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 ИУ «Информатика и системы управления»

КАФЕДРА ИУ-7 «Программное обеспечение ЭВМ и информационные технологии»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2

по дисциплине «Защита информации»

«Алгоритм шифрования DES»

Студент группы **ИУ7-76Б** _____ **В. М. Мансуров**
(Подпись, дата) (И.О. Фамилия)

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

2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Шифрование информации — занятие, которым человек занимался ещё до начала первого тысячелетия, занятие, позволяющее защитить информацию от посторонних лиц.

Шифровальная алгоритм DES — алгоритм, разработанный в 1977 году компанией IBM и являющийся официальным стандартом шифрования.

Целью данной работы является реализация в виде программы на языке программирования C или C++ шифровального алгоритма 3DES в режиме работы ECB.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1) изучить шифроовальный алгоритм 3DES и его режим работы ECB;
2) реализовать шифровальный алгоритм 3DES в виде программы, обеспечив возможности шифрования и расшифровки файла в режиме работы ECB;
3) описать и обосновать полученные результаты в отчёте о выполненной лабораторной работе.

1 Аналитическая часть

В этом разделе будут рассмотрен шифровальный алгоритм DES в режиме шифрования ECB.

1.1 Алгоритм DES

Шифровальная алгоритм DES (англ. *Data Encryption Standart* — DES) — симметричный шифровальный алгоритм, разработанный в 1977 году компанией IBM. Он использует блочное шифрование, длина блока фиксирована и равна 64 битам. Однако каждые 8 бит в ключе игнорируются, что приводит к правильной длине ключа 56 бит в DES. Однако в любом случае один блок на 64 бита является вечной организацией DES. Он состоит из 3 следующих шагов, рисунок 1.1:

— начальная перестановка (англ. *Initial Permutation* — IP), во время которой биты переставляются в порядке, определённом в специальной таблице;

— 16 раундов шифрования;

— завершающей перестановки (англ. *Final Permutation* – FP), соовершающей преобразования, обратные сделанным на первом шаге.

Раунд шифрования состоит из 5 следующих этапов

1) расширение (англ. *expansion* — E);
2) получение ключа раунда (англ. *Round Key* – RK);
3) скремблирование (англ. *substitution* — S);
4) перестановка (англ. *permutation* — P)
5) смешивание ключа (англ. *key mixing* — KM).

Рисунок 1.1 – Обобщенная схема шифрования в алгоритме DES

Расширение, во время которого каждая из половин блока шифрования по 32 бит дополняется путём перестановки и дублировоания бит до длины в 48 бит.

Получение ключа раунда необходимо для применения в раунде шифрования 48-битного ключа раунда, полученного из основного ключа DES. Основной ключ имеет длину 64 бита, однако значащих бит из 64 всего 56, остальные добавлены для избыточности и контроля передачи ключа. Из этих 56 бит получают 48 путём разбиения на равные части и применению битовой операции циклического сдвига и нахождению нового значения посредством специальной таблицы.

Скремблирование предназначено для получения из 48-битного потока 32-битного путём разбиения на 6 частей по 8 бит и обработки каждой части в S-блоках (англ. *Substitution boxes*), которые заменяют блоки с длиной 6 бит на блоки 4 бит посредством использования специальной таблицы.

Перестановка представляет из себя перемешивания полученной после-

довательности из 32 бит при помощи таблицы перемешивания.

Смешивание ключа представляет из себя операцию XOR полученного 32-битного значения с ключом раунда.

1.2 Режимы работы алгоритма DES

Режим шифрования — метод применения блочного шифра, позволяющий преобразовать последовательность блоков открытых данных в последовательность блоков зашифрованных данных.

Для DES рекомендованы следующие режими работы:

1) режим электронной кодовой книги (англ. *Electronic Code Bloc* — ECB);
2) режим сцепления блоков (англ. *Cipher Block Chaining* – CBC);
3) режим параллельноого сцепления блоков (англ. *Parallel Cipher Block Chaining* – PCBC);
4) режим обратной связи по шифротексту (англ. *Cipher Feed Back* — CFB);
5) режим обратной связи по выходу (англ. *Output Feed Back* — OFB).

В данной работе будет электронной кодовой книги (ECB).

1.3 3DES

3DES был разработан как более безопасная альтернатива из-за небольшой длины ключа DES. В 3DES алгоритм DES выполняется три раза с тремя ключами, однако он считается безопасным только при использовании трех отдельных ключей.

Существуют 3 типа алгоритма 3DES:

— DES-EEE3: Шифруется три раза с тремя разными ключами;
— DES-EDE3: 3DES операции шифровка-расшифровка-шифровка с тремя разными ключами.

— DES-EEE2: первый и третьей ключ одинаковы, второй отличается от остальных.

1.4 DES-ECB

В этом режиме исходный файл M разбивается на 64-битовые блоки (по 8 байтов): M = M(1)M(2)...M(n). Каждый из этих блоков кодируется независимо с использованием одного и того же ключа шифрования.

Основное достоинство этого алгоритма — простота реализации.

Недостаток — относительно слабая устойчивость против квалифицированных криптоаналитиков.

2 Конструкторская часть

В этом разделе представлена схема алгоритма шифровальной машины «Энигма».

2.1 Разработка алгоритмов

На рисунках 2.1–2.4 представлены схемы алгоритмов DES, раунда DES, функции Фейстеля, а также режимы работы ECB при зашифровке и расшифровке.

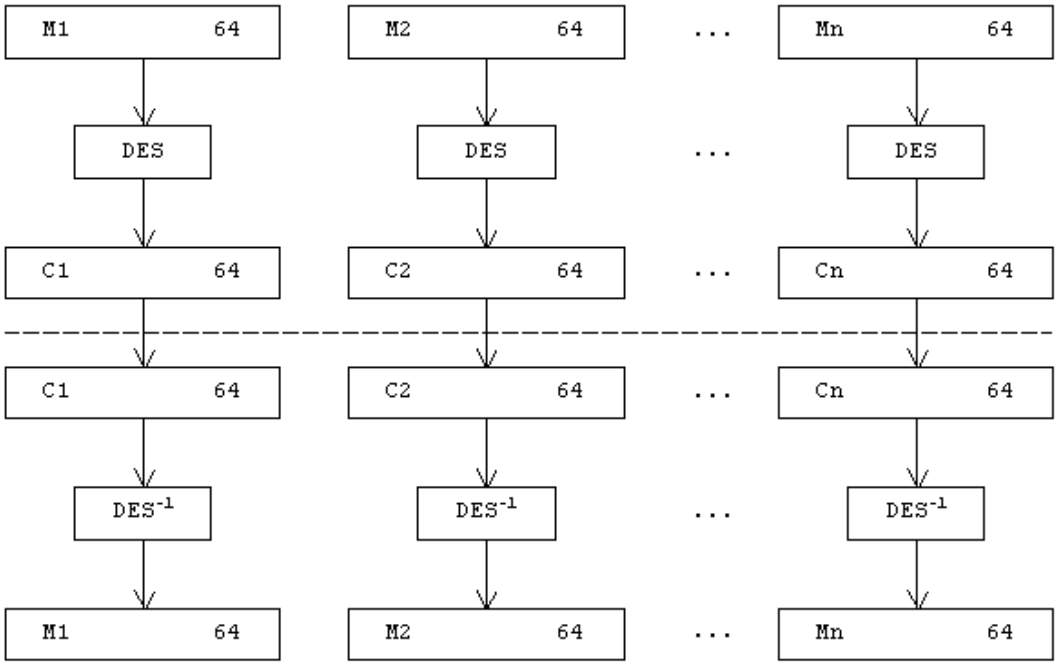

Рисунок 2.1 – Схема алгоритма DES в режиме ECB

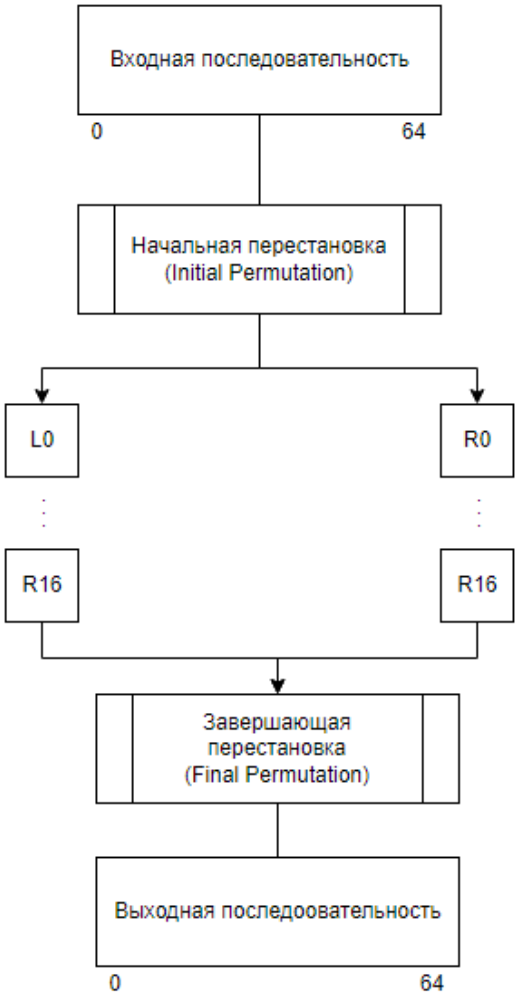

Рисунок 2.2 – Схема алгоритма DES

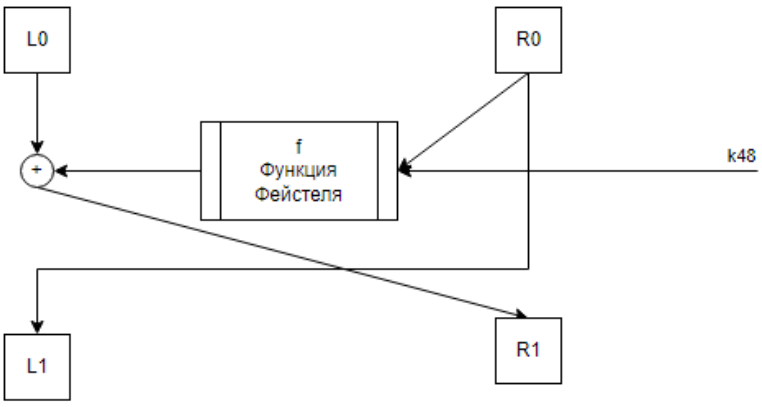

Рисунок 2.3 – Схема алгоритма раунда DES

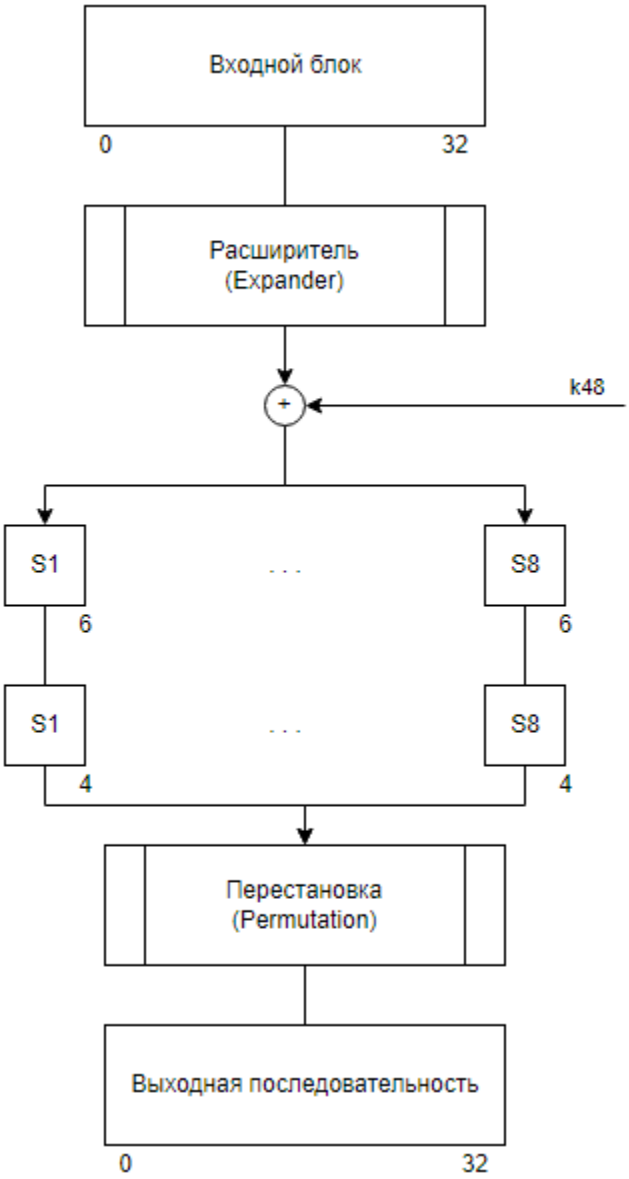

Рисунок 2.4 – Схема алгоритма функции Фейстеля

3 Технологическая часть

3.1 Средства реализации

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

3.2 Реализация алгоритма

Листинг 3.1 – Класс реализации режима ECB

```
1  class ECB {
2  public:
3      ECB() {};
4
5      string cypher(string message, string key, bool decrypt=false);
6      vector<char> cypher(vector<char> message, vector<char> key,
           bool decrypt=false);
7
8  protected:
9      bitset<64> vchar_to_bitset64(vector<char> input);
10
11     vector<char> bitset64_to_vchar(bitset<64> input);
12
13     DES _des;
14 };
```

Листинг 3.2 – Реализация метода шифрования и дешифрования 3DES в режиме ECB

```
ector<char> ECB::cypher(vector<char> input, vector<char> key,
    bool decypher)
{
    vector<char> buffer = {};
    vector<char> result = {};
    int last_cnt = 0;

    if (decypher) {
        last_cnt = input.back();
        input.pop_back();
    }

    auto key_b = vchar_to_bitset64(key);

    for (auto sym : input) {
        if (buffer.size() < 8) {
            buffer.push_back(sym);
        }

        if (buffer.size() == 8) {
            auto buf_b = vchar_to_bitset64(buffer);
            auto tmp_b_1 = _des.process_block(buf_b, key_b,
                decypher);
            auto tmp_b_2 = _des.process_block(tmp_b_1, key_b,
                decypher);
            auto tmp_b_3 = _des.process_block(tmp_b_2, key_b,
                decypher);
            auto tmp_res = bitset64_to_vchar(tmp_b_3);

            result.insert(result.end(), tmp_res.begin(),
                tmp_res.end());

```

```
28                 buffer.clear();
29             }
30         }
31
32         if (!decypher)
33         result.push_back((char)last_cnt);
34
35         if (decypher) {
36             for (int i = 0; i < last_cnt; i++) {
37                 result.pop_back();
38             }
39         }
40
41         return result;
42 }
```

Листинг 3.3 – Реализация алгоритма DES

```
1 bitset<64> DES::process_block(bitset<64> value, bitset<64> key,
      bool decypher)
2 {
3     auto keys = generate_keys(key, decypher);
4
5     auto round_val = IP_f(value);
6
7     for (auto rkey : keys) {
8         round_val = wround(round_val, rkey);
9     }
10
11    auto final_val = FP_f(round_val);
12
13    return final_val;
14 }
```

Вывод

В данном разделе были рассмотрены средства реализации, а также представлены листинги реализации шифровального алгоритма DES и режима работы ECB.

Заключение

В результате лабораторной работы был реализован в виде программы шифровальный алгоритма 3DES в режиме работы ECB

Был и выполнены следующие задачи:

1) изучен шифроовальный алгоритм 3DES и его режим работы ECB;
2) реализован шифровальный алгоритм 3DES в виде программы, обеспечена возможность шифрования и расшифровки файла в режиме работы ECB;
3) описаны и обоснованы полученные результаты в отчёте о выполненной лабораторной работе.

Список использованных источников

1. И.М. Шолин. Алгоритм переносной шифровальной машины энигма. — Кубанский государственный технологический университет.

2. Язык программирования C++. `https://learn.microsoft.com/en-us/cpp/cpp/cpp-language-reference?view=msvc-170`. дата обращения: 15.10.2023.

3. CLion. `jetbrains.com`. дата обращения: 15.10.2023.