Домашнее задание №1 по курсу „Теоретико-сложностные основы криптографии“

сдать к 22 февраля 2018 г.

1. Покажите, что не существует протокола с секретным ключом и совершенной надежностью, если длина ключа строго меньше длины кодируемого сообщения.

2. Покажите, что если слабые односторонние функции существуют, то P $\neq$ NP.

3. Докажите, что существование инъективной односторонней в наихудшем случае функции эквивалентно P $\neq$ UP. Класс UP состоит из языков L, для которых существует такая недетерминированная полиномиальная по времени машина Тьюринга M, которая принимает язык L и дополнительно для каждого $x \in L$ существует ровно одно принимающее вычисление машины M на входе x.

4. Докажите, что односторонняя функция против схемного противника является односторонней и против противника, который является вероятностным алгоритмом.

5. Докажите, что если существуют односторонние функции, то существует слабая односторонняя, которая не является сильной.

6. Докажите, что а) сильная; б) слабая односторонняя функция не может иметь полиномиально ограниченный размер образа.

7. Пусть $f_n : \{0,1\}^n \to \{0,1\}^n$ является возведением в квадрат по модулю 2^n. Докажите, что f_n не является слабо односторонней даже для равномерного противника.