УДК 003.26.09

«Анализ и моделирование работы шифровальной машины Энигма»

М. В. Билошицкий, ГБОУ Лицей 144, Санкт-Петербург.

Научный руководитель – научный сотрудник, Э.О. университет ИТМО, Санкт-Петербург.

В работе представлено исследование работы шифровальной машины Энигма и реализована ее симуляция на языке программирования C#.

Enigma - переносная трехроторная шифровальная машина, использовавшаяся для шифрования и расшифровывания секретных сообщений. В машине имелось три отсека для помещения трех роторов и дополнительный отсек для размещения рефлектора. Как только оператор нажимал на нужную букву, — замыкалась электрическая цепь, в результате чего появлялась зашифрованная буква. Замыкание цепи происходило за счет рефлектора. Отдельно ротор представлял собой кольцо, имеющее 26 сечений, что соответствовало отдельной букве алфавита, а также 26 контактов для взаимодействия с соседними роторами. Внутри ротора находилось 26 проводов, переплетенных между собой и каждый провод соответствовал замене одной буквы алфавита на другую, а на какую именно, это уже соответствовало конфигурации ротора, как нам известно, их было создано 8 типов, все они по структуре были одинаковы и отличались лишь тем, какие буквы они заменяют внутри себя. То есть каждый ротор выполнял четкую поставленную себе задачу по коммуникации. Такой алгоритм шифрования обладает высокой степенью безопасности. Число всех возможных комбинаций шифрования у Энигмы – 158 квинтиллионов 962 квадриллиона 555 триллионов 217 миллиардов 826 миллионов 360 тысяч.

Для симуляции шифровальной машины Enigma был реализован каркас программы:

1. 26 кнопок, каждая из которой соответствует своей букве в алфавите.
2. 3 показателя положений роторов и кнопки для их смены.
3. 26 меток, которые будут осуществлять работу лампочек для вывода зашифрованных букв.
4. Текстовое поле, в котором будут отображаться входные данные.
5. Текстовое поле, в котором будет отображаться выходные данные.
6. Кнопка стирания последнего набранного символа и отката сдвига ротора на 1 позицию одновременно
7. Кнопка стирания всего текстового поля, с откатом сдвигов роторов на количество, равное количеству символов в строке.
8. Кнопка для копирования зашифрованного сообщения в буфер обмена компьютера.
9. Кнопка вставки сообщения из буфера обмена компьютера во входное текстовое поле для шифрования сообщения.
10. Кнопка, открывающая окно с настройкой коммутационной панели.
11. Кнопка, открывающая окно с настройками, в которых можно осуществить выбор типа роторов и рефлекторов, и разместить их в определённые отсеки.
12. Кнопка, открывающая окно с визуализацией алгоритма шифрования каждой буквы.
13. Кнопка, при нажатии на которую происходит случайная настройка конфигурации Энигмы.
14. Кнопка замены вида роторов с буквенного, на числовой.
15. Кнопка, которая открывает окно с сохранением конфигурации Энигмы в один файл, для дальнейшей загрузки с него.

Далее был написан алгоритм сдвига, создана визуализация коммутационной панели и реализован основной алгоритм шифрования. Симулятор дает возможность выбора одного из пяти вписанных в код программы роторов, для заполнения одного отсека, также можно выбрать тип рефлектора. Панель визуализацией алгоритма шифрования, заключает в себе отображения замены всех отсеков, типов роторов и четкий путь, который проходила буква.

Программа допускает добавление возможности ввода с клавиатуры, проверки на недопустимые символы и написание обработчика событий для каждого компонента, в том числе для кнопок очистки текстового поля, кнопок работы с буфером обмена и исправление абсолютно всех исключений и ошибок программы в коде, для корректной ее работы и использования.