Расчётно-графическая работа

по теме «Доказательство с нулевым знанием».

Это задание выполняется по вариантам, в зависимости от номера студента в журнале. Для определения номера варианта необходимо взять номер студента в журнале, вычислить его остаток от деления на 3 и прибавить 1.

$$N_{\text{в}} = (N_{\text{ж}} \,\%\, 3) + 1$$

Варианты задания:

1) Необходимо написать программу, реализующую протокол доказательства с нулевым знанием для задачи «Раскраска графа».
2) Необходимо написать программу, реализующую протокол доказательства с нулевым знанием для задачи «Гамильтонов цикл».
3) Необходимо написать программу, реализующую протокол доказательства с нулевым знанием Фиата-Шамира.

Раскраска графа и Гамильтонов цикл

Обе рассматриваемые задачи являются NP-полными и не имеют быстрых методов для решения, поэтому для тестирования необходимо будет генерировать правильные решения при помощи дополнительно разработанных программ.

Вне зависимости от варианта задания, необходимо информацию о графах считывать из файла. В файле описание графа будет определяться следующим образом:

1) в первой строке файла содержатся два числа $n < 1001$ и $m \leq n^2$, количество вершин графа и количество рёбер соответственно;
2) в последующих m строках содержится информация о рёбрах графа, каждое из которых описывается с помощью двух чисел (номера вершин, соединяемых этим ребром);
3) в зависимости от варианта указывается необходимая дополнительная информация: в первом варианте перечисляются цвета вершин графа; во втором варианте указывается последовательность вершин, задающая гамильтонов цикл (этот пункт можно вынести в отдельный файл).

Протокол Фиата-Шамира

Для выполнения этого варианта задания необходимо разработать клиент-серверное приложение с авторизацией по протоколу Фиата-Шамира. Открытые ключи с соответствующими логинами должны храниться в файле

(или базе данных) на сервере, клиентское приложение при этом не должно отправлять на сервер никаких закрытых данных, закрытый ключ нигде не хранится и используется исключительно для осуществления работы протокола с клиентской стороны. Все открытые параметры системы рассылаются сервером при установке соединения с клиентом.

Общие рекомендации

Программа должна наглядно демонстрировать работу алгоритма, возможно (но не обязательно) в графическом режиме. Текст программы должен содержать исчерпывающие комментарии, тем не менее, следует воздержаться от описания очевидных действий. К РГР необходимо представить отчёт, оформленный в соответствии с требованиями, предъявляемыми к работам подобного типа. В отчёт должны быть включены в обязательном порядке: Титульный лист, содержание, постановка задачи, исходный код с комментариями, скриншоты с результатами работы программы.