Министерство образования Республики Беларусь

Учреждение образование

«Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

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

Выполнил:

студент 3 курса 8 группы ФИТ

Ярмолик Николай Сергеевич

Проверил:

Берников В. О.

Минск 2020

**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, состояла 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, 1 (дают сигнал поворота роторных дисков);
* трех (или более) роторных дисков, 2, каждый имеет контакты по сторонам, по 26 на каждую, которые коммутируют в случайном порядке; по окружности нанесены буквы латинского алфавита либо числа;
* рефлектора, 3 (имеет контакты с крайним слева ротором);
* коммутационной панели, 4 (служит для того, чтобы дополнительно менять местами электрические соединения (контакты) двух букв);
* панели в виде электрических лампочек, 5; 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 сдвигается на одну позицию, а при определённых условиях сдвигаются и другие роторы. Движение роторов приводит 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). Замыкание цепи происходило за счет рефлектора.

**1.1 Шифры Энигмы**

Среди шифров рассматриваемого подкласса иногда выделяют *шифры простой перестановки* (или *перестановки без ключа*). Символы открытого текста *Мi* перемешиваются по каким-либо правилам. Формально каждое из таких правил может рассматриваться в качестве ключа.

*Пример 1*. Простейшим примером является запись открытого текста в обратной последовательности. Так, если *Мi* = «шифр перестановки», то С*i* = «иквонатсереп рфиш». Если переставляются в соответствующем порядке пары букв, то *Сi* = «киованстрепе фрши». При более длинных сообщениях можно таким же образом перемещать целые слова или блоки слов.

Подобную перестановку можно трактовать как *транспозицию*.

В общем случае для использования *шифров одинарной перестановки* используется таблица, состоящая из двух строк: в первой строке, записываются буквы, во второй – цифры *J*. Строки состоят из *n* столбцов. Буквы составляют шифруемое сообщение. Цифры *J* = *j*1, *j*2, …, *jn*, где *j*1 – номер позиции в зашифрованном сообщении первого символа открытого текста, где *j*2 – номер позиции в зашифрованном сообщении второго символа открытого текста и т. д. Таким образом, порядок следования цифр определяется используемым правилом (ключом) перестановки символов открытого текста для получения шифрограммы.

**1.2 Оценка криптостойкости Энигмы**

Чтобы оценить криптостойкость шифра, нужно учитывать все возможные настройки машины. Для этого необходимо рассмотреть следующие свойства Энигмы:

* выбор и порядок роторов,
* разводку (коммутацию) роторов,
* настройку колец на каждом из роторов,
* начальное положение роторов в начале сообщения,
* отражатель,
* настройки коммутационной панели.

Используются различные варианты подсчета всех возможных состояний перечисленных конструктивных модулей машины. К сожалению, для немцев, взломщики шифра союзников знали машину, роторы и внутреннюю разводку этих роторов. Поэтому им нужно было учитывать только возможные способы настройки Энигмы. Такая априорная информация о конструктивных особенностях устройства для шифрования (вспомним об основных постулатах О. Керкгоффса) в нашем случае снижает уровень (теоретический) крипто-стойкости (до практического). Немецкие криптологи полагали, что один ротор может быть подключен 4 х 1026 различными способами. Сочетание трех роторов и отражателя позволяет получить астрономические цифры возможных вариантов подстановок. Для союзников, которые знали конструкции роторов, число различных вариантов существенно уменьшалось.

Рассмотрим пример для трехроторной Энигмы Вермахта с отражателем (по умолчанию – B, см. рис. 4.6) и выбором из 5 роторов. Использовались 10 штекерных кабелей на коммутационной панели (количество кабелей по умолчанию, поставляемых с машиной).

Чтобы выбрать 3 ротора из возможных 5, существует 60 комбинаций (5 х 4 х 3). Каждый ротор (его внутренняя проводка) может быть установлен в любом из 26 положений. Следовательно, с 3 роторами имеется 17 576 различных положений ротора (26 x 26 x 26). Кольцо на каждом роторе содержит маркировку ротора (что здесь неважно) и выемку, которая влияет на шаг перемещения расположенного левее ротора. Каждое кольцо может быть установлено в любом из 26 положений. Поскольку слева от третьего (наиболее левого) ротора нет ротора, на расчет влияют только кольца самого правого и среднего ротора. Это дает 676 комбинаций колец (26 х 26).

Коммутационная панель обеспечивает самый большой набор возможных настроек. Для первого кабеля одна сторона может иметь любое из 26 положений, а другая сторона - любое из 25 оставшихся положений (одна буква коммутируются с другой). Однако, поскольку комбинация и ее обратная сторона идентичны (AB такая же, как BA), мы должны игнорировать все двойные числа во всех возможных комбинациях для одного кабеля, предоставляя (26 x 25) / (1! х 21) или 325 уникальных способов коммутаций одним кабелем. Для двух кабелей: есть (26 x 25) комбинаций – для первого кабеля и, поскольку два разъема уже используются, то получается (24 x 23) комбинаций – для второго кабеля. Следуя этой простой логике, получается (26 x 25 x 24 x 23) / (2! X 22) = 44 850 уникальных способов коммутаций с использованием двух кабелей. Для трех кабелей – (26 x 25 x 24 x 23 x 22 x 21) / (3! х 23) = 3 453 450 комбинаций и так далее. Таким образом, с использованием 10 кабелей на коммутационной панели получаются 150 738 274 937 250 различных комбинаций. Формула, где *n* равно количеству кабелей, равна 26! / (26 - 2*n*)! · *n*! · 2*n*. Численно это дает: 60 x 17 576 x 676 x 150 738 274 937 250 = 107 458 687 327 250 619 360 000 или 1,07 x 1023.

Таким образом, практически рассматриваемая версия Энигмы (три ротора с выбором из 5 роторов, отражатель В и 10 штекерных кабелей для коммутационной панели) может быть настроена на 1,07 x 1023 различных состояний, что сопоставимо с 77-битным криптографическим ключом.

Добавление четвертого ротора (например, для *Naval Enigma M4*) для повышения его криптостойкости было практически бесполезным: неподвижный четвертый ротор «усложнил машину» только в 26 раз и вместе с тонким отражателем мог рассматриваться как настраиваемый отражатель с 26 положениями. Внедрение общего числа роторов в 8 единиц (на *Kriegsmarine M3*), а затем – на четырехроторной версии (*M4*) было гораздо более эффективным шагом. Они увеличили комбинации роторов с 60 до 336.

Оценим далее практический размер криптографического ключа (или его эквивалент) для четырехроторной версии *Krigsmarine Enigma M4*. Эта машина использует 3 обычных ротора, выбранных из набора из 8. Это, как мы уже отметили, дает 336 комбинаций подключений роторов (8 х 7 х 6). *M4* также имела специальный четвертый ротор, называемый *Beta* или *Gamma* (без кольца), который дает 2 варианта. Они не совместимы с другими роторами и подходят только как четвертый (самый левый) ротор. Четыре ротора могут быть установлены в любом из 456 976 положений (26 x 26 x 26 x 26). Рефлектор не меняется. Четвертый ротор был неподвижным. Версия *М4* была снабжена также 10 кабелями для коммутационной панели.

В сумме это дает: 336 x 2 x 456 976 x 676 x 150 738 274 937 250 = = 31 291 969 749 695 380 357 632 000 или 3,1 x 1025, *что сопоставимо с 84-битным ключом*.

Проблема криптоанализа шифров Энигмы была экстраординарной (с учетом электромеханических конструкций устройств для криптоанализа, приме-няемых в то время). Исчерпывающий поиск всех возможных 1,07 x 1023 настроек (атака *brute force*) был невозможен в 1940-х годах, а его сопоставимый 77-битный ключ огромен даже для современных электронных систем. Чтобы дать представление о размере этого числа, представим, что у нас есть 1,07 x 1023 листов бумаги толщиной около 1 мм. Из этих листов можно сложить примерно 70 000 000 стопок бумаги, каждая из которых простирается от Земли до Солнца. Кроме того, 1,07 x 1023 дюйма равно 288 500 световых лет.

**2 Практическая часть**

В данной лабораторной работе необходимо было произвести зашифрование сообщения (собственные имя, отчество, фамилия) при 8-10 различных настройках машины-симулятора. Оценить частотные свойства символов в шифртекстах и сравнить этот параметр с частотными свойствами символов для исходного текста. В результате была описана таблица для 8 различных настроек машины-симулятора (Рисунок 2.1).

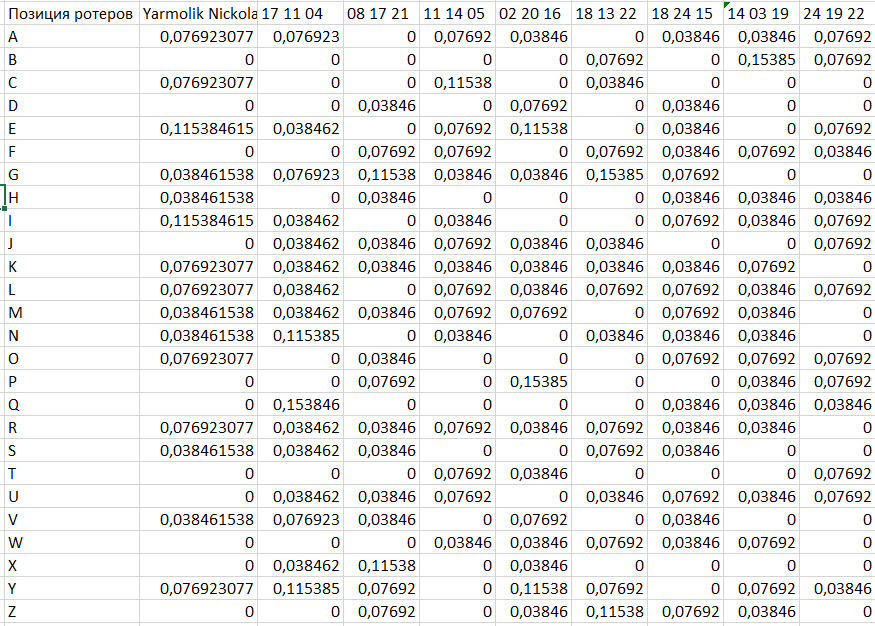


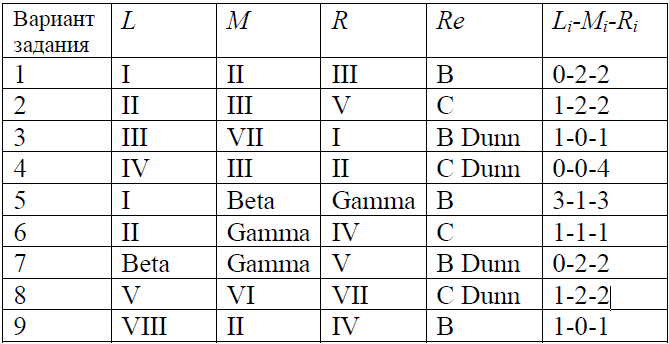
Рисунок 2.1 *–* Частотная таблица символов

Общий интерфейс эмулятора Энигмы приведен на рисунке (Рисунок 2.2).



Рисунок 2.2 – Общий интерфейс эмулятора Энигмы

В соответствии с вариантом также требовалось разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Таблица характеристик согласно 12 варианту приведена на рисунке (Рисунок 2.3).



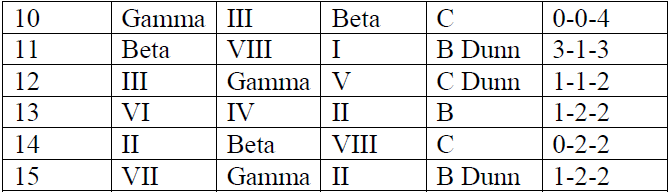


Рисунок 2.3 – Шифрование множественной перестановкой

Общий интерфейс программы приведен на рисунке (Рисунок 2.4).

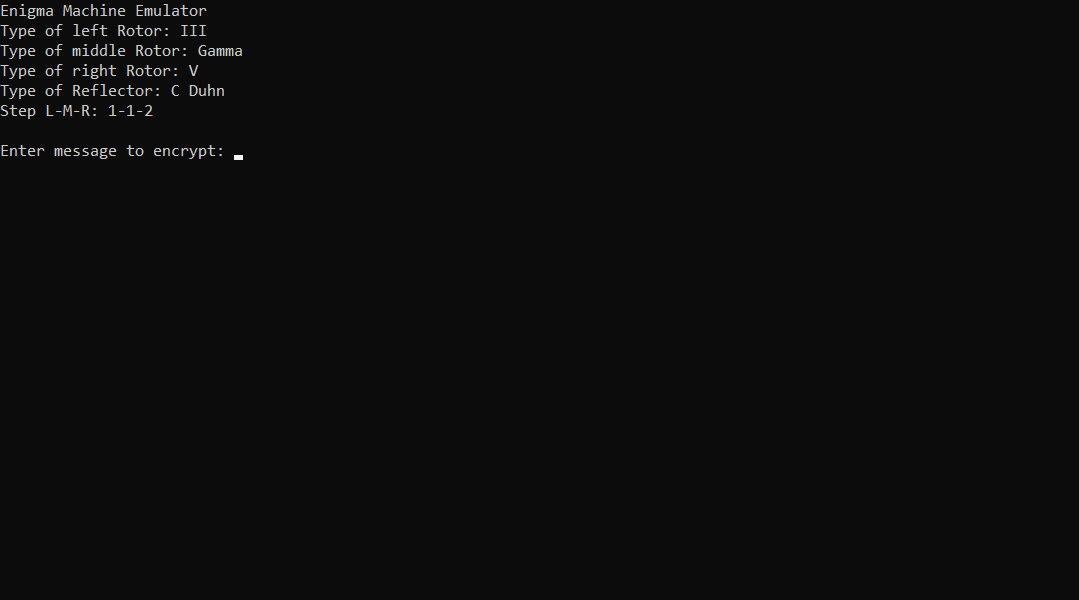


Рисунок 2.4 – Общий интерфейс программы

Пример работы программы приведен на рисунке (Рисунок 2.5).

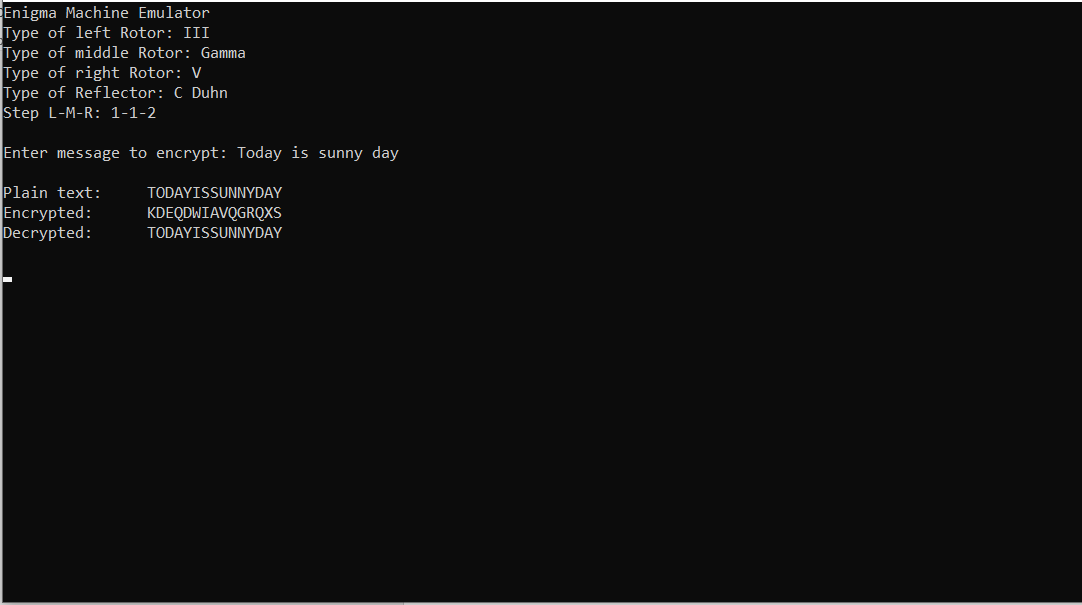


Рисунок 2.5 – Пример зашифрования/расшифрования текста программой

Вывод: В данной лабораторной работе были изучены теоретические сведения об принципах шифрования и расшифрования Энигмой, а также получены навыки работы с эмулятором Энигмы и разработано программное средство для эмуляции работы Энигмы согласно варианту.