Отчет по лабораторной работе № 2. Шифры перестановки

дисциплина: Математические основы защиты информации и информационной безопасности

Наливайко Сергей Максимович

Содержание

# Цель работы

Научиться реализовывать алгоритмы шифрования перестановкой.

# Задание

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

# Выполнение лабораторной работы

## 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 password\_length");  
  
 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 be unique");  
 }  
  
 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, 'a'));  
 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. 1.

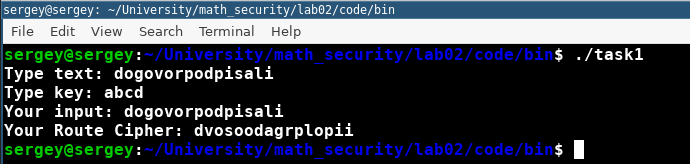


Figure 1: Маршрутное шифрование

## 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. 2.

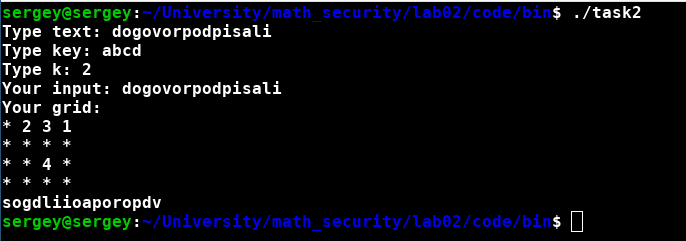


Figure 2: Шифрование с помощью решеток

## 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.

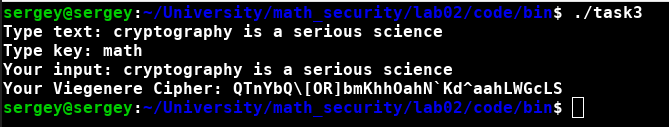


Figure 3: Шифр Виженера

# Выводы

В ходе лабораторной работы мы научились реализовывать алгоритмы шифрования перестановкой.