Задание на десятую неделю

1. В протоколе RSA выбраны $p = 17$, $q = 23$, $N = 391$, $e = 3$. Выберите ключ d и зашифруйте сообщение 41. Затем расшифруйте полученное сообщение и убедитесь, что получится исходное 41.

2. Пусть в протоколе RSA открытый ключ (N, e), $e = 3$. Покажите, что если злоумышленник узнаёт закрытый ключ d, то он может легко найти разложение N на множители.

3. Схема RSA позволяет также создавать защищенные электронные подписи. Если открытый ключ (N, e), то автор сообщения, обладающий закрытым ключом d, отправляет сообщение A^d, где A — незашифрованное сообщение. После этого идентификация подписи - это возведение в степень e. Пусть открытый ключ $(25, 2021)$. В какую степень автору нужно возвести сообщение, чтобы отправить его за своей электронной подписью?

4 (2 балла). В памяти хранится массив чисел $A[1, \ldots, n]$. Назовем **горкой** элемент $A[i]$, который не меньше обоих своих соседей, если $1 < i < n$, или не меньше своего правого или левого соседа, если $i = 1$ или $i = n$.

а) Постройте как можно более быстрый алгоритм, использующий попарные сравнения, находящий "горку" в A, докажите его корректность и оцените число сравнений.

б) Приведите как можно более точную $\Omega(\cdot)$–оценку числа попарных сравнений, которые должен использовать любой алгоритм, находящий "горку" посредством попарных сравнений.

Чтобы получить полный балл за эту задачу, время работы алгоритма из первого пункта должно соответствовать теоретической нижней оценке, которую нужно получить во втором пункте.

5. Пусть $G(V, E)$ — простой неориентированный граф, множество вершин которого допускает дизъюнктное разбиение на непересекающиеся подмножества $V = S \sqcup T$, такие, что индуцированные подграфы G_S и G_T являются кликами.

Верно ли, что соответствующий язык всех графов, обладающих таким свойством, принадлежит NPC?

По определению, **индуцированный подграф** G_{V_1}, $V_1 \subseteq V(G)$ *имеет вершинами множество* V_1, *а ребрами — все ребра* G *с вершинами из* V_1.

6. Пусть $L = \{(\langle G \rangle, s, t)\}$ — это язык, состоящий из стандартных описаний неориентированных графов G, в которых выделены различные вершины s и t такие, что для любого $S \geq 10$ существует путь из s в t длины S.

Длина пути равна числу рёбер в нем, а в пути допускается повторение вершин и повторение ребер, т. е. можно, например, возвращаться по ребру, по которому только что был сделан переход.

7. Дан неориентированный граф G без петель и кратных рёбер, имеющий m рёбер, которым приписаны положительные веса. Раскрасим вершины в два цвета, **трудностью раскраски** назовем наибольший вес ребра между вершинами одного и того же цвета, а если таких рёбер нет, то трудность раскраски считаем равной нулю.

Постройте и обоснуйте $O(m \log m)$–алгоритм, находящий раскраску с **наименьшей трудностью**.