МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа № 6**

**ИЗУЧЕНИЕ УСТРОЙСТВА**

**И ФУНКЦИОНАЛЬНЫХ ОСОБЕННОСТЕЙ**

**ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА»**

Разработал: Бай И.О.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров (работа 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 о проведенных исследованиях, методике выполнения практической части задания и оценке криптостойкости шифров.

**Теоретические сведения**

**История:**

Первая шифровальная машина, «Enigma A», появилась на рынке в 1923 г. Это была большая и тяжелая машина со встроенной пишущей машинкой и весом около 50 кг. По достоинству шифровальную машину оценили в немецкой армии. В 1925 г. ее принял на вооружение сначала военно-морской флот, а в 1930 г. – Вермахт. Общее количество шифраторов, произведенных до и во время Второй мировой войны, превысило 100 тысяч. Применялись они всеми видами вооруженных сил Германии, а также военной разведкой и службой безопасности.

В 1927 г. «Enigma D» была представлена и коммерциализирована в нескольких версиях с различными роторами и продана военным и дипломатическим службам многих стран Европы. В «Enigma D» было три обычных ротора и один отражатель (рефлектор), которые можно было установить в одном из 26 положений (по числу букв используемого алфавита). Именно эта модель стала основным прототипом многих известных версий машин «Энигма», которые использовала Германия в годы Второй мировой войны.

**Структура:**

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. 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.

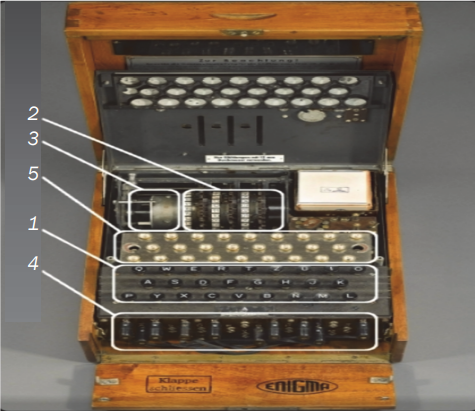


Рис. 1 - Одна из моделей (трехроторная) «Энигмы» [19]:

1 – панель механических клавиш; 2 – роторные диски; 3 – рефлектор;

4 – коммутационная панель; 5 – индикационная панель

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.

**Алгоритм шифрования:**

Всего за время Второй мировой войны немцами было изготовлено восемь роторов (рис. 2) и четыре рефлектора (рис. 4), но одновременно могло использоваться ровно столько, на сколько была рассчитана машина.



Рис.2 - Спецификация на роторы «Энигмы»

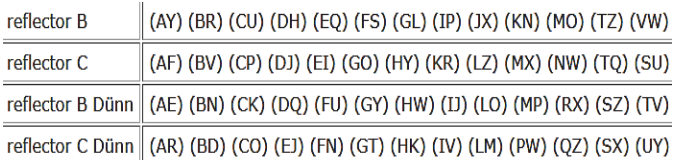


Рис.3 - Спецификация на рефлекторы «Энигмы»

**Пример.** В этом примере рассмотрим процедуру зашифрования только одной буквы («G»).

Предположим, что «Энигма» оснащена роторами I, II, III (см. рис. 2). Таким образом, правым ротором (R) является III приведенной спецификации. Предположим также, что каждый ротор находится в своем положении A, когда выполняется шифрование. Если взять информацию из рис. 2 и 3, указав фактическую разводку ротора, это означает, что правый ротор R производит подстановку в соответствии с переставленными буквами исходного алфавита, т. е. буква «G» будет заменена буквой «C»:

****

Центральный ротор (М) или II заменяет букву «С» на букву «D»:



Левый ротор (L) или III – соответственно букву «D» на букву «F»:



Предположим далее, что используется рефлектор В (спецификация на рис. 3 – первая строка):



Обратим внимание на то, что рефлектор имеет только 13 соединений, т. е. имеется 13 пар подстановок: A – Y, В – R и т. д. В нашем примере произошла подстановка F → S.

Ток теперь проходит обратный путь через три ротора в последовательности

L → M → R.

Эффект преобразования левого ротора (обратный):



соответственно – среднего ротора (обратный):



и, наконец, правого ротора (обратный):



После всех (в данном случае – 7) подстановок буква «G» будет зашифрована буквой «P».

**Практическое задание**

Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Типы роторов (L – M – R) и отражателя Re следует выбрать из рис. 2 и 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.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вариант задания | L | M | R | Re | Li-Mi-Ri |
| 2 | II | III | V | C | 1-2-2 |

В листинге 1 представлен код реализации шифрования энигмы:

function rotorForward(letter, rotor) {

    let index = ALPH.indexOf(letter);

    let newLetter = rotor.array[index + rotor.position];

    let newIndex = ALPH.indexOf(newLetter);

    return ALPH[newIndex];

}

function rotorBack(letter, rotor) {

    let index = rotor.array.indexOf(letter);

    let newLetter = ALPH[index];

    let newIndex = rotor.array.indexOf(newLetter);

    return rotor.array[newIndex];

}

function reflect(letter) {

    return REFLECTOR[letter];

}

function getEncryptKey(key) {

    let newLetter = rotorForward(key, rotors.rotor2);

    newLetter = rotorForward(newLetter, rotors.rotor1);

    newLetter = rotorForward(newLetter, rotors.rotor0);

    newLetter = reflect(newLetter);

    newLetter = rotorBack(newLetter, rotors.rotor0);

    newLetter = rotorBack(newLetter, rotors.rotor1);

    newLetter = rotorBack(newLetter, rotors.rotor2);

    rotors = rotate(rotors);

    document.querySelector('.output-text').value += newLetter;

    positionsDiv.innerHTML = '<p> Positions: ' + ALPH[rotors.rotor0.position] + ' ' + ALPH[rotors.rotor1.position] + ' ' + ALPH[rotors.rotor2.position] + '</p>';

}

Листинг 1 – Реализация энигмы

Реализация выполнения программы:

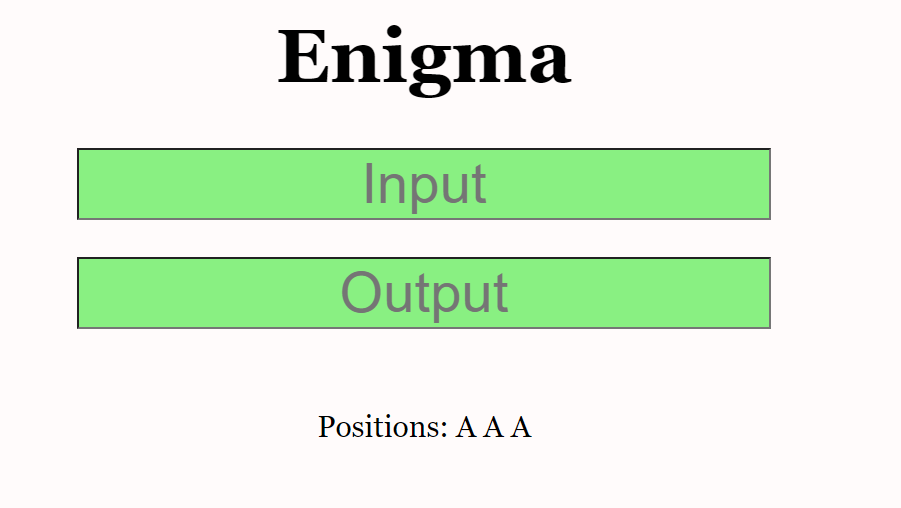


Рис. 4 – Интерфейс программного приложения

**Криптостойкость энигмы:**

С учетом существования 10 возможных роторов, чтобы выбрать 3 ротора из возможных 10, существует 720 комбинаций

10×9×8 = 720

Каждый ротор (его внутренняя проводка) может быть установлен в любом из 26 положений. Следовательно, с 3 роторами имеется 17 576 различных положений ротора

26×26×26 = 17 576

Количество различных перестановок рефлекторов: 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 рефлекторе будет равно:

26! / (13! × 213) = 64 764 752 532 480 000 / 8 192 = 7 905 853 580 625

Таким образом, практически рассматриваемая версия «Энигмы» может быть настроена на 21 557 568 614 400 различных состояний.

720 × 17 576 × 7 905 853 580 625 = 100 046 363 423 806 800 000 ~ 1e20

**Вывод:** «Эни́гма» (от нем. Änigma — загадка) — переносная шифровальная машина, использовавшаяся для шифрования и расшифрования секретных сообщений. Для непосредственного шифрования в структуре энигмы используются роторы и отражатель. В ходе лабораторной работы было разработано приложение-симулятор шифровальной машины, состоящей из трех роторов и отражателя, а также вычислена криптостойкость разработанного алгоритма, равная 1e20 различных состояний.