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»

Отчет по лабораторной работе №1

по курсу "Защита информации"

Тема Алгоритм работы шифровальной машины “Энигма”

Студент Золотухин А. В.

Группа ИУ7-74Б

Преподаватели Чиж И.С.

Москва, 2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель данной лабораторной работы — реализовать в виде программы аналог шифровальной машины “Энигма”.

Информацию для разных целей пытались засекречивать с помощью шифрования на протяжении всей истории человечества. Шифр — это множество обратимых преобразований открытого текста, проводимых с целью его защиты от несанкционированного использования. Одним из таких шифров является энигма.

В рамках выполнения лабораторной работы необходимо решить следующие задачи:

— описать алгоритм шифровальной машины Энигма;

— реализовать алгоритм.

1 Аналитический раздел

1.1 Шифровальная машина “Энигма”

Шифровальная машина “Энигма” внешне выглядит как печатающая машинка, за исключением того факта, что шифруемые символы не печатаются автоматически на определённый лист бумаги, а указываются на панели посредством загорания лампочки.

Шифровальная машина “Энигма” обладает тремя основными механизмами.

Роторы. Сердце всех шифровальных машин того времени. Со стороны классической криптографии они реализуют полиалфавитный алгоритм шифрования, а их определённо выстроенная позиция представляет собой один из основных ключей шифрования. Каждый ротор не эквивалентен другому ротору, потому как обладает своей специфичной настройкой. Выбор позиций, для вставки роторов, также играл свою роль, потому как образовывал свойство некоммутативности.

Рефлектор (отражатель). Статичный механизм, позволяющий шифровальным машинам типа“Энигма” не вводить помимо операции шифрования дополнительную операцию расшифрования. Нефлектор представляет собой частный случай моноалфавитного шифра — парный шифр, особенностью которого является инволютивность шифрования, где функция шифрования E становится равной функции расшифрования D, иными словами E = D. Это приводит к следующим выводам: если существует сообщение M, то справедливы становятся следующие утверждения D(E(M)) = E(E(M)) = M, E(E(E(M))) = E(M) = D(M).

Коммутаторы. Своеобразный "множитель"возможных вариаций ключей шифрования. Представляет собой также как и рефлектор парный шифр, но в отличие от последнего является динамическим механизмом, то-есть редактируемым и сменяемым. Коммутаторы, можно их рассматривать как некие кабеля, вставляются в коммутационную панель, на которой изображены символы английского алфавита. Один коммутатор имеет два конца, каждый из которых вставляется в два отверстия коммутационной панели. Связь коммутатора с двумя отверствиями, над которыми изображены символы алфавита и представляет собой связь парного шифра между выбранными двумя символами. Так например, если коммутатор был вставлен в два отверстия (Q, D), то это говорит о том, что Q и D стали парными символами при шифровании. На одну шифровальную машину давалось десять коммутаторов, существовало 26 возможных отверстий в коммутационной панели (количество символов алфавита), один коммутатор одновременно связывал два символа такой панели, то-есть все коммутаторы затрагивают в общей сложности 20 отверстий.

Вывод

В данном разделе была рассмотрена логика работы шифровальной машины “Энигма”.

2 Конструкторский раздел

В данном разделе будет представлена схема алгоритма работы шифровальной машины “Энигма”.

2.1 Алгоритм работы шифровальной машины “Энигма”

Схема алгоритма изображена на рисунке 2.1.

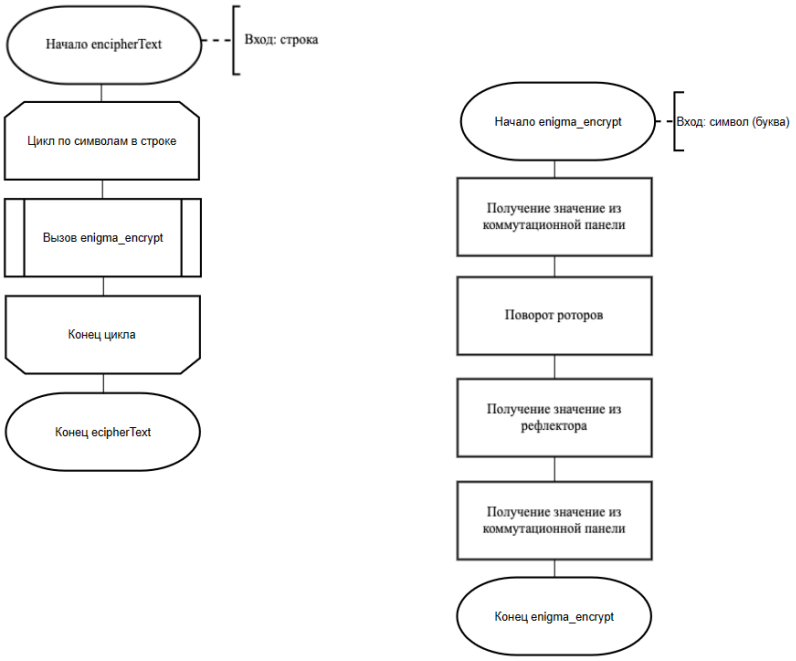

Рисунок 2.1 — Схема алгоритма работы шифровальной машины “Энигма”

Вывод

В данном разделе были приведены схемы алгоритма работы шифровальной машины “Энигма”.

3 Технологический раздел

3.1 Средства реализации

В качестве языка программирования для реализации данной лабораторной работы использовался язык программирования C [1], так как он позволяет работать с файлами и строками. В качестве среды разработки использовалась Visual Studio.

3.2 Реализация алгоритмов

В листингах 3.1, 3.2 представлена реализация алгоритма работы шифровальной машины “Энигма”.

Листинг 3.1 — Структура enigma_t

```
1  typedef struct enigma_t
2  {
3      int counter;
4      int size_rotor;
5      int num_rotors;
6      char* reflector;
7      char* com_panel;
8      char** rotors;
9  } enigma_t;
```

Листинг 3.2 — Реализация алгоритма работы шифровальной машины “Энигма”

```
1  char enigma_encrypt(enigma_t* enigma, char ch, int* rc)
2  {
3      int rotor_queue;
4      char new_ch;
5      if (ch - 'A' >= enigma->size_rotor) {
6          *rc = 0;
7          return 0;
8      }
9      new_ch = enigma->com_panel[ch - 'A'];
10     for (int i = 0; i < enigma->num_rotors; i++)
11         new_ch = enigma->rotors[i][new_ch - 'A'];
12     new_ch = enigma->reflector[new_ch - 'A'];
13     for (int i = enigma->num_rotors - 1; i >= 0; i--)
14     {
15         new_ch = enigma_rotor_find(enigma, i, new_ch, rc);
16         if (*rc != 0)
17             return 0;
18     }
19     new_ch = enigma->com_panel[ch - 'A'];
20     rotor_queue = 1;
```

```
21      enigma->counter += 1;
22      for (int i = 0; i < enigma->num_rotors; i++)
23      {
24          if (enigma->counter % rotor_queue == 0)
25              enigma_rotor_shift(enigma, i);
26          rotor_queue *= enigma->size_rotor;
27      }
28      *rc = 0;
29      return new_ch;
30  }
```

Вывод

В данном разделе были перечислены средства разработки, с помощью которых были реализованы алгоритм работы шифровальной машины “Энигма”, приведена реализация алгоритма.

ЗАКЛЮЧЕНИЕ

В результате выполнения данной лабораторной работы была достигнута цель работы: реализован аналог шифровальной машины “Энигма”.

Были решены все задачи — описан и реализован алгоритм шифровальной машины “Энигма”.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. C language standard ISO/IEC 9899:1999 C99 [Электронный ресурс]. — Режим доступа: `https://www.open-std.org/jtc1/sc22/wg14/www/docs/n1256.pdf` (дата обращения: 01.10.2022).