

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 $2n$.
33. Покажите, что если RSA надёжен, то два игрока, играющие в покер по телефону, могут честным образом раздать друг другу по пять карт 5.
34. Докажите, что алгоритм S в любом протоколе привязки к биту не может быть детерминированным.
35. (Теорема 9.3) Докажите, что если существует одноразовый протокол подписи одного бита, то для любого полинома $p(n)$ существует одноразовый протокол подписи сообщений из $p(n)$ битов.
36. Покажите, что с помощью псевдослучайных функций можно сделать подписывающий алгоритм в протоколе электронной подписи детерминированным.
37. Докажите, что если существует протокол подписи одного бита, то существуют односторонние функции. Верно ли это для одноразового протокола?