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, искусственный интеллект и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

ОТЧЕТ

по лабораторной работе № 3

по курсу «Защита Информации»

на тему: «Шифрование симметричным алгоритмом AES»

Вариант № 3

Студент ИУ7-71Б _____ Корниенко К. Ю.
(Группа) (Подпись, дата) (И. О. Фамилия)

Преподаватель _____ Чиж И. С.
(Подпись, дата) (И. О. Фамилия)

2024 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ **3**

1 Аналитический раздел **4**

1.1 Алгоритм шифрования «AES» 4

2 Конструкторская часть **5**

2.1 Разработка алгоритма 5

3 Технологическая часть **6**

3.1 Средства реализации 6

3.2 Реализация алгоритма 6

3.3 Тестирование ПО 7

ЗАКЛЮЧЕНИЕ **10**

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ **11**

ВВЕДЕНИЕ

Цель лабораторной работы — разработать программу, осуществляющую шифрование в соответствии с алгоритмом «AES»

Задачи лабораторной работы:

1. провести анализ алгоритма шифрования «AES»;
2. описать алгоритм шифрования;
3. релизовать описанный алгоритм.

1 Аналитический раздел

1.1 Алгоритм шифрования «AES»

AES (Advanced Encryption Standard) — 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 2.1 представлена схема алгоритма шифрования AES.

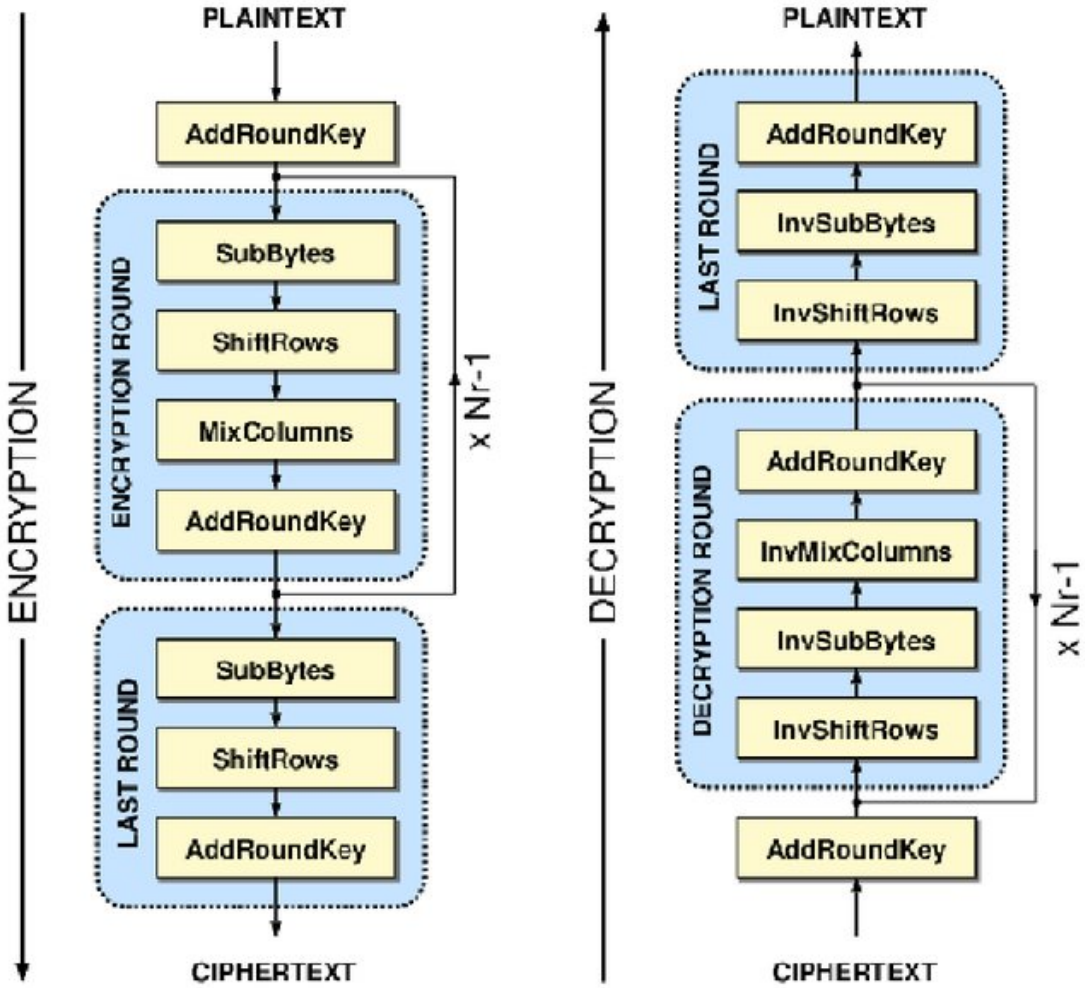

Рисунок 2.1 – Схемы алгоритма AES

3 Технологическая часть

3.1 Средства реализации

Для реализации ПО был выбран язык C++ [1]. В данном языке есть все требующиеся инструменты для данной лабораторной работы. В качестве среды разработки была выбрана среда VS code [2].

3.2 Реализация алгоритма

На листинге ниже приведены алгоритмы шифрования/дешифрования блока, а также методы шифрования и дешифрования текста.

Листинг 3.1 – Алгоритм шифрования блока

```
uint128_t cipher_block(const std::array<uint128_t, 11> &keys,
   uint128_t block)
{
    block ^= keys[0];
    for (int i = 1; i <= 9; i++)
    {
        block = sub_bytes128(block);
        block = shift_rows(block);
        block = mix_columns(block);
        block ^= keys[i];
    }
    block = sub_bytes128(block);
    block = shift_rows(block);
    block ^= keys[10];
    return block;
}
uint128_t decipher_block(const std::array<uint128_t, 11> &keys,
   uint128_t block)
{
    block ^= keys[10];
    block = inv_shift_rows(block);
    block = inv_sub_bytes128(block);
    for (int i = 9; i >= 1; i--)
    {
        block ^= keys[i];
        block = inv_mix_columns(block);
        block = inv_shift_rows(block);
        block = inv_sub_bytes128(block);
```

```
    }
    block ^= keys[0];
    return block;
}

uint128_t AESCryptor::encrypt(uint128_t data)
{
    auto keys = expand_key(key);
    return cipher_block(keys, data);
}

uint128_t AESCryptor::decrypt(uint128_t data)
{
    auto keys = expand_key(key);
    return decipher_block(keys, data);
}
```

3.3 Тестирование ПО

В таблице 3.1 представлены тестовые данные, для проверки корректности работы программы. Применена методология черного ящика. Тесты пройдены *успешно*.

Таблица 3.1 – Функциональные тесты для текстовых файлов

Файл	16-ричный дамп файла	
Ключ	TODO	
Входной файл 1	00000000: 7365 6372 6574 206d 00000008: 6573 7361 6765	secret m essage
Зашифрованный файл 1	00000000: 327b 33f9 248f 9d39 00000008: 655d 73df 265b	2{3.$..9 e]s.&.
Дешифрованный файл 1	00000000: 7365 6372 6574 206d 00000008: 6573 7361 6765	secret m essage
Ключ	TODO	
Входной файл 2	00000000: 3131 3131 3131 3131 00000008: 3131 3131 3131 3131 00000010: 3131 3131 3131 3131 00000018: 3131 3131 3131 310a	11111111 11111111 11111111 1111111.
Зашифрованный файл 2	00000000: d072 b537 61bd e940 00000008: 0e2b 9179 3144 1265 00000010: 31bc 879b cfb7 2268 00000018: 98e6 3535 67f1 2d0a	.r.7a..@ .+.y1D.e 1.....\"h ..55g.-.
Дешифрованный файл 2	00000000: 3131 3131 3131 3131 00000008: 3131 3131 3131 3131 00000010: 3131 3131 3131 3131 00000018: 3131 3131 3131 310a	11111111 11111111 11111111 1111111.

Таблица 3.2 – Функциональные тесты для бинарных файлов

Файл	16-ричный дамп начала файла
Ключ	TODO
Входной файл 3	00000000: 8950 4e47 0d0a 1a0a .PNG.... 00000008: 0000 000d 4948 4452 ....IHDR 00000010: 0000 02c9 0000 02c7 .... 00000018: 0806 0000 007c 3fdf .....|?. ...
Зашифрованный файл 3	00000000: 113d 4afc 85b4 3982 .=J...9. 00000008: a449 000d d9d8 fb52 .I.....R 00000010: 9b78 a44c a200 027f .x.L.... 00000018: 27dd 70aa 0026 4cdf '.p..&L. ...
Дешифрованный файл 3	00000000: 8950 4e47 0d0a 1a0a .PNG.... 00000008: 0000 000d 4948 4452 ....IHDR 00000010: 0000 02c9 0000 02c7 .... 00000018: 0806 0000 007c 3fdf .....|?. ...
Ключ	TODO
Входной файл 4	00000000: 7f45 4c46 0201 0100 .ELF.... 00000008: 0000 0000 0000 0000 .... 00000010: 0300 3e00 0100 0000 ..>..... 00000018: 4011 0000 0000 0000 @....... ...
Зашифрованный файл 4	00000000: 48cb 0cad d4d3 0100 H....... 00000008: a449 00f0 0000 40aa .I....@. 00000010: 0378 3a00 0100 2300 .x:...#. 00000018: 40c4 70aa 0000 d2d7 @.p..... ...
Дешифрованный файл 4	00000000: 7f45 4c46 0201 0100 .ELF.... 00000008: 0000 0000 0000 0000 .... 00000010: 0300 3e00 0100 0000 ..>..... 00000018: 4011 0000 0000 0000 @....... ...

ЗАКЛЮЧЕНИЕ

В данной лабораторной работе:

— проведен анализ работы алгоритма «AES»;

— описан алгоритм шифрования;

— реализован описанный алгоритм.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Josuttis N. M.* The C++ standard library: a tutorial and reference. — 2012.
2. *Code V. S.* Visual studio code // línea]. Available: https://code. visualstudio. com. — 2019.