Министерство образования Республики Беларусь

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет к лабораторной работе № 3:

«Изучение устройства и функциональных особенностей шифровальной машины “Энигма”»

Выполнила:

студентка 3 курса 2 группы

Шастовская М. С.

Вариант: 12

Преподаватель:

Сазонова Д.В.

Минск 2023

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации подстановочно-перестановочных шифров.

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-перестановочных шифров.
* Изучить структуру, принципы функционирования, реализацию процедур зашифрования сообщений в машинах семейства «Энигма».
* Изучить и приобрести практические навыки выполнения криптопреобразований информации на платформе «Энигма», реализованной в виде симуляторов.
* Получить практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе «Энигма».
* Результаты выполнения лабораторной работы оформить в виде отчета о проведенных исследованиях, методике выполнения практической части задания и оценке криптостойкости шифров.

1 Теоретические сведения

Машина «Энигма» – это электромеханическое устройство. Как и другие роторные машины, «Энигма» состоит из комбинации механических и электрических подсистем.

Механическая часть включает в себя клавиатуру, набор вращающихся дисков – роторов, которые расположены вдоль вала и прилегают к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу.

Электрическая часть, в свою очередь, состоит из электрической схемы, соединяющей между собой клавиатуру, коммутационную панель, лампочки и роторы (для соединения роторов использовались скользящие контакты).

«Энигма» состоит из 5 основных блоков:

Панели механических клавиш (дают сигнал поворота роторных дисков).

Трех (или более) роторных дисков, каждый имеет контакты по сторонам, по 26 на каждую, которые коммутируют в случайном порядке; по окружности нанесены буквы латинского алфавита либо числа.

Рефлектора (имеет контакты с крайним слева ротором).

Коммутационной панели (служит для того, чтобы дополнительно менять местами электрические соединения (контакты) двух букв).

Панели в виде электрических лампочек; индикационная панель с лампочками служит индикатором выходной буквы в процессе шифрования.

Конкретный механизм мог быть разным, но общий принцип был таков: при каждом нажатии на клавишу самый правый ротор сдвигался на одну позицию, а при определенных условиях сдвигались и другие роторы. Движение роторов приводило к различным криптографическим преобразованиям при каждом следующем нажатии на клавишу на клавиатуре, т. е. зашифрование/расшифрование сообщений основано на выполнении ряда замен (подстановок) одного символа другим. Идея А. Шербиуса состояла в том, чтобы добиться этих подстановок электрическими связями.

Механические части двигались и, замыкая контакты, образовывали меняющийся электрический контур. При нажатии на клавишу клавиатуры контур замыкается, ток проходит через созданную (для зашифрования/расшифрования одного конкретного символа сообщения) цепь и в результате включает одну из набора лампочек, отображающую искомую букву шифртекста (или расшифрованного сообщения).

2 Практическая часть

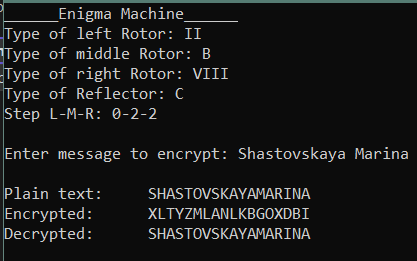


Рисунок 2.1 – Результат шифрования/дешифрования исходного сообщения машиной «Энигма»

На данном скриншоте отображен процесс работы программы с шифрованием и дешифрованием исходного сообщения машиной «Энигма». Так же выведена информация об шифровальном устройстве.

Основные функции программы представлены на рисунке 2.2.

private void rotateRotors(Rotor[] r)

{

if (r.Length == 3)

{

if (r[1].isInTurnOver())

{

r[0].step(rightPosition);

r[1].step(centerPosition);

}

else if (r[2].isInTurnOver())

{

r[1].step(centerPosition);

}

r[2].step(leftPosition);

}

}

private char encryptChar(char c)

{

rotateRotors(rotors);

if (plugBoard.ContainsKey(c))

{

c = plugBoard[c];

}

c = rotorMap(c, false);

c = reflectorMap(c);

c = rotorMap(c, true);

if (plugBoard.ContainsKey(c))

{

c = plugBoard[c];

}

return c; }

Рисунок 2.2 – Основные функции программы

Вывод

В ходе выполнения лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации подстановочно-перестановочных шифров.