Общие требования: все программы должны корректно обрабатывать операции с числами порядка 10^9.

Лабораторная работа №1

Написать криптографическую библиотеку с тремя функциями.

1) Функция быстрого возведения числа в степень по модулю. Данная функция должна позволять находить значение y в уравнении $y = a^x \bmod p$.

2) Функция, реализующая тест простоты Ферма. Функция должна определять, является ли число простым с высокой вероятностью.

3) Функция, реализующая обобщённый алгоритм Евклида. Данная функция должна позволять находить наибольший общий делитель НОД (a, b) и обе неизвестных x, y из уравнения $ax + by =$ НОД (a, b).

Предусмотреть возможности:

- ввода a, b с клавиатуры;
- генерации a, b внутри функции;
- генерации a, b внутри функции таким образом, чтобы a, b являлись простыми числами (с вызовом функции проверки на простоту тестом Ферма).

Лабораторная работа №2

Добавить в криптографическую библиотеку (созданную в Лаб. работе №1) функцию, которая решает задачу нахождения дискретного логарифма при помощи алгоритма «Шаг младенца, шаг великана». Данная функция должна позволять находить значение x в уравнении $y = a^x \bmod p$ при известных a, y, p.

Трудоёмкость работы функции должна соответствовать описанной в учебнике и составлять $O(p \log_2 p)$.

Предусмотреть возможности:

- ввода a, y, p с клавиатуры;
- генерации a, y, p и других параметров внутри функции.

Лабораторная работа №3

Добавить в криптографическую с основными функциями библиотеку (созданную в Лаб. работе №1 и №2) функцию построения общего ключа для двух абонентов по схеме Диффи-Хеллмана.

Предусмотреть возможности:

- ввода p, g, X_A, X_B с клавиатуры;
- генерации p, g, X_A, X_B и других параметров внутри функции.

Лабораторная работа №4

Необходимо реализовать программу, которая позволит как шифровать, так и расшифровывать любые файлы (с любым расширением) при помощи шифра Шамира.

Предусмотреть возможности:

- ввода p, C_A, C_B с клавиатуры;
- генерации p, C_A, C_B, D_A, D_B внутри функции.

Лабораторная работа №5

Необходимо реализовать программу, которая позволит как шифровать, так и расшифровывать любые файлы (с любым расширением) при помощи шифра Эль-Гамаля.

Предусмотреть возможности:

- ввода p, g, C_B с клавиатуры;
- генерации p, g, C_B, D_B и других параметров внутри функции.

Лабораторная работа №6

Необходимо реализовать программу, которая позволит как шифровать, так и расшифровывать любые файлы (с любым расширением) при помощи шифра RSA.

Предусмотреть возможности:

- ввода p, q, D_B с клавиатуры;
- генерации p, q, C_B, D_B и других параметров внутри функции.

Лабораторная работа №7

Необходимо реализовать программу, которая позволит как шифровать, так и расшифровывать любые файлы (с любым расширением) при помощи шифра Вернама.

Предусмотреть возможность генерации ключа K с использованием метода Диффи-Хеллмана.

Лабораторная работа №8

Необходимо написать программу, реализующую алгоритм электронной подписи RSA. Программа должна позволять подписывать любой файл (подпись сохранять либо в подписанном файле, либо в отдельном), и уметь проверять подпись. Для вычисления хеш-функции допустимо использовать сторонние библиотеки, однако хеш-функция должна быть не слабее MD5.

Внимание! Рассматриваемые в Лаб.работах 8-10 алгоритмы подписи предполагают работу с результатом хеш-функции как с одним числом, и это условие действительно будет выполнено, если во всех алгоритмах использовать «длинную арифметику» и работать с числами порядка 1024 бита. Тем не менее, так как требования к лабораторным работам позволяют использовать стандартные типы данных, предлагается следующий подход. Представить значение хеш-фукнции как массив байт, и каждый из этих байт подписать отдельно, применив к нему алгоритм подписи с одними и теми же изначальными параметрами (общие данные, секретный и открытый ключи).

Лабораторная работа №9

Необходимо написать программу, реализующую алгоритм электронной подписи Эль-Гамаля. Программа должна позволять подписывать любой файл (подпись сохранять либо в подписанном файле, либо в отдельном), и уметь проверять подпись. Для вычисления хеш-функции допустимо использовать сторонние библиотеки, однако хеш-функция должна быть не слабее MD5.

Лабораторная работа №10

Необходимо написать программу, реализующую алгоритм электронной подписи ГОСТ Р 34.10-94. Программа должна позволять подписывать любой файл (подпись сохранять либо в подписанном файле, либо в отдельном), и уметь проверять подпись. Для вычисления хеш-функции допустимо использовать сторонние библиотеки, однако хеш-функция должна быть не слабее MD5.

Лабораторная работа №11

Необходимо написать программу, реализующую алгоритм электронной подписи FIPS 186. Программа должна позволять подписывать любой файл (подпись сохранять либо в подписанном файле, либо в отдельном), и уметь проверять подпись. Для вычисления хеш-функции допустимо использовать сторонние библиотеки, однако хеш-функция должна быть не слабее MD5.

Лабораторная работа №12

Необходимо реализовать алгоритм «Ментальный покер» с графическим интерфейсом 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.

Лабораторная работа №13

Необходимо реализовать протокол «слепой» подписи на базе системы анонимного голосования. В программе 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 также выводить все необходимые для работы системы числа.