

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 учебнике и составлять $O(P \times \log_2 P)$.

Лабораторная работа 2:

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

- 1) Шифр Шамира
- 2) Шифр Эль-Гамала
- 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-Гамала
- 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 протокола «слепой» подписи на базе системы анонимного голосования. Необходимо разработать программу, в которой разделить серверную и клиентскую часть (хотя бы логически). Данная программа должна на основе выбора пользователя по некоторому голосованию (допустим, пусть будет один вопрос с вариантами ответов {Да, Нет, Воздержался}) формировать бюллетень при помощи алгоритма слепого подписывания, после чего передавать этот бюллетень на сервер, который будет осуществлять проверку корректности бюллетеня. Программа должна быть наглядной, а так же выводить все необходимые для работы системы числа.