Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Изучение устройства и функциональных особенностей шифровальной машины «Энигма»

Выполнила:

студентка 3 курса 6 группы

Трошко В.Н.

Преподаватель:

Нистюк О.А.

Минск 2022

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 (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 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).



Рисунок 1.1 - Пояснение к принципу шифрования путем формирования электрической цепи

Военная модель Энигмы использовала только 26 букв. Прочие символы заменялись редкими комбинациями букв. Пробел пропускался либо заменялся на «X». Символ «X» также использовался для обозначения точки либо конца сообщения. Некоторые особые символы использовались в отдельных вооруженных частях, например, Wehrmacht заменял запятую двумя символами ZZ и вопросительный знак – словом FRAGE либо буквосочетанием FRAQ, a Kriegsmarine М4 запятой соответствовала буква «У».

Как мы отмечали выше, Энигма строится на основе подстановочных шифров, подобных на шифр Цезаря, в котором, как известно, ключ сообщения, который должен знать получатель, – это просто смещение между двумя алфавитами. Принято считать, что в основе шифра Энигмы лежит динамический шифр Цезаря.

Более сложная система использует случайный ряд символов для нижнего алфавита. Принцип, положенный в основу этой «случайности», имеет много общего с перестановочными шифрами.

Этот принцип случайности использовался и при изготовлении роторов и рефлекторов для Энигмы. Всего за время Второй мировой войны немцами было изготовлено восемь роторов и четыре рефлектора, но одновременно могло использоваться ровно столько, на сколько была рассчитана машина.

Как мы неоднократно подчеркивали, преобразование «Энигмы» для каждой буквы может быть определено математически как результат подстановок. Рассмотрим трехроторную модель Энигмы. Положим, что символом В обозначаются операции с использованием коммутационной панели, соответственно символы Re – отражателя, а L, M и R – обозначают действия левых, средних и правых роторов соответственно. Тогда процесс зашифрования символа m c использованием некоторой ключевой информации К формально можно записать в следующем виде:

EК = f (m, В, Re, L, M, R).



Рисунок 1.2 – Спецификация на роторы Энигмы



Рисунок 1.3 - Спецификация на рефлекторы «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 [27]. 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 [2]) в нашем случае снижает уровень (теоретический) криптостойкости (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).

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 2^1) 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 2^2) = 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 2^3) = 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 - 2n)! · n! · 2n. 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 10^23.

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 10^25, что сопоставимо с 84- битным ключом.

Проблема криптоанализа шифров Энигмы была экстраординарной (с учетом электромеханических конструкций устройств для криптоанализа, применяемых в то время). Исчерпывающий поиск всех возможных 1,07 x 10^23 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 10^23 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 10^23 дюйма равно 288 500 световых лет.

1. **Практическая часть**

В данной лабораторной работе необходимо было:

1. Произвести зашифрование сообщения (собственные имя, отчество, фамилия) настройках машины-симулятора. Оценить частотные свойства символов в шифр текстах и сравнить этот параметр с частотными свойствами символов для исходного текста.



Рисунок 2.1 – Онлайн модель-эмулятор машины «Enigma-М3»

Шифрование теста: TroshkoValeriaNikolaevna.



Рисунок 2.2 – Результат шифрования

Расшифрование теста: OCNNMOMHLPNLRTOKVRMBYNZO



Рисунок 2.3 – Результат расшифровки

1. Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Типы роторов (*L – M – R*) и отражателя *Re* следует выбрать из рис. 1.2 и 1.3 в соответствии со своим вариантом, представленным в таблице. Крайний правый столбец этой таблицы показывает, на какое число шагов (букв, *i*) перемещается соответствующий ротор при зашифровании одного (текущего) символа; число 0 означает перемещение соответствующего ротора на один шаг при условии, что расположенный правее ротор совершит один оборот.

С помощью разработанного приложения зашифровать сообщение в соответствии с п.1 практического задания, применив не менее 5 вариантов начальных установок роторов.

В связи с поставленными требованиями было разработано приложение, симулирующее работу шифровальной машины Энигма.

Код реализации “Enigma” на языке C#:

Устанавливаем спецификации левого, среднего и правого роторов, устанавливаем начальное положение каждого ротора, прописываем спецификацию на рефлектор (рис. 2.4)

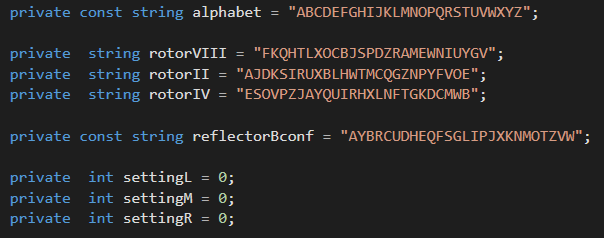


Рисунок 2.4 – Стартовые настройки машины

Прописываем метод зашифрования и расшифрования элемента (рис. 2.5)

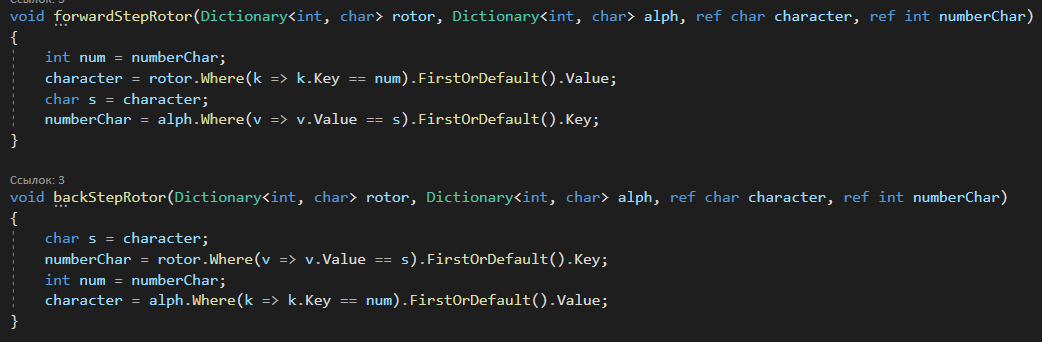


Рисунок 2.5 – Описания «шага» ротора вправо и влево

Переключение ротора на новое положение (рис. 2.6)

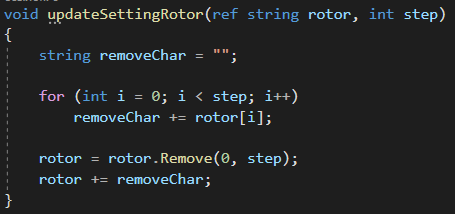


Рисунок 2.6 – Описание переключения ротора

Сам процесс шифрования/расшифрования элемента (рис. 2.7)



Рисунок 2.7 – Метод шифрования/расшифрования элемента

Давайте разберем принцип работы на примере

* левый ротор – VII;
* средний ротор – II;
* правый ротор – IV;
* схема рефлектора – B;
* шаги роторов – 1-0-1;
* символ – ‘a’.

Входной символ «t» посредством правого ротора преобразуется в «g», таблица 2.1.

Таблица 2.1 – Первое преобразование

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 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 |

Далее символ «g» посредством среднего ротора преобразуется в «r», таблица 2.2.

Таблица 2.2 – Второе преобразование

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 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 |

Далее символ «r» посредством левого ротора преобразуется в «m», таблица 2.3.

Таблица 2.3 – Третье преобразование

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 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 |

Далее символ «m» посредством рефлектора преобразуется в «o», таблица 2.4.

Таблица 2.4 – Четвертое преобразование

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 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 |

После чего роторы идут в обратной последовательности. Далее символ «o» посредством левого ротора преобразуется в «h», таблица 2.5.

Таблица 2.5 – Пятое преобразование

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 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 |

Далее символ «h» посредством среднего ротора преобразуется в «l», таблица 2.6.

Таблица 2.6 – Шестое преобразование

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 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 |

Далее символ «a» посредством правого ротора преобразуется в «l», таблица 2.7. В результате получаем «p».

Таблица 2.7 – Седьмое преобразование

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 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 |

На рисунке 2.8 показан результат шифрования ФИО.

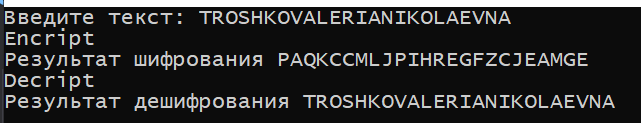


Рисунок 2.2 – Шифрование ФИО

Исходная строка “TROSHKOVALERIANIKOLAEVNA” в результате получим “ PAQKCCMLJPIHREGFZCJEAMGE”.

Для дешифрации требуется:

* установить роторы в нужной последовательности;
* установить начальные позиции роторов;
* установить шаг (если шифруется несколько символов);
* установить коммутатор.

На рисунке 2.3 показан результат дешифрования.

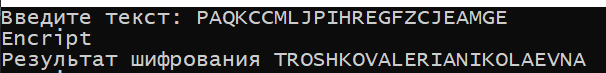


Рисунок 2.3 – Дешифрование ФИО

Оценка криптостойкости «Энигмы» (пользовательского приложения):

Количество различных перестановок роторов: всего имеется 10 роторов, из которых одномоментно может использоваться только 3, поэтому количество перестановок = 10 x 9 x 8 = 720.

На каждом роторе имеется 26 символов, поэтому общее количество перестановок букв – 26 x 26 x 26 = 17576.

Количество различных перестановок коммутаторов: всего имеется 26 букв, нам не важно, в каком порядке идут эти 13 пар, а также для каждой пары обратная пара будет той же парой («AB» = «BA»), поэтому число всех возможных перестановок 26 букв в коммутаторе будет равно:

26! / (13! x 2^13) = 64764752532480000 / 8192 = 7905853580625.

Таким образом, количество всевозможных состояний равно:

720 x 17576 x 7905853580625 = 100046363423806800000 ~ 1 x 10^20.

**Вывод**

В ходе лабораторной работы были закреплены теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-перестановочных шифров. Были изучены структура, принципы функционирования, реализацию процедур зашифрования сообщений в машинах семейства Энигма. Были изучены и приобретены практические навыки выполнения криптопреобразований информации на платформе Энигма, реализованной в виде симуляторов. Были получены практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе Энигма. Было разработано пользовательское приложение-симулятор Энигма.