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 Динь Вьет Ань.

Группа ИУ7И-74Б

Оценка (баллы)

Преподаватели Чиж И. С.

Москва — 2023 г.

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 Вернама;

— шифр Виженёра.

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

Целью данной работы является реализация в виде программы на языке программирования C или C++ аналога шифровальной машины «Энигма», обеспечеие 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) протестировать разработанную программу, показать, что удаётся дешфировать все сообщения и получить исходные;

4) 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 этом разделе будут рассмотрены классический 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.

1.1 Основные детали

Шифровальная машина «Энигма» состоит из следующих деталей: роторы, входное колесо, рефлектор, а также коммутационная панель.

1.1.1 Роторы

«Энигма» предназначена для шифрации сообщений, написанных на английском языке. Ротор — прикреплённый к шестерёнке с 26 зубцами (по одному на каждую букву алфавита) элемент, предназначенный для преобразования одной буквы в другую.

В разное время в разных реализациях «Энигмы» использовалось разное количество роторов. Во время Второй мировой войны использовались 3 ротора, причём всего было 10 роторов, преобразовывающих буквы в соответствии с таблицей 1.1.

Таблица 1.1 – Преобразования роторов «Энигмы»

Ротор	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
II	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E
III	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O
IV	E	S	O	V	P	Z	J	A	Y	Q	U	I	R	H	X	L	N	F	T	G	K	D	C	M	W	B
V	V	Z	B	R	G	I	T	Y	U	P	S	D	N	H	L	X	A	W	M	J	Q	O	F	E	C	K
VI	J	P	G	V	O	U	M	F	Y	Q	B	E	N	H	Z	R	D	K	A	S	X	L	I	C	T	W
VII	N	Z	J	H	G	R	C	X	M	Y	S	W	B	O	U	F	A	I	V	L	P	E	K	Q	D	T
VIII	F	K	Q	H	T	L	X	O	C	B	J	S	P	D	Z	R	A	M	E	W	N	I	U	Y	G	V
IX	L	E	Y	J	V	C	N	I	X	W	P	B	Q	M	D	R	T	A	K	Z	G	F	U	H	O	S
X	F	S	O	K	A	N	U	E	R	H	M	B	T	I	Y	C	W	L	Q	P	Z	X	V	G	J	D

1.1.2 Входное колесо

Входное колесо — элемент, позволяющий выставить роторы в необходимые значения. В физической машине было 3 отверстия, позволяющих просматривать, в каком состоянии находится каждый ротор. Положения роторов является ключевым для процесса шифрования, поскольку в зависимости от них одно и то же сообщение будет зашифровано по-разному и будет требовать сответствующих начальных значений роторов для дешифрации.

1.1.3 Рефлектор

Рефлектор — элемент, попарно соединяющий контакты последнего ротора, тем самым направляя ток обратно на последний ротор. Так, после этого электрический сигнал пойдёт в обратном направлении, пройдя через все роторы повторно. Во время Второй мировой войны было создано 2 рефлектора, представленных в таблице

Таблица 1.2 – Преобразования роторов «Энигмы»

Рефлектор	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I	F	V	P	J	I	A	O	Y	E	D	R	Z	X	W	G	C	T	K	U	Q	S	B	N	M	H	L
II	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T

1.1.4 Коммутационная панель

Коммутационная панель позволяет оператору шифровальной машины варьировать содержимое проводов, попарно соединяющих буквы английского алфавита. Эффект состоял в том, чтобы усложнить работу машины, не увеличивая число роторов. Так, если на коммутационной панели соединены буквы 'A' и 'Z', то каждая буква 'A', проходящая через коммутационную панель, будет заменена на 'Z' и наоборот. Сигналы попадали на коммутационную панель 2 раза: в начале и в конце обработки отдельного символа.

1.2 Алгоритм работы

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

Вот последовательность действий, приводящих к обработке сигнала:

1. Выбор из 10 роторов трёх нужных, из 2 рефлекторов 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 рефлектор.

11. Осуществляется преобразование на рефлекторе. Это значение подаётся на третий ротор с обратной стороны.

12. Код полученной после рефлектора буквы складываются по модулю 26 с значением на третьем роторе. Это значение отправляется на третий ротор с обратной стороны.

13. Осуществляется обратное пребразование 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 пребразование 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 пребразование 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.

Рассмотрим пример преобразования буквы 'A' при отсутствии соединений на коммутационной панели, при выборе роторов I, II и III из таблицы 1.1 для первого, второго и третьего ротора соответственно, а также для начальных значений роторов 'R', 'V' и 'C' соответственно:

1. Буква 'A' проходит через коммутационную панель и остаётся буквой 'A'.

2. Код буквы 'A' складывается по модулю с кодом буквы 'R' на первом роторе. Получается буква 'R'.

3. Буква 'R' на первом роторе преобразовывается в букву 'U'.

4. Код буквы 'U' складывается по модулю 26 с кратчайшим расстоянием от буквы 'V' до буквы 'R'. Получается буква 'Y'.

5. Буква 'Y' на втором роторе преобразовывается в букву 'O'.

6. Код буквы 'O' складывается по модулю 26 с кратчайшим расстоянием от буквы 'C' до буквы 'V'. Получается буква 'V'.

7. Буква 'V' на третьем роторе преобразовывается в букву 'M'.

8. Код буквы 'M' вычитается по модулю 26 с кодом буквы 'C'. Получается буква 'K'.

9. Рефлектор преобразовывает букву 'K' в букву 'N'.

10. Буква 'N' складывается по модулю 26 с кодом буквы 'C'. Получается буква 'P'.

11. Буква 'P' на третьем роторе обратно преобразовывается в букву 'H'.

12. Код буквы 'H' вычитается по модулю 26 с кратчайшим расстоянием от буквы 'C' до буквы 'V'. Получается буква 'A'.

13. Буква 'A' на втором роторе обратно преобразовывается в букву 'A'.

14. Код буквы 'A' вычитается по модулю 26 с кратчайшим расстоянием от буквы 'V' до буквы 'R'. Получается буква 'W'.

15. Буква 'W' на первом роторе обратно преобразовывается в букву 'N'.

16. Код буквы 'N' вычитается по модулю 26 с кодом буквы 'R'. Получается буква 'W'.

17. Первый ротор вращается, теперь на нём стоит значение 'C'.

Так, буква 'A' преобразовалась в букву 'W'. Дешифрация сообщений с использованием шфировальной машины «Энигма» осуществляется тем же образом, что и шифрация, только сначала при помощи вводного колеса устанавливается начальное значение роторов. Так, при значениях роторов 'R', 'V' и 'C' соответственно, буква 'W' будет преобразована обратно в букву 'A'.

1.3 Общее число комбинаций

Рассмотрим 3 значения: количество комбинаций роторов в машине, количество комбинаций положений роторов и количество возможных способов соединения проводов на коммутационной панели.

Количество комбинаций роторов будет вычисляться по формуле (1.1).

$$C_{rotors} = 10 \cdot 9 \cdot 8 = 720. \tag{1.1}$$

Количество комбинаций положений роторов будет вычисляться по формуле (1.2).

$$C_{positions} = 26 \cdot 26 \cdot 26 = 17576. \tag{1.2}$$

Количество возможных способов соединения проводов на коммутационной панели будет вычисляться по формуле (1.3).

$$C_{commutation} = \frac{26!}{6! \cdot 10! \cdot 2^{10}} = 150738274937250. \tag{1.3}$$

Итоговое количество комбинаций будет произведением данных трёх параметров и числа 2 (количество комбинаций выбора рефлектора). что будет вычислять по формуле (1.4).

$$C_{total} = 2 \cdot 720 \cdot 17576 \cdot 150738274937250 = 3815101325227832640000. \tag{1.4}$$

Итоговое число комбинаций составляет 3 секстиллиона 815 квинтиллионов 101 квадриллион 325 триллионов 227 миллиардов 832 миллиона 640 тысяч.

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.

Алгоритмы будут получать на вход две матрицы, причём количество столбцов одной матрицы должно совпадать с количеством строк второй матрицы. При вводе пустой матрицы будет выведено сообщение об ошибке. Требуется реализовать программное обеспечение, которое даёт возможность выбрать один из алгоритмов или все сразу, ввести две матрицы и вывести результат их перемножения. Также необходимо провести замеры времени работы реализаций алгоритмов для чётных и нечётных размеров матриц и сравнить результаты, используя графическое представление.

2 Конструкторская часть

В этом разделе будут представлены описания используемых типов данных, а также требования к программе.

2.1 Описание используемых типов данных

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

— набор роторов - одномерный список чисел;

— рефлектор - одномерный список чисел;

— сообщение - список символов;

2.2 Требования к программе

Входными данными программы должен быть файл input.txt, содержащий количество байтов и символьных байтов, которые необходимо зашифровать или дешифровать.

Выходными данными программы является строка символов — результат зашифрования или дешифрования входной строки после использования машины «Энигма».

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 удоволетворяет 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  int main(int argc, char* argv[]) {
2      int stringSize;
3      char *string;
4
5      FILE *f = fopen("input.txt", "rb");
6      if (!f) {
7          printf("Can not open input file.");
8          return 1;
9      }
10
11     if (fscanf(f, "%d\n", &stringSize) != 1) {
12         printf("Can not input size of symbols.");
13         return 1;
14     }
15
16     string = malloc(stringSize);
17     for (int i = 0; i < stringSize; i++) {
18         if (fscanf(f, "%c", &string[i]) != 1) {
19             printf("Can not read symbols.");
```

```
20              return 1;
21          }
22      }
23
24      int scrollCounter = 0;
25      for (int i = 0; i < stringSize; i++) {
26          if (string[i] != ' ') {
27              string[i] = secondSwitch(
28                  secondFastRotorEncoding(
29                  secondMiddleRotorEncoding(
30                  secondSlowRotorEncoding(
31                  getReflectedChar(
32                  firstSlowRotorEncoding(
33                  firstMiddleRotorEncoding(
34                  firstFastRotorEncoding(
35                  firstSwitch(string[i])
36                  ))))))));
37              scrollCounter++;
38              scrollFastRotor();
39              if (scrollCounter % 26 == 0)
40                  scrollMiddleRotor();
41              if (scrollCounter % (26 * 26) == 0)
42                  scrollSlowRotor();
43          }
44      }
45
46      for (int i = 0; i < stringSize; i++) printf("%c", string[i]);
47      printf("\n");
48  }
```

Вывод

Были представлены листинги реализаций алгоритма шифрования в машине «Энигма» согласно алгоритму, представленному в первой части, а также проведено тестирование разработанной программы.

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) полученная программа протестирована, произведена демонстрация того, что во всех случаях сообщение удаётся дешифровать и получить исходное;

4) полученные результаты описаны в отчёте о выполненной лабораторной работе, выполненном как расчётно-пояснительная записка к работе, содержащая три раздела: аналитический, конструкторский и технологический.