****

**Московский авиационный институт**

**(Национальный исследовательский университет)**

**Институт № 3**

**Кафедра 311**

**Информационная безопасность**

**Лабораторная работа № 2**

**«Шифр Виженера (шифровка, расшифровка)»**

**Выполнил студент  
Максимов Евгений Викторович**

**Группа М3З-302-БК**

**Дата 12.05.2022 г.**

**Принял преподаватель  
Кос Оксана Игоревна**

Оглавление

[Цель лабораторной работы 3](#_Toc89363528)

[Глава 1. Принцип Шифра Виженера. 4](#_Toc89363529)

[Глава 2. Шифрование с помощью Шифра Виженера. 5](#_Toc89363530)

[Глава 3. Расшифровка текста 7](#_Toc89363531)

[Итоги лабораторной работы 9](#_Toc89363532)

[Список литературы 10](#_Toc89363533)

# Цель лабораторной работы

Изучить:

* 1. Принцип Шифра Виженера;
  2. Зашифровать текст с помощью Шифра Виженера;
  3. Расшифровать зашифрованный текст.

# Глава 1. Принцип Шифра Виженера.

Шифр Виженера — это метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций.

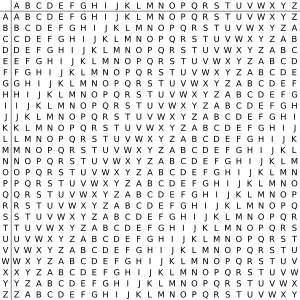


Рисунок 1.1 – Квадрат Виженера

# Глава 2. Шифрование с помощью Шифра Виженера.

**Задача**: зашифровать исходный текст Шифром Виженера.

**Дано**:

*Исходный текст*: "In a hole in the ground there lived a hobbit. Not a nasty, dirty, wet hole, filled with the ends of worms and an oozy smell, nor yet a dry, bare, sandy hole with nothing in it to sit down on or to eat it was a hobbit hole, and that means comfort."

*Ключевое слово:* «QWERTY»

**Результат**:

YJEYHJUERKACWNSLGBJDIIXJYRIUTFEXFZMLEPEETQJUHZKROSIKAMBAJZEJUZAZMFJDIVGBIKJNHPCOEEWYDKSQRQCAPCGMHUIKTBHUFRKCIWRURFEHINBRXJSKAGDCMEBRJKWZMBESRFGMHPSVTRYPARLYXKFSBRXKPVTLTPLRMKUWRJVMCBSIM»

**Листинг программы**:

*Метод наполнения алфавита*

private static List<Character> fillAlphabet() {  
 List<Character> cypherAlphabet = new ArrayList<>();  
 List<Character> engAlphabet = getAlphabet("A", ENG\_ALPHABET\_SIZE);  
 List<Character> ruAlphabet = getAlphabet("А", RU\_ALPHABET\_SIZE);  
 List<Character> specAlphabet = getAlphabet(" ", SPEC\_ALPHABET\_SIZE);  
 specAlphabet = specAlphabet.stream()  
 .distinct()  
 .collect(toList());  
 cypherAlphabet.addAll(engAlphabet);  
 cypherAlphabet.addAll(ruAlphabet);  
 cypherAlphabet.addAll(specAlphabet);  
 return cypherAlphabet;  
}

*Метод получения английского алфавита*

static {

ALPHABET = new ArrayList<>();

char letter = 'A';

for (int i = 0; i < ENG\_ALPHABET\_SIZE; i++) {

ALPHABET.add(letter);

letter++;

}

}

*Метод шифрования текста.*

private static String encode(String inputText, String key) {

int maxLength = max(inputText.length(), key.length());

StringBuilder sb = new StringBuilder();

for (int i = 0; i < maxLength; i++) {

int alphabetCharIdx = ALPHABET.indexOf(inputText.charAt(i >= inputText.length() ? i % inputText.length() : i)); // подгон сообщения к ключу (если меньше)

Character keyChar = key.charAt(i >= key.length() ? i % key.length() : i); // подгон ключа к сообщению (если короткий)

int keyCharIdx = ALPHABET.indexOf(keyChar);

Character tableSymbol = ALPHABET.get((ALPHABET.size() + (alphabetCharIdx + keyCharIdx)) % ALPHABET.size()); // символ по таблице Виженера

sb.append(tableSymbol);

}

result = sb.toString();

return result;

}

# Глава 3. Расшифровка текста

**Задача**: расшифровать зашифрованный текст.

**Дано**:

*Зашифрованный текст:* «YJEYHJUERKACWNSLGBJDIIXJYRIUTFEXFZMLEPEETQJUHZKROSIKAMBAJZEJUZAZMFJDIVGBIKJNHPCOEEWYDKSQRQCAPCGMHUIKTBHUFRKCIWRURFEHINBRXJSKAGDCMEBRJKWZMBESRFGMHPSVTRYPARLYXKFSBRXKPVTLTPLRMKUWRJVMCBSIM»

*Ключевое слово:* «LEMON»

**Результат (Все символы в верхнем регистре и без пробелов и спец.символов):**

«INAHOLEINTHEGROUNDTHERELIVEDAHOBBITNOTANASTYDIRTYWETHOLEFILLEDWITHTHEENDSOFWORMSANDANOOZYSMELLNORYETADRYBARESANDYHOLEWITHNOTHINGINITTOSITDOWNONORTOEATITWASAHOBBITHOLEANDTHATMEANSCOMFORT»

**Листинг программы:**

*Метод дешифровки текста*

private static String decode(String inputText, String key) {

int maxLength = max(inputText.length(), key.length());

StringBuilder sb = new StringBuilder();

for (int i = 0; i < maxLength; i++) {

int alphabetCharIdx = ALPHABET.indexOf(inputText.charAt(i >= inputText.length() ? i % inputText.length() : i)); // подгон сообщения к ключу (если меньше)

Character keyChar = key.charAt(i >= key.length() ? i % key.length() : i); // подгон ключа к сообщению (если короткий)

int keyCharIdx = ALPHABET.indexOf(keyChar);

keyCharIdx -= keyCharIdx \* 2;

Character tableSymbol = ALPHABET.get((ALPHABET.size() + (alphabetCharIdx + keyCharIdx)) % ALPHABET.size()); // символ по таблице Виженера

sb.append(tableSymbol);

}

return sb.toString();

}

# Итоги лабораторной работы

Мы научились шифровать и расшифровывать текст с помощью метода Виженера.

# Список литературы

1. [[Wikipedia.org](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F)] – Шифр Виженера;
2. [[lingua.com](https://lingua.com/english/reading/wonderful-family/)] – Исходный английский текст;
3. «Война и Мир», Л.Н. Толстой, 1873 г. – Исходный русский текст.