Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «**Информатика и системы управления**»

КАФЕДРА «**Программное обеспечение ЭВМ и информационные технологии**»

ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

Студент Ковель Александр Денисович

Группа ИУ7-76Б

Предмет Защита информации

Студент		**Ковель А. Д.**
	подпись, дата	*фамилия, и.о.*
Преподаватель		**Чиж И. С.**
	подпись, дата	*фамилия, и.о.*

2023 г.

ВВЕДЕНИЕ

Цель лабораторной работы — разработать программу шифровальной машины «AES» [1].

Задачи лабораторной работы:

1) провести анализ работы шифровальной машина «AES»;
2) описать алгоритм шифрования;
3) релизовать описанный алгоритм.

1 Аналитическая часть

1.1 Алгоритм шифрования AES

AES (Advanced Encryption Standard;) [1] — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES.

Раунды шифрования:

— **Деление на блоки**:в AES элементы организованы в матрицы 4 на 4 по 128 бит. Получается, нас есть сообщение размером 128 бит или 16 байтов в виде матрицы 4 на 4.

— **Наложение фрагмента ключа через XOR**: Сначала функция SubBytes подставляет на место одних байтов другие из таблицы замены (S-блока). Затем ShiftRows сдвигает элементы в каждом ряду матрицы. После этого MixColumns перемешивает элементы в каждом столбце. Первый шаг – это подстановка, второй и третий – перестановка. В конце каждого раунда мы добавляем раундовый ключ (Round Key).

Алгоритм шифрования AES может использоваться в следующих режимах.

1. **PCBC** (Cipher Block Chaining) — режим сцепления блоков;
2. **CBC** (Cipher Block Chaining) — режим сцепления блоков;
3. **CFB** (Cipher Feed Back) — режим обратной связи по шифротексту;
4. **OFB** (Output Feed Back) — режим обратной связи по выходу.

2 Конструкторская часть

2.1 Разработка алгоритма

На рисунке 1 представлена схема алгоритма шифрования AES.

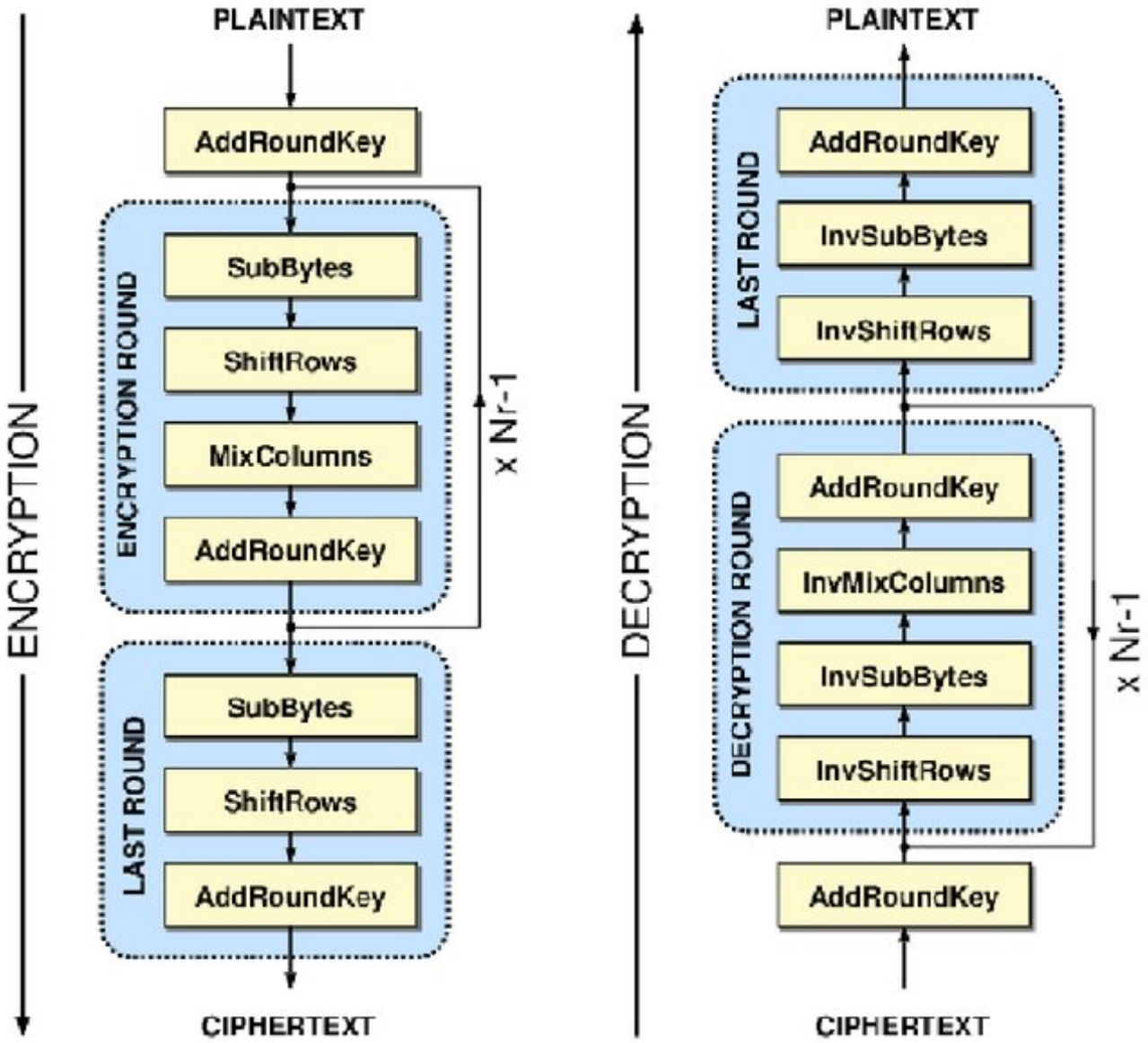

Рисунок 1 – Схемы алгоритма AES

3 Технологическая часть

3.1 Средства реализации

Для реализации ПО был выбран язык C++ [2]. В данном языке есть все требующиеся инструменты для данной лабораторной работы. В качестве среды разработки была выбрана среда VS code [3].

3.2 Реализация алгоритма

Реализация OFB.

```
void encrypt(FILE *inputData, FILE *outputData)
{
    //input list of 16 bytes
    uchar list[16];
    int suffix=0;
    uchar temp=0x00;
    uchar *preC = IV;
    fwrite(preC,16,1,outputData);
    while(fread(list,16,1,inputData)==1)
    {
        unitEncrypt(list, preC);
        fwrite(list,16,1,outputData);
    }

    //encrypt least data, whose length < 128
    while((temp = fgetc(inputData)!=EOF))
    {
        list[suffix++] = temp;
    }

    if(suffix > 0)
    {
        for(int i=suffix; i<16; i++)
        {
            list[i] = 0x00;
        }
        unitEncrypt(list, preC);
        fwrite(list,16,1,outputData);
    }
```

```
        fclose(inputData);
        fclose(outputData);
    }
```

3.3 Тестовые данные

В таблице 1 приведены тесты для алгоритма шифрования AES. Применена методология черного ящика. Тесты пройдены *успешно*.

Таблица 1 – Функциональные тесты

Входная строка	Выходная строка
$ABOBA$	$BCRGJ$
$BCRGJ$	$ABOBA$
$<<>>$	$<<>>$
A	T
T	A

ЗАКЛЮЧЕНИЕ

В данной лабораторной работе:

1) проведен анализ работы шифровальной машина «AES»;
2) описан алгоритм шифрования;
3) реализован описанный алгоритм;

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Список литературы

1. AES. https://electromicro.ru/resources/wiki/aes/aes1/. дата обращения: 17.09.2023.
2. Язык программирования C++. https://learn.microsoft.com/en-us/cpp/cpp/cpp-language-reference?view=msvc-170. дата обращения: 17.09.2023.
3. Vscode. https://code.visualstudio.com/. дата обращения: 17.09.2023.