Шифры перестановки

Лабораторная работа №2

Данилова А.С.

Цели и задачи

Изучить и реализовать шифры перестановки: маршрутное шифрование, шифрование с помощью решеток, таблица Виженера

Маршрутное шифрование

1. Открытый текст последовательно разбивается на части (блоки) с длиной, равной произведению m и n.
2. Блок вписывается построчно в таблицу размерности m × n. Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Этот маршрут вместе с числами m и n составляет ключ шифра.

Шифрование с помощью решеток

Рис. 1: Шифрование с помощью решеток

Шифрование с помощью *таблицы Виженера* основано на том, что каждая буква в исходном шифруемом тексте сдвигается по алфавиту не на фиксированное, а на переменное количество символов. Величина сдвига каждой буквы задаётся ключом.

Для шифрования используется так называемый «квадрат Виженера» — таблица, где в каждой строке алфавит сдвигается на одну позицию вправо.

Маршрутное шифрование

Рис. 2: Маршрутное шифрование

Полученный результат

Зашифрованный текст

Рис. 3: Зашифрованный текст

Шифрование с помощью решеток

Рис. 4: Шифрование с помощью решеток

Полученный результат

Зашифрованный текст

Рис. 5: Зашифрованный текст

Шифрование с таблицей Виженера

Рис. 6: Шифрование с таблицей Виженера

Полученный результат

Зашифрованный текст

Рис. 7: Зашифрованный текст

Выводы

Мы изучили 3 шифра перестановки и реализовали их на языке программирования Julia.