Лабораторные работы

Рекомендации к выполнению лабораторных работ

ЛАБОРАТОРНАЯ РАБОТА 1. Шифры с открытым ключом

ЛАБОРАТОРНАЯ РАБОТА 2. Шифры с секретным ключом

ЛАБОРАТОРНАЯ РАБОТА 3. Цифровая подпись

ЛАБОРАТОРНЫЕ РАБОТЫ

по дисциплине “Основы криптографии”

Всего требуется выполнить три лабораторных работы, соответствующих трем основным главам лекционного курса. Прежде чем приступать к выполнению очередной лабораторной работы, необходимо изучить соответствующую главу и выполнить хотя бы по одному варианту прилагаемых к ней задач. Задание на лабораторные работы общее для всех *(вариантов нет)*. Каждая последующая лабораторная работа обычно включает в себя наработки из предыдущих работ.

Требования к оформлению отчета

Для проверки лабораторной работы необходимо представить:

1. Файл с текстом программы (программ);
2. Файл с результатами.

Если программа написана в соответствии с заданием, в ней нет ошибок, и получен правильный результат ее работы, то обучающийся получает зачет по данной лабораторной работе. В противном случае работа отправляется на доработку.

В каждой лабораторной работе есть рекомендации к выполнению. Приведенная в них последовательность действий при написании программы, реализующей поставленную задачу, не является единственной и обязательной. Допускается выбор любого языка программирования, позволяющего получать 32-битные исполняемые файлы. Реализация всех алгоритмов выполняется с использованием встроенных типов данных (без применения арифметики длинных чисел). Важно, чтобы целочисленный тип со знаком имел размер 32 бита.

Лабораторная работа №1

Тема: Шифры с открытым ключом (Глава 2)

Задание:

1.Написать и отладить набор подпрограмм (функций), реализующих алгоритмы возведения в степень по модулю, вычисление наибольшего общего делителя, вычисление инверсии по модулю.

2. Используя написанные подпрограммы, реализовать систему Диффи-Хеллмана, шифры Шамира, Эль-Гамаля и RSA, в частности:

2.1. Для системы Диффи-Хеллмана с параметрами $p = 30803$, $g = 2$, $X_A = 1000$, $X_B = 2000$ вычислить открытые ключи и общий секретный ключ.

2.2. Для шифра Шамира с параметрами $p = 30803$, $g = 2$, $c_A = 501$, $c_B = 601$ и сообщения $m = 11111$ вычислить d_A, d_B, x_1, x_2, x_3, x_4.

2.3. Для шифра Эль-Гамаля с параметрами $p = 30803$, $g = 2$, $c = 500$, $k = 600$ и сообщения $m = 11111$ вычислить зашифрованное сообщение.

2.4. Для шифра RSA с параметрами пользователя $P = 131$, $Q = 227$, $d = 3$ и сообщения $m = 11111$ вычислить зашифрованное сообщение.

Лабораторная работа №2

Тема: Шифры с секретным ключом (Глава 4)

Задание:

Выполнить программную реализацию шифра по ГОСТ 28147-89.

Написать программу, которая, используя полученную реализацию шифра, зашифровывает сообщение в режимах ECB, CBC, OFB и CTR (сообщение, режим и ключ задаются при запуске программы).

Написать программу, которая расшифровывает ранее зашифрованное сообщение.

Рекомендации к выполнению:

Зашифрованное сообщение выводить в бинарный файл. Исходный файл так же имеет смысл рассматривать как бинарный.

Лабораторная работа №3

Тема: Цифровая подпись (Глава 5)

Задание:

Разработать программы для генерации и проверки подписей по ГОСТ Р34.10-94. Рекомендуемые значения общих открытых параметров $q = 787$, $p = 31481$, $a = 1928$. Остальные параметры пользователей выбрать самостоятельно. Хеш-функцию реализовать на основе блокового шифра по ГОСТ 28147-89.

Рекомендации к выполнению:

Сообщение брать из файла. Подпись писать в файл с таким же именем, но другим расширением (например, если сообщение в файле `message.doc`, то подпись помещается в файл `message.doc.sign`). Все используемые файлы рассматривать как бинарные (т.е. как потоки произвольных байт).