Домашнее задание №2 по курсу „Теоретико-сложностные основы криптографии“

сдать к 15 марта 2018 г.

8. Покажите, что генератор псевдослучайных чисел $G_n : \{0,1\}^n \to \{0,1\}^{2n}$ является сильной односторонней функцией.

9. Проверьте, что функция Рабина является перестановкой на области определения.

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

11. Покажите а) что если существуют односторонние функции, то существуют односторонние функции из $\{0,1\}^{k(n)} \to \{0,1\}^{k(n)}$; что если существуют односторонние функции, то существуют односторонние функции из $\{0,1\}^n \to \{0,1\}^n$.

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.

13. Верно ли, что если f сохраняющая длину односторонняя функция, то $f(x) \oplus x$ тоже односторонняя?

14. Пусть случайные величины α_n, β_n и γ_n имеют совместное распределение. И пусть для любой последовательности значений c_n случайной величины γ_n случайные величины $(\alpha_n \mid \gamma_n = c_n)$ и $(\beta_n \mid \gamma_n = c_n)$ вычислительно неотличимы. Тогда и $\alpha_n\gamma_n$ и $\beta_n\gamma_n$ вычислительно неотличимы.

15. Доказать то же самое для равномерного противника для независимых случайных величин α_n, γ_n, где случайная величина γ_n полиномиально моделируема.

16. Предположим, что существует слабо односторонняя частичная функция. Докажите, что тогда существует и слабо односторонняя всюду определённая функция.

17. Докажите, что определение генератора ПСЧ нельзя усилить, заменив вычислительную неотличимость на статистическую неотличимость.