Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет по лабораторной работе №6

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

Студентка: Пунько А.А,

ФИТ 3 курс 5 группа

Преподаватель: Берников В. О.

Минск 2020

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров (рассчитана на 4 часа аудиторных занятий).

**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 проведенных исследованиях, методики выполнения практической части задания и оценки криптостойкости шифров.

**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.

Машина представлена на рисунке 1.



Рисунок 1 – Шифровальная машина Энигма.

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.

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).

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 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.

**Практическая часть**

Полный алгоритм для шифрования с использованием алгоритма Энигмы представлен в листинге 1.

const rotor = [

    ['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', 'k', 'm', 'f', 'l', 'g', 'd', 'q', 'v',

    'z', 'n', 't', 'o', 'w', 'y', 'h', 'x', 'u',

    's', 'p', 'a', 'i', 'b', 'r', 'c', 'j'],

    ['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'],

    ['b', 'd', 'f', 'h', 'j', 'l', 'c', 'p', 'r',

    't', 'x', 'v', 'z', 'n', 'y', 'e', 'i', 'w',

    'g', 'a', 'k', 'm', 'u', 's', 'q', 'o']

];

const reflector = {

    'a': 'y', 'b': 'r', 'c': 'u', 'd': 'h',

    'e': 'q', 'f': 's', 'g': 'l', 'i': 'p',

    'j': 'x', 'k': 'n', 'm': 'o', 't': 'z', 'v': 'w'

};

const rotorShifts = [0, 2, 2];

//[1] I II III B 0-2-2

function shiftRotor(n){

    temp = [];

    shCount = rotorShifts[n-1];

    for(let i = 0; i < rotor[n].length; i++){

        temp[i] = (i-shCount<0)?

            rotor[n][rotor[n].length + (i-shCount)] : rotor[n][i-shCount];

    }

    for(let i = 0; i < rotor[n].length; i++){

        rotor[n][i] = temp[i];

    }

}

function Enigma(key){

    console.log('Enigma');

    key = key.toLowerCase();

    let keySH = [];

    for(e in key){

        keySH[e] = key[e];

    }

    for(let k = 0; k < key.length; k++){

        for(let n = rotor.length-1; n > 0; n--){

            keySH[k] = rotor[n][rotor[0].indexOf(keySH[k])];

        }

        for(e in reflector){

            if(keySH[k] == reflector[e]){

                keySH[k] = e;

            }

            else if(keySH[k] == e){

                keySH[k] = reflector[e];

            }

        }

        for(let n = 1; n < rotor.length; n++){

            keySH[k] = rotor[n][rotor[0].indexOf(keySH[k])];

        }

        for(let i = 1; i < rotor.length; i++){

            shiftRotor(i);

        }

    }

    console.log('keySH: ' + keySH.join(''));

    console.log('key: ' + key);

    console.log('--------------------------------------------');

}

Листинг1 – Эмулятор шифровальной машины Энигма

**Вывод**

В процессе выполнения данной лабораторной работы было изучено строение и принцип работы шифровальной машины Энигма, изучили и приобрели практические навыки выполнения криптопреобразований информации на платформе Энигма, реализованной в виде симулятора.