

# **Отчет по лабораторной работе № 2.**

## **Шифры перестановки**

**дисциплина: Математические основы защиты информации и  
информационной безопасности**

**Наливайко Сергей Максимович**

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>3</b>
<b>2</b>	<b>Задание</b>	<b>4</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
3.1	Маршрутное шифрование . . . . .	5
3.2	Шифрование с помощью решеток. . . . .	6
3.3	Шифр Виженера . . . . .	7
<b>4</b>	<b>Выводы</b>	<b>9</b>

# **1 Цель работы**

Научиться реализовывать алгоритмы шифрования перестановкой.

## 2 Задание

- Реализовать маршрутное шифрование.
- Реализовать шифрование с помощью решеток.
- Реализовать шифр Виженера.

## 3 Выполнение лабораторной работы

### 3.1 Маршрутное шифрование

Реализуем маршрутное шифрование на языке программирования C++. Код программы представлен ниже.

```
std::string Route_Cipher::crypt(const std::string &text,
                                const std::string &key) {

    if(text.size() < key.size())
        throw std::invalid_argument("text_length must be bigger then

std::map<char, size_t> ordered_pass;
for(size_t i = 0; i < key.size(); ++i) {
    if(!ordered_pass.insert({tolower(key[i]), i}).second)
        throw std::invalid_argument("all password characters must

}

size_t col = key.size();
size_t row = text.size() / col + (text.size() % col == 0 ? 0: 1)
std::vector<std::vector<char>> matrix(row, std::vector<char>(col,
std::stringstream ss;

for(size_t i = 0, k = 0; i < row; ++i) {
```

```

        for(size_t j = 0; j < col && k < text.length(); ++j, ++k)
            matrix[i][j] = text[i * col + j];
    }

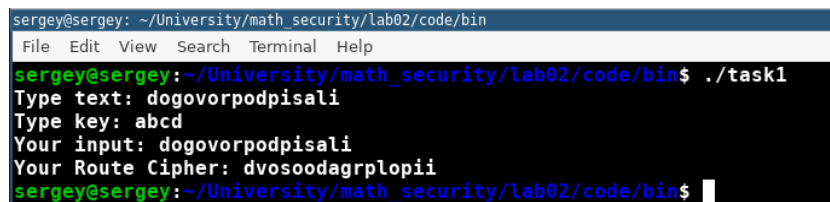
    for(auto element: ordered_pass) {
        size_t j = element.second;
        for(size_t i = 0; i < row; ++i) {
            ss << matrix[i][j];
        }
    }

    return ss.str();
}

```

Полный листинг программного кода точки входа в программу и шифрования прикреплен в архиве (code/task1.cpp и code/crypters/route\_cipher.cpp).

Скомпилируем и запустим программу fig. 3.1.



```

sergey@sergey: ~/University/math_security/lab02/code/bin
File Edit View Search Terminal Help
sergey@sergey:~/University/math_security/lab02/code/bin$ ./task1
Type text: dogovorpodpisali
Type key: abcd
Your input: dogovorpodpisali
Your Route Cipher: dvosoodagrplopii
sergey@sergey:~/University/math_security/lab02/code/bin$

```

Figure 3.1: Маршрутное шифрование

## 3.2 Шифрование с помощью решеток.

Полный листинг программного кода точки входа в программу и шифрования прикреплен в архиве (code/task2.cpp и code/crypters/route\_cipher.cpp).

Полный код алгоритма шифрования здесь не будет приведен, в связи с громоздкостью (множество вспомогательных методов переворота решетки, проверки корректности данных и т. д.).

Скомпилируем и запустим программу fig. 3.2.

```
sergey@sergey:~/University/math_security/lab02/code/bin$ ./task2
Type text: dogovorpodpisali
Type key: abcd
Type k: 2
Your input: dogovorpodpisali
Your grid:
* 2 3 1
* * * *
* * 4 *
* * * *
sogdliioaporopdv
sergey@sergey:~/University/math_security/lab02/code/bin$
```

Figure 3.2: Шифрование с помощью решеток

### 3.3 Шифр Виженера

Реализуем алгоритм шифрования на языке программирования C++. Код программы представлен ниже.

```
std::string Vigenere_Cipher::crypt(const std::string &text, const std::string &key) {
    std::stringstream ss, nk;
    nk << key;
    int k = text.size() - key.size();
    for(int i = 0; i < k; ++i) {
        nk << (key[i % key.size()]);
    }
    std::string new_key{nk.str()};

    for(int i = 0; i < text.size(); ++i) {
        char letter = (text[i] - ' ' + new_key[i] - ' ') % 95 + ' ';
        ss << letter;
    }

    return ss.str();
}
```

Полный листинг программного кода точки входа в программу и шифрования прикреплен в архиве (code/task3.cpp и code/crypters/viginer\_cipher.cpp).

Скомпилируем и запустим программу fig. 3.3.

```
sergey@sergey:~/University/math_security/lab02/code/bin$ ./task3
Type text: cryptography is a serious science
Type key: math
Your input: cryptography is a serious science
Your Viegenere Cipher: QTnYbQ\[OR]bmKhhOahN`Kd^aahLWGcLS
sergey@sergey:~/University/math_security/lab02/code/bin$
```

Figure 3.3: Шифр Виженера



## 4 Выводы

В ходе лабораторной работы мы научились реализовывать алгоритмы шифрования перестановкой.