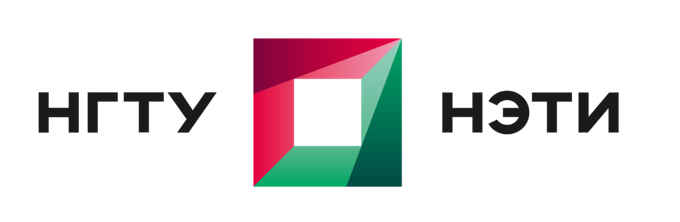
# Министерство науки и Высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное   
учреждение высшего образования

«Новосибирский государственный технический университет»



Кафедра теоретической и прикладной информатики

Лабораторная работа № 4  
по дисциплине «Программные средства защиты информации»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Факультет: | ПМИ |  |  | |
| Группа: | ПМИМ-21 |  |  | |
| Бригада: | 3 | | |  | |
| Студенты: | Бортников. Н, Ефименко А., Кутузова И. | | |  | |
|  |  |  |  | |
| Преподаватель: | Авдеенко Т.В. |  |  | |

Новосибирск

2023

1. **Формулировка задания**

**Задание:**

I. Реализовать приложение для шифрования, позволяющее выполнять следующие действия:

1. Шифровать данные с использованием заданного в варианте режима шифрования, применённого для того симметричного алгоритма, который был реализован в предыдущей лабораторной работе:

1) шифруемый текст должен храниться в одном файле, ключ шифрования – в другом, а вектор инициализации – в третьем;

2) зашифрованный текст должен сохраняться в файл;

3) в процессе шифрования предусмотреть возможность просмотра и изменения ключа, вектора инициализации, шифруемого и зашифрованного текстов в шестнадцатеричном и символьном виде.

2. Шифровать данные по заданной в варианте схеме кратного шифрования.

3. Исследовать лавинный эффект:

1) приложение может самостоятельно строить необходимые графики либо графики можно строить в стороннем ПО, но тогда приложение для шифрования должно сохранять в файл необходимую для построения графиков информацию.

II. Реализовать приложение для дешифрования, позволяющее выполнять следующие действия:

1. Дешифровать данные с использованием заданного в варианте режима шифрования, применённого для того симметричного алгоритма, который был реализован в предыдущей лабораторной работе:

1) зашифрованный текст должен храниться в одном файле, ключ – в другом, а вектор инициализации – в третьем;

2) расшифрованный текст должен сохраняться в файл;

3) в процессе дешифрования предусмотреть возможность просмотра и изменения ключа, вектора инициализации, зашифрованного и расшифрованного текстов в шестнадцатеричном и символьном виде.

2. Дешифровать данные по заданной в варианте схеме кратного шифрования.

III. С помощью реализованных приложений выполнить следующие задания:

1. Протестировать правильность работы разработанных приложений.

2. Исследовать лавинный эффект для реализованного режима шифрования (рассматривать текст из трёх блоков):

1) построить графики зависимости числа изменённых бит в блоках, от позиции изменившегося бита в открытом тексте (3 отдельных графика или 3 зависимости на 1 графике);

2) построить графики зависимости числа изменённых бит в блоках, от позиции изменившегося бита в ключе (3 отдельных графика или 3 зависимости на 1 графике);

3) построить графики зависимости числа изменённых бит в блоках, от позиции изменившегося бита в векторе инициализации (3 отдельных графика или 3 зависимости на 1 графике);

4) построить графики зависимости числа изменённых бит в блоках, от позиции изменившегося бита в зашифрованном тексте (3 отдельных графика или 3 зависимости на 1 графике).

3. Исследовать лавинный эффект для реализованной схемы кратного шифрования (рассматривать текст из 1 блока).

4. Сделать выводы о проделанной работе.

**Вариант 3:**

|  |
| --- |
| Режим шифрования: PCBC |
| Схема кратного шифрования: EDE |

1. **Описание разработанного программного средства**

Решение задачи реализовано в виде программы, написанной на языке C#. Интерфейс, через который осуществляется работа с ней, имеет следующий вид:

1. **Тестирование**

* Тест 1. Шифрование и дешифрование с одним ключом
* Тест 2. Шифрование и дешифрование с двумя ключами
* Тест 3. Шифрование и дешифрование с тремя ключами
* Тест 4. Шифрование и дешифрование с нулевым padding
* Тест 5. Шифрование и дешифрование с единичным padding
* Тест 6. Шифрование и дешифрование со случайным padding
* Тест 7. Шифрование и дешифрование с нулевым вектором инициализации
* Тест 8. Шифрование и дешифрование со случайным вектором инициализации
* Тест 9. Исследование лавинного эффекта для PCBC
  + Тест 9.1 для исходного текста
  + Тест 9.2 для ключа
  + Тест 9.3 для вектора инициализации
  + Тест 9.4 для зашифрованного текста
* Тест 10. Исследование лавинного эффекта для EDE
  + Тест 9.1 для исходного текста
  + Тест 9.2 для ключа
  + Тест 9.3 для вектора инициализации
  + Тест 9.4 для зашифрованного текста

1. **Вывод**

В лабораторной работе мы реализовали приложение, позволяющее шифровать и дешифровать информацию алгоритмом DES с использованием схемы тройного шифрования EDE и режимом шифрования PCBC. Был реализован и проверен лавинный эффект.