Задания на лабораторные работы

Общие требования: Все программы должны корректно обрабатывать операции с числами порядка 10^9. Все шифры и подписи должны работать с файлами (т.е. программа должна уметь шифровать или подписывать совершенно любой файл с любым расширением). **Все лабораторные выполняются и защищаются индивидуально.**

Лабораторная работа 1:

Написать криптографическую библиотеку с 4мя основными функциями:

1) Функция быстрого возведения числа в степень по модулю.
2) Функция, реализующая обобщённый алгоритм Евклида. Функция должна позволять находить наибольший общий делитель и обе неизвестных из уравнения.
3) Функция построения общего ключа для двух абонентов по схеме Диффи-Хеллмана
4) Функция, которая решает задачу нахождения дискретного логарифма при помощи алгоритма «Шаг младенца, шаг великана». Трудоёмкость работы функции должна соответствовать описанной в учебники и составлять$O(\mathrm{P} \times \log_2 P)$.

Лабораторная работа 2:

Написать библиотеку, реализующую основные алгоритмы шифрования данных. Обязательно в библиотеке должны присутствовать:

1) Шифр Шамира
2) Шифр Эль-Гамаля
3) Шифр Вернама
4) Шифр RSA

С помощью этой библиотеки необходимо реализовать программу, которая позволит как шифровать, так и расшифровывать любые файлы при помощи описанных выше алгоритмов.

Лабораторная работа 3:

Написать библиотеку, реализующую основные алгоритмы электронной подписи файлов. В библиотеке должны быть представлены алгоритмы:

1) Эль-Гамаля
2) RSA

3) ГОСТ

Программа, написанная с использованием этой библиотеке должна подписывать любой файл (подпись сохранять либо в подписанном файле, либо в отдельном), и уметь проверять подпись. Для вычисления хэш-функции допустимо использовать сторонние библиотеки, однако хэш-функция должна быть не слабее MD5.

Лабораторная работа 4:

Реализация алгоритма «Ментальный покер» для произвольного числа игроков и карт. Для примера использовать правила покера Техасский холдем. Каждому игроку раздать по 2 карты и выложить 5 карт на стол. Обязательно обоснование защищённости и честности предложенной вами схемы. Приветствуется написание нормального графического интерфейса.

Лабораторная работа 5:

Реализация алгоритма «Электронные деньги» из учебника. Обязательно доказательство надёжности предложенной схемы. Необходимо наличие графического интерфейса.

Лабораторная работа 6:

Реализация алгоритма «Доказательство с нулевым знанием». Эта лабораторная выполняется по вариантам. Студенты с чётным номером в списке выполняют задание «Раскраска графа», студенты с нечётным – «Гамильтонов цикл». Граф задаётся в файле в следующем формате:

В первой строке файла два числа n и m – количество вершин и количество рёбер графа соответственно. Числа большие, порядка 10^6. В следующих n строках идёт перечисление рёбер графа в виде двух чисел (номера вершин, которые соединяет ребро). В последней строке задаётся информация, необходимая для варианта. Для гамильтонова цикла – описывается сам цикл, в раскраске графа – задаются цвета каждой вершины (т.е. сама раскраска).