

Лабораторная работа №14

Применение алгоритмов шифрования данных

1 Цель работы

1.1 Познакомиться с методами применения алгоритмов шифрования данных.

2 Литература

2.1 Зверева В. П., Сопровождение и обслуживание программного обеспечения компьютерных систем : учебник для студ. учреждений сред. проф. Образования / В. П. Зверева, А. В. Назаров. – М. : Издательский центр «Академия», 2018. – 256 с.

3 Подготовка к работе

3.1 Повторить теоретический материал (см. п.2).

3.2 Изучить описание лабораторной работы.

4 Основное оборудование

4.1 Персональный компьютер.

5 Задание

5.1 Разработать оконное приложение-мессенджер для обмена зашифрованными сообщениями со вторым экземпляром приложения (см п.9). Для шифрования сообщений используйте симметричный алгоритм шифрования (например, AES).

5.2 Модифицировать приложение таким образом, чтобы клиентские приложения обменивались зашифрованными сообщениями с использованием ключа шифрования, который должен шифроваться ассиметричным алгоритмом шифрования (например, RSA)

6 Порядок выполнения работы

6.1 Повторить теоретический материал п. 3.1;

6.2 Выполнить задания 5.1-5.2

6.3 Ответить на контрольные вопросы п. 8;

6.4 Заполнить отчет п. 7.

7 Содержание отчета

7.1 Титульный лист;

7.2 Цель работы;

7.3 Ответы на контрольные вопросы п. 6.3;

7.4 Вывод по проделанной работе.

8 Контрольные вопросы

8.1 Перечислите преимущества и недостатки симметричных алгоритмов шифрования.

8.2 Перечислите преимущества и недостатки ассиметричных алгоритмов

шифрования.

9 Приложение

9.1 Схема работы программы:

