Домашнее задание №3 по курсу „Теоретико-сложностные основы криптографии“

сдать к 5 апреля 2018 г.

10. Докажите, что если функция Рабина не является сильно односторонней, то и произведение (определенное на парах n-битных простых чисел) не является сильной односторонней.

12. Покажите, что функция $f(xy) = prime(x) + prime(y)$, где x и y - бинарные строки равной длины, а $prime(n)$ - это наименьшее простое число, которое больше, чем n, не является односторонней.

18. Покажите, что если у полиномиально вычислимой перестановки $f_n : D_n \to D_n$, где $D_n \subseteq \{0,1\}^{k(n)}$ есть трудный бит, то она является сильно односторонней.

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.

20. Пусть $cyc_f(x)$ - это минимальное такое число n, что $f^{(n)}(x) = x$. Докажите, что среднее значение cyc_f на строчках длины n не может быть ограничена полиномом от n для слабой односторонней f.

21. а) Покажите, что если случайные величины α_n и β_n неразличимы схемными противниками, то неразличимы и вероятностными алгоритмами. б) Покажите, что существуют такие величины α_n и β_n, которые вычислительно неразличимы полиномиальными вероятностными алгоритмами, но различимы схемами полиномиального размера.

22. Покажите, что если существуют односторонние функции, то существует и такая односторонняя функция, что не один из битов x не является для нее трудным битом.

23. Докажите, что если существует генератор псевдослучайных чисел $G_n : \{0,1\}^n \to \{0,1\}^{\ell(n)}$, то для любого многочлена $p(n)$ для всех достаточно больших n для любой строки $\alpha \in \{0,1\}^{\ell(n)}$ выполняется $\Pr_{x \leftarrow U_n}[G(x) = \alpha] < \frac{1}{p(n)}$.

24. Докажите утверждение 4.1.