Упражнения по курсу “Современные задачи криптографии”

Юрий Лифшиц

1. (Лекция 1) Какое минимальное количество замков требуется для построения схемы доступа 6 из 11?
2. (Лекция 2) Придумайте протокол раздачи карт для трех игроков, не требующий вычислительной ограниченности участников (абсолютно стойкий)
3. (Лекция 5) Докажите, что IP$\subseteq$PSPACE
4. (Лекция 5) Пусть $N = pq$. Пусть у остатка x символ Лежандра равен 1, т.е. или $x \equiv y^2 \mod N$, или x — квадратичный невычет и по модулю p, и по модулю q. Как с нулевым разглашением доказать, что $x \equiv y^2 \mod N$?
5. (Лекция 6) Рассмотрим две проблемы. Первая: даны три графа G,H,C, такие что $G \ncong H$. Требуется определить, какому из графов G или H не изоморфен C. Вторая: по графам G и H определить, изоморфны они или нет. Докажите, что если первая задача решается за полиномиальное время, то и вторая тоже.
6. (Лекция 7) Пусть есть граф из n вершин, степень каждой вершины не больше трех. Для какой наименьшей функции $f(n)$ всегда можно разбить вершины на две группы по $n/2$ так, чтобы между ними было не более $f(n)$ ребер? Гипотеза: $f(n) = c \cdot n$ для некоторого c Нижние оценки. Можете ли придумать граф, в котором в любом разрезе будет хотя бы $\log n$ ребер? Задача имеет приложения в разработке эффективных алгоритмов
7. (Лекция 8) Постройте протокол для передачи данных вслепую “1-из-4”
8. (Лекция 9) Пусть есть физический источник независимых битов, но вероятности 0 и 1 немного отличаются (неизвестно как). Как получить действительно случайную последовательность?
9. (Лекция 10) Постройте из псевдослучайного генератора $G : B^n \to B^N$ псевдослучайную функцию $F : n \times \log N \to \{0, 1\}$
10. (Лекция 10) Докажите, что если существуют псевдослучайные функции, то псевдослучайные генераторы тоже существуют