**Федеральное государственное бюджетное образовательное учреждение высшего образования "Белгородский государственный технологический университет им. В.Г. Шухова"**

Кафедра программного обеспечения вычислительной техники и автоматизированных систем.

**Лабораторная работа №3**

Объединение блочных шифров.

Выполнил:

Студент группы КБ-211

Коренев Д.Н.

Принял:

Смакаев А.В.

Оглавление

[Задание 3](#_Toc180021098)

[Требования к консольному приложению 4](#_Toc180021099)

[Разработанная программа 5](#_Toc180021100)

[Код программы 6](#_Toc180021101)

[Вывод 9](#_Toc180021102)

*Цель работы:* ознакомится с принципами объединения блочных шифров и алгоритмом 3DES. Разработать консольное приложение, использующее для шифрования и расшифрования алгоритм 3DES.

Задание

1. Разработать консольное приложение, реализующее шифрование/расшифрование файла по алгоритму 3DES EDE (Encrypt-Decrypt-Encrypt) с использованием следующих режимов сцепления блоков:

* 3DES ECB;
* 3DES Inner CBC;
* 3DES Outer CBC;
* 3DES with pad;
* native 3DES (если есть в вашей криптографической библиотеке -<https://pycryptodome.readthedocs.io/en/latest/src/cipher/des3.html>).

Для шифрования использовать три разных ключа. Ключи записывать в файл в бинарном виде без разделителей.

Инициализирующий вектор размером 8 байт также записывать в бинарном виде в отдельный файл.

2. Сравнить производительность алгоритма с каждым режимом сцепления блоков, произведя замеры времени шифрования и расшифрования файлов размером 1МБ, 5МБ, 10МБ, 50МБ, 100МБ. Визуализировать результаты в виде графиков или столбчатых диаграмм.

3. Сделать вывод по полученным данным, соотнести его с информацией о криптостойкости каждого из решений, выбрать оптимальный метод сцепления блоков.

Требования к консольному приложению

Консольное приложение должно иметь три режима:

* генерация ключа;
* шифрование файла;
* расшифрование файла.

Консольное приложение должно принимать на вход следующие аргументы:

* режим работы;
* режим шифрования;
* путь к файлу для шифрования/расшифрования (если требуется);
* путь к файлу для сохранения зашифрованного/расшифрованного файла
* (если требуется);
* путь к файлу с инициализирующим вектором (если требуется);
* путь к файлу с ключом.

Приветствуется использование аргументов командной строки для передачи вышеописанных параметров. Наличие интерактивного режима не обязательно – при его отсутствии или при запуске с неверными аргументами приложение должно показывать инструкцию по использованию.

Ключ для 3DES состоит из трех ключей DES. Для хранения ключа использовать бинарный формат, записывать все три ключа подряд без разделителей.