Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

**Отчёт по лабораторной работе №6**

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

Исполнитель:

Студент 3 курса группы 4

Гурина К. С.

Руководитель:

Ассистент Сазонова Д. В.

1. **Цель и задачи работы**

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

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-перестановочных шифров.

2. Изучить структуру, принципы функционирования, реализацию процедур зашифрования сообщений в машинах семейства «Энигма».

3. Изучить и приобрести практические навыки выполнения криптопреобразований информации на платформе «Энигма», реализованной в виде симуляторов.

4. Получить практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе «Энигма». 5. Результаты выполнения лабораторной работы оформить в виде отчета о проведенных исследованиях, методике выполнения практической части задания и оценке криптостойкости шифров.

**2. Теоретические сведения**

Сущность перестановочного шифрования состоит в том, что исходный текст (М) и зашифрованный текст (С) основаны на использовании одного и того же алфавита, а тайной или ключевой информацией является алгоритм перестановки. Шифры перестановки относятся к классу симметричных. Элементами текста могут быть отдельные символы (самый распространенный случай), пары, тройки букв и т. д.

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). На рис. 2.1 показана фотография одной из моделей «Энигмы» с указанием месторасположения основных модулей машины. Как видно на этом рисунке, «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.

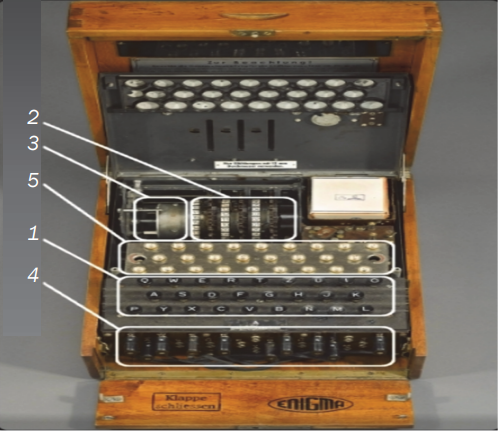


Рисунок 2.1. Трёхроторная модель «Энигмы»

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).

Замыкание цепи происходило за счет рефлектора. На рис. 2.2 схематично показано, как некоторая буква (например, «а») будет зашифрована другой буквой (например, «g»), а следующая за ней буква сообщения (также «а») – уже буквой «с».

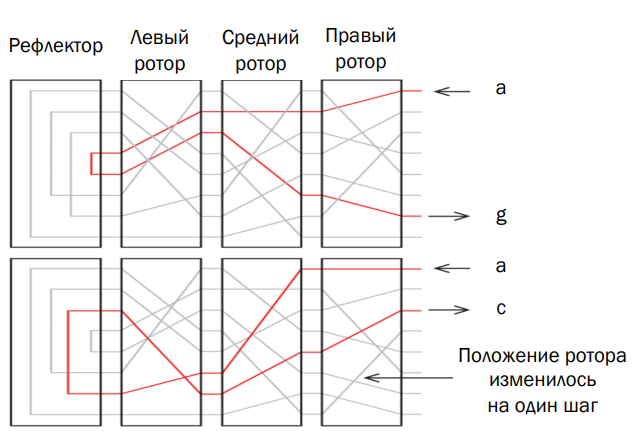


Рисунок 2.2. Пояснение к принципу шифрования путём формирования электрической цепи

Отметим, что на рис. 2.2 электрическая цепь не представлена в виде замкнутой, поскольку не показаны части коммутационной панели и электрическая лампочка.

Замкнутую цепь составляют: батарея 1 (это могут быть и иные источники питания), нажатая двунаправленная буквенная клавиша 2, разъем коммутационной панели 3 (как видим, в одном случае – буква «а» – коммутационного перехода на другую букву нет), входной разъем (входное колесо) роторного модуля 4, роторный модуль 5 (состоит из трех роторов, как в версии «Энигмы» для Вермахта, Wehrmacht Enigma М3, или четырех – в версии «Энигмы» для военно-морского флота, Kriegsmarine Enigma M4), рефлектор 6. Последний возвращает ток (цепь) по другому пути через те же узлы, «зажигая» на ламповой панели букву «D», к другому полюсу батареи. Обратим внимание, что обратная часть цепи уже проходит с учетом выполненной коммутации (7 и 8). Отметим также, что клавиатура соответствовала немецкой раскладке QWERTZ.

«Энигма» строится на основе подстановочных шифров, подобных шифру 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.

На рисунке 2.3 представлены спецификации на роторы.



Рисунок 2.3. Спецификации на роторы «Энигмы»

На рисунке 2.4 представлены спецификации на рефлекторы.

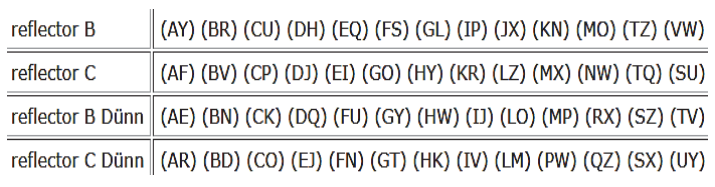


Рисунок 2.4. Спецификации на рефлекторы «Энигмы»

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

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 K формально можно записать в следующем виде:



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.

Проблема криптоанализа шифров «Энигмы» была экстраординарной (с учетом электромеханических конструкций устройств для криптоанализа, применяемых в то время). Исчерпывающий поиск всех возможных 1,07 · 1023 настроек (атака brute force) был невозможен в 1940-х гг., а его сопоставимый 77-битный ключ огромен даже для современных электронных систем

**3. Ход работы**

**Практическое задание:**

1. Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя (L — III, M — VII, R — I, Re — B Dunn, Li-Mi-Ri — 1-0-1).

**Ход работы**

Для создания приложение-симулятор шифровальной машины «Энигма» была разработана функция enigma, код которой представлен на листинге 3.1.

|  |
| --- |
| function enigma(message, a, b, c) {    let rotorIII = Array.from("BDFHJLCPRTXVZNYEIWGAKMUSQO");    let rotorVII = Array.from("NZJHGRCXMYSWBOUFAIVLPEKQDT");    let rotorI = Array.from("EKMFLGDQVZNTOWYHXUSPAIBRCJ");    let reflectorBDunn = Array.from("AEBNCKDQFUGYHWIJLOMPRXSZTV");    let alpabet = Array.from("ABCDEFGHIJKLMNOPQRSTUVWXYZ");    for (let i = 0; i < a; i++) {      rotorIII = rotorShift(rotorIII);    }    for (let i = 0; i < b; i++) {      rotorVII = rotorShift(rotorVII);    }    for (let i = 0; i < c; i++) {      rotorI = rotorShift(rotorI);    }    let ind;    let result = [];    //R    ind = rotorI[alpabet.indexOf(message[0])];    //M    ind = rotorVII[alpabet.indexOf(ind)];    //L    ind = rotorIII[alpabet.indexOf(ind)];    //рефлектор    if (reflectorBDunn.indexOf(ind) % 2 == 0) {      ind = reflectorBDunn[reflectorBDunn.indexOf(ind) + 1];    } else {      ind = reflectorBDunn[reflectorBDunn.indexOf(ind) - 1];    }    //L    ind = alpabet[rotorIII.indexOf(ind)];    //M    ind = alpabet[rotorVII.indexOf(ind)];    //R    ind = alpabet[rotorI.indexOf(ind)];    result.push(ind);    for (let i = 1; i < message.length; i++) {      rotorIII = rotorShift(rotorIII);      if (rotorI[0] === "A") {        rotorVII = rotorShift(rotorVII);      }      rotorI = rotorShift(rotorShift(rotorI));      //R      ind = rotorI[alpabet.indexOf(message[i])];      //M      ind = rotorVII[alpabet.indexOf(ind)];      //L      ind = rotorIII[alpabet.indexOf(ind)];      //рефлектор      if (reflectorBDunn.indexOf(ind) % 2 == 0) {        ind = reflectorBDunn[reflectorBDunn.indexOf(ind) + 1];      } else {        ind = reflectorBDunn[reflectorBDunn.indexOf(ind) - 1];      }      //L      ind = alpabet[rotorIII.indexOf(ind)];      //M      ind = alpabet[rotorVII.indexOf(ind)];      //R      ind = alpabet[rotorI.indexOf(ind)];      result.push(ind);    }    return result;  } |

Листинг 3.1. Код функции enigma

Функция enigma принимает на вход сообщение для шифрования (message) и параметры настройки роторов (a, b, c). Она реализует алгоритм шифрования, который состоит из нескольких этапов: настройка начального положения роторов, шифрование каждого символа сообщения и возвращение зашифрованного сообщения.

Для каждого символа в сообщении:

* Выполняется шифрование, проходя через роторы в порядке: сначала правый (rotorI), затем средний (rotorVII) и, наконец, левый (rotorIII).
* Происходит отражение символа на рефлекторе (reflectorBDunn), который отображает символ обратно на левом роторе.
* Происходит обратный проход через роторы (в обратном порядке).
* Зашифрованный символ добавляется в результирующий массив (result).

Так как алгоритм основан на механизмах перестановки символов и обратного прохождения через роторы и рефлектор, он также используется для декодирования зашифрованной информации.

Также были разработаны вспомогательная функция rotorShift. Функция осуществляет циклический сдвиг элементов массива на одну позицию вправо. Она принимает массив, который необходимо сдвинуть, и возвращает новый массив, полученный после сдвига. Код функции можно увидеть на рисунке 3.1.

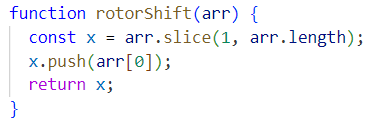


Рисунок 3.1 – Код функции rotorShift

С помощью разработанного приложения было зашифровано сообщение, с применением не менее 5 вариантов начальных установок роторов. Результат представлен на рисунке 3.2.

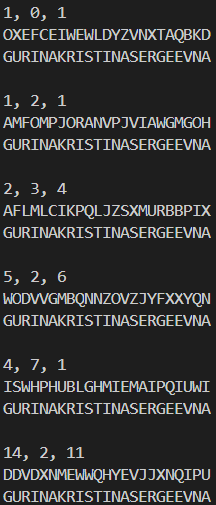


Рисунок 3.2 – Результат работы функции enigma с различными вариантами начальных установок

Далее, нужно было сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений. Гистограмма частот появления символов исходного сообщения приведена на рисунке 3.3.



Рисунок 3.3 – Гистограмма частот появления символов исходного сообщения

Гистограмма частот появления символов зашифрованного сообщения приведена на рисунке 3.4.

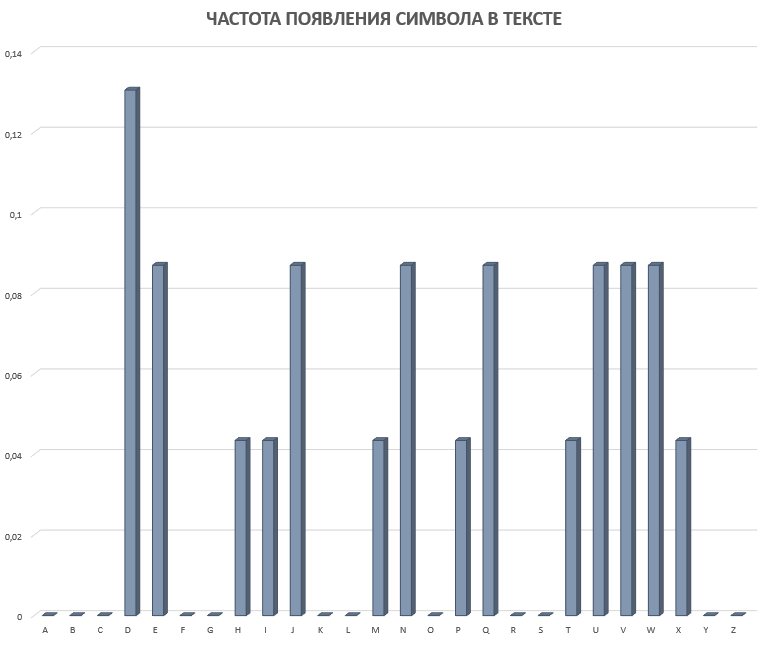


Рисунок 3.4 – Гистограмма частот появления символов зашифрованного сообщения

Можно заметить, что частоты появления не совпадают, что значительно увеличивает криптостойкость шифра машины «Энигма».

**Вывод**

В ходе выполнения лабораторной работы было разработано приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Так же были закреплены теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-перестановочных шифров. Программа была протестирована на нескольких наборах параметров (a, b, c), и результаты шифрования и дешифрования были проверены на корректность. Все тестовые примеры показали соответствие ожидаемым результатам, что подтверждает правильность реализации алгоритма моделирования шифровальной машины «Энигма».