и такое, что функцию g_n можно сузить на некоторое множество, получив сильно необратимое семейство.

10. Пусть случайные величины α_n и β_n вычислительно неотличимы. Докажите, что в результате отрезания от них начала полиномиальной длины получаются вычислительно неотличимые случайные величины.

11. Пусть случайные величины α_n и β_n вычислительно неотличимы, а γ_n произвольная случайная величина, независимая от α_n и β_n. Докажите, что $\alpha_n\gamma_n$ и $\beta_n\gamma_n$ вычислительно неотличимы.

12. Докажите, что если имеется трудный бит вычислимой перестановки $g_n : D_n \to D_n$, то перестановка сильно необратима.