Московский физико-технический институт
Физтех-школа прикладной математики и информатики
Кафедра дискретной математики
Криптография, осень 2022
Домашние задачи, набор №1

Вам предлагается 9 задач. Срок сдачи — 15 ноября. Каждая задача оценивается в 10 баллов. В зачёт идут 7 наилучшим образом решённых задач, при этом не более 4 среди первых 5 (про односторонние функции) и не более 3 из последних 4 (про псевдослучайные объекты). В отдельных случаях (например, решение задачи или пункта, который больше никто не решил) могут начисляться бонусы сверх этой квоты. Задачи принимаются в письменном виде по почте `musatych@gmail.com` *или в телеграм* `@musatych` *одним файлом в формате PDF. (Желательно набрать решение в TEXe, можно также отсканировать или сфотографировать написанное от руки, собрав всё в PDF. При фотографировании следите за резкостью, контрастностью и балансом белого. Фотографии плохого качества, например, снятые на телефон при слабом освещении, проверяться не будут). Если вы решаете задачи совместно с кем-то, то в работе нужно указать, с кем и в каком объёме вы сотрудничали. При этом собственно тексты решений необходимо записывать самостоятельно. Обнаруженные списанные решения не засчитываются всем авторам. Пороги на экзаменационные оценки будут объявлены позже.*

1. (**Универсальная односторонняя функция**)

а) Докажите, что если односторонние функции существуют, то существует и односторонняя функция, вычислимая за кубическое время.

б) Постройте функцию f со следующим свойством: если односторонние функции существуют, то f односторонняя. (Указание: используйте идею построения универсальной вычислимой функции).

2. (**Гибридизация при помощи чередования битов**) Пусть $f\colon \{0,1\}^n \to \{0,1\}^n$ и $f\colon \{0,1\}^n \to \{0,1\}^n$ — некоторые функции, а $h\colon \{0,1\}^n \to \{0,1\}^n$ определена как комбинация f на нечётных местах и g на чётных местах. Иными словами,

$$h(x)\big|_i = \begin{cases} f(x)\big|_i, & i \not\vdots\ 2; \\ g(x)\big|_i, & i \vdots\ 2. \end{cases}$$

Докажите, что если односторонние функции существуют, то существуют и такие различные сильно односторонние f и g, что:

а) Функция h также сильно односторонняя;

б) Функция h не является даже слабо односторонней;

в) Функция h слабо односторонняя, но не сильно односторонняя.

3. (**Сохранение односторонности при итерации**)

а) Пусть f является односторонней перестановкой. Докажите, что для любого фиксированного c композиция f^{n^c} также является односторонней перестановкой.

б) В предположении, что односторонние функции существуют, постройте одностороннюю функцию (не перестановку), для которой предыдущее утверждение неверно.

4. (**Односторонние функции с неподвижными точками**)

а) Докажите, что если односторонние функции существуют, то существует и такая односторонняя функция f, что $f(0^n) = 0^n$.

б) Пусть $\alpha(n)$ стремится к нулю быстрее любого обратного полинома и вычислима за время $\mathrm{poly}(n)$. Докажите, что если односторонние функции существуют, то существует и такая односторонняя функция f, что $f(x) = x$ для доли x, равной $\alpha(|x|)$.

5. (**Универсальный трудный бит**) Назовём функцию $\beta\colon \{0,1\}^n \to \{0,1\}$ универсальным трудным битом, если β является трудным битом для любой односторонней функции $f\colon \{0,1\}^n \to \{0,1\}^n$. Заметим, что стандартная функция $\beta(x,y) = x \odot y$ является универсальным трудным битом для класса перестановок, имеющих вид $g(x,y) = (f(x),y)$. На самом деле это доказательство работает и для функций f, не являющихся перестановками.

а) Докажите, что если односторонние функции существуют, то для некоторой односторонней функции $g(x,y)$ предикат $\beta(x,y) = x \odot y$ не является трудным битом.

б) Докажите, что если односторонние функции существуют, то никакой предикат $g(x,y)$ не будет являться универсальным трудным битом.

в) Решите предыдущие 2 пункта для односторонних обобщённых перестановок (т. е. таких функций g, что распределение $g(z)$ вычислительно неотличимо от равномерного).

г*) (Бонусный пункт) Решите первые 2 пункта для односторонних перестановок.

6. Докажите, что найдутся случайные величины X_n и Y_n, не отличимые вероятностными полиномиальными алгоритмами, но отличимые схемами полиномиального размера.

7. Пусть G является генератором псевдослучайных чисел. Рассмотрим следующие модификации:

- $G'(s) = 0^{|G(s)|}$, если s содержит ровно $\frac{|s|}{2}$ единиц, и $G'(s) = G(s)$ иначе;
- $G''(s) = 0^{|G(s)|}$, если s содержит ровно $\frac{|s|}{3}$ единиц, и $G''(s) = G(s)$ иначе.

Какие из этих функций являются генераторами псевдослучайных чисел и почему?

8. Пусть генераторы псевдослучайных чисел существуют. Рассмотрим преобразование функций $H'(x) = H(xx)$ (неявная операция — конкатенация). Докажите, что существуют генераторы псевдослучайных чисел G, такие что G' также является генератором, и такие что это неверно.

9. Рассмотрим следующую альтернативную конструкцию семейства псевдослучайных функций. Пусть $G\colon \{0,1\}^n \to \{0,1\}^{2n}$ есть генератор псевдослучайных чисел. Обозначим через G_0 и G_1 его первую и вторую половины. Тогда определим $f_s(x) = G_{\sigma_1}(G_{\sigma_2}(\dots(G_{\sigma_n}(x))\dots))$, где σ_i — биты слова s (по сравнению со стандартной конструкцией s и x поменялись местами). Покажите, что если генераторы псевдослучайных чисел существуют, то существует и генератор, для которого так определённое семейство не будет семейством псевдослучайных функций.