



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 №1 по курсу «Защита информации»

Тема Шифровальная машина «Энигма»

Студент Калашков П. А.

Группа ИУ7-76Б

Оценка (баллы)

Преподаватели Чиж И. С.

Введение

Шифрование информации — занятие, которым человек занимался ещё до начала первого тысячелетия, занятие, позволяющее защитить информацию от посторонних лиц. Существует большое число шифровальных алгоритмов, таких, как:

- шифр Цезаря;
- шифр Вернана;
- шифр Виженёра.

Шифровальная машина «Энигма» — одна из самых известных шифровальных машин, использовавшихся для шифрования и расшифровывания секретных сообщений.

Целью данной работы является реализация в виде программы на языке программирования С или С++ аналога шифровальной машины «Энигма», обеспечение шифрования и расшифровки файла.

Для достижения поставленной цели необходимо выполнить следующие задачи:

- 1) изучить алгоритм работы шифровальной машины «Энигма»;
- 2) реализовать алгоритм работы шифровальной машины «Энигма» в виде программы, обеспечив возможности шифрования и расшифровки текстового файла;
- 3) описать и обосновать полученные результаты в отчёте о выполненной лабораторной работе, выполненном как расчётно-пояснительная записка к работе, содержащая три раздела: аналитический, конструкторский и технологический.

1 Аналитическая часть

В данной работе будет подразумеваться, что у оператора машины есть выбор из 10 роторов и 2 рефлексоров, а также 10 соединительных проводов для коммутационной панели.

Вот последовательность действий, приводящих к обработке сигнала:

1. Выбор из 10 роторов трёх нужных, из 2 рефлексоров одного, а также настройка коммутационной панели.
2. Нажатие одной из 26 клавиш, обозначающих буквы английского алфавита. Замыкается контакт и отправляется соответствующий нажатой клавише электрический сигнал.
3. Код нажатой клавиши преобразовывается на коммутационной панели в код другой буквы и передаётся дальше.
4. Код полученной буквы складывается по модулю 26 с кодом буквы, стоящей на первом роторе. Это значение отправляется на первый ротор.
5. Осуществляется преобразование на первом роторе.
6. Код полученной после первого ротора буквы складывается по модулю 26 с кратчайшим расстоянием от буквы второго ротора до буквы первого ротора. Это значение отправляется на второй ротор.
7. Осуществляется преобразование на втором роторе.
8. Код полученной после второго ротора буквы складывается по модулю 26 с кратчайшим расстоянием от буквы третьего ротора до буквы второго ротора. Это значение отправляется на третий ротор.
9. Осуществляется преобразование на третьем роторе.
10. Код полученной после третьего ротора буквы вычитается по модулю 26 с значением на третьем роторе. Это значение отправляется на рефлексор.
11. Осуществляется преобразование на рефлексоре. Это значение подаётся на третий ротор с обратной стороны.

12. Код полученной после рефлектора буквы складывается по модулю 26 с значением на третьем роторе. Это значение отправляется на третий ротор с обратной стороны.
13. Осуществляется обратное преобразование на третьем роторе.
14. Код полученной после третьего ротора буквы складывается по модулю 26 с кратчайшим расстоянием от буквы третьего ротора до буквы второго ротора. Это значение отправляется на второй ротор с обратной стороны.
15. Осуществляется обратное преобразование на втором роторе.
16. Код полученной после второго ротора буквы складывается по модулю 26 с кратчайшим расстоянием от буквы второго ротора до буквы первого ротора. Это значение отправляется на первый ротор с обратной стороны.
17. Осуществляется обратное преобразование на первом роторе.
18. Код полученной после первого ротора буквы вычитается по модулю 26 со значением на первом роторе. Это значение отправляется на коммутационную панель.
19. Осуществляется преобразование на коммутационной панели.
20. Первый ротор проворачивается на одну позицию. Если он совершил полный оборот, второй ротор поворачивается на одну позицию. Если второй ротор совершил полный оборот, третий ротор поворачивается на одну позицию.

Вывод

В данном разделе были рассмотрены алгоритм работы шифровальной машины «Энигма», а также её вариант, использованный во время Второй мировой войны, приведён пример преобразования буквы, а также подсчитано количество комбинаций «Энигмы» с 3 роторами.

2 Конструкторская часть

В этом разделе будут представлены описания используемых типов данных, а также схема алгоритма разрабатываемой программы.

2.1 Описание используемых типов данных

При реализации алгоритмов будут использованы следующие типы данных для соответствующих значений:

- матрица — двумерный список символов;
- набор роторов - матрица;
- набор рефлекторов - матрица;
- сообщение - список символов;

2.2 Сведения о модулях программы

Программа состоит из четырёх модулей:

- 1) *main.c* — файл, содержащий точку входа;
- 2) *menu.c* — файл, содержащий код меню программы;
- 3) *rotors.c* — файл, содержащий значения различных роторов и рефлекторов;
- 4) *enigma.c* — файл, содержащий алгоритм шифрации.

2.3 Разработка алгоритмов

На рисунке 2.1 представлена схема работы программы, реализующей шифровальную машину «Энигма».

Алгоритм шифрования предлагается реализовать согласно описанному в аналитическом разделе алгоритму.

3 Технологическая часть

В данном разделе будут рассмотрены средства реализации, а также представлены листинги реализаций алгоритма шифрования машины «Энигма».

3.1 Средства реализации

В данной работе для реализации был выбран язык программирования *C*. Данный язык удовлетворяет поставленным критериям по средствам реализации.

3.2 Реализация алгоритма

В листингах 3.1 представлена реализация алгоритма шифрования машины «Энигма».

Листинг 3.1 – Реализация алгоритма шифрования машины «Энигма»

```
1 char cypher(char let)
2 {
3     if (let == ' ') let = 'X';
4     if (!is_letter(let)) return let;
5     if (let > 'Z') let = let - ('a' - 'A');
6
7     int letter = (int)let;
8
9     letter = commutation[letter - 'A'];
10    letter = ((letter - 'A') + (rotors_positions[0] - 'A')) % 26;
11    letter = rotors[chosen_rotors[0]][letter] - 'A';
12    letter = (letter + (letter_distance(rotors_positions[1],
13    rotors_positions[0]))) % 26;
14    letter = rotors[chosen_rotors[1]][letter] - 'A';
15    letter = (letter + (letter_distance(rotors_positions[2],
16    rotors_positions[1]))) % 26;
17    letter = rotors[chosen_rotors[2]][letter] - 'A';
18    letter = letter - (rotors_positions[2] - 'A');
```

Листинг 3.2 – Реализация алгоритма шифрования машины «Энигма»

```
1  if (letter < 0) letter = 26 + letter;
2
3  letter = reflectors[chosen_reflector][letter] - 'A';
4  letter = (letter + (rotors_positions[2] - 'A')) % 26;
5  letter = find_letter_in_rotor((letter + 'A'), 2);
6  letter = (letter - (letter_distance(rotors_positions[2],
    rotors_positions[1])));
7  if (letter < 0) letter = 26 + letter;
8  letter = find_letter_in_rotor((letter + 'A'), 1);
9  letter = (letter - (letter_distance(rotors_positions[1],
    rotors_positions[0])));
10 if (letter < 0) letter = 26 + letter;
11 letter = find_letter_in_rotor((letter + 'A'), 0);
12 letter = letter - (rotors_positions[0] - 'A');
13 if (letter < 0) letter = 26 + letter;
14 letter = commutation[letter];
15
16 rotate_first_rotor();
17 return (char) letter;
18 }
```

Вывод

Были представлены листинги реализаций всех алгоритмов умножения матриц – стандартного, Винограда и оптимизированного алгоритма Винограда. Также в данном разделе была приведена информации о выбранных средствах для разработки алгоритмов.

Заключение

В результате лабораторной работы были изучены принципы работы шифровальной машины «Энигма», была реализована программа, способная шифровать и дешифровать текстовый файл, позволять настраивать роторы, рефлектор и коммутационную панель.

Были решены следующие задачи:

- 1) изучен алгоритм работы шифровальной машины «Энигма»;
- 2) реализован алгоритм работы шифровальной машины «Энигма» в виде программы, обеспечив возможности шифрования и расшифровки текстового файла;
- 3) полученные результаты описаны в отчёте о выполненной лабораторной работе, выполненном как расчётно-пояснительная записка к работе, содержащая три раздела: аналитический, конструкторский и технологический.