Отчет по лабораторной работе №2

Дисциплина: Математические основы защиты информации и информационной безопасности

Живцова Анна

Содержание

# 1 Цель работы

Изучить алгоритмы шифрования с помощью перестановки. Реализовать шифрование с помощью маршрутов, шифрование с помощью решеток, и шифрование Виженера.

# 2 Задание

Реализовать шифрование с помощью маршрутов, шифрование с помощью решеток, и шифрование Виженера.

# 3 Теоретическое введение

Шифры перестановки преобразуют открытый текст в криптограмму путем перестановки его символов. Подробнее в источниках [1,2].

Маршрутное шифрование реализуется следующим образом. Исходный текст построчно записывается в таблицу размера . При недостатке символов исходного текста свободные места в таблице заполняются произвольными символами. В последнюю строчку таблицы записывается пароль. Символы из таблицы считываются по столбцам, отсортированным по последнему элементу (букве пароля), формируя зашифрованный текст.

Шифрование с помощью решеток. Таблица размера заполняется различными числами от 1 до . Далее эту таблицу три раза поворачивают на 90 градусов и из полученных четырех таблиц, отличающихся только поворотом, формируют таблицу размером . Из этой таблицы случайно выбирается различных чисел. Исходный текст записывается в пустую таблицу в ячейки, которые соответствуют выбранным числам. Далее таблица переворачивается. Операция повторяется еще три раза. К полученной заполненной таблице в последней строке приписывается пароль. Символы из таблицы считываются по столбцам, отсортированным по последнему элементу (букве пароля), формируя зашифрованный текст.

Шифр Виженера. Тип 1. Исходный текст разибается на блоки длины (если символов не хватает, то дописываются произвольные). Каждый блок циклически сдвигается по алфавиту на величину .

Шифр Виженера. Тип 2. Задана таблица в которой каждая строчка представляет собой алфавит циклически сдвинутый на позиций. Посредством циклического повторения пароля формируется кодовое слово , по длине равное исходному тексту . Символ под номером исходного текста шифруется с помощью символа таблицы, стоящего в столбце, начинающемся на символ , и строке, начинающейся на символ .

# 4 Выполнение лабораторной работы

## 4.1 Маршрутное шифрование

Для реализации маршрутного шифрования на языке Python была написанна следующая функция.

def crypt1(n, m, text, password):   
 min\_char, max\_char = ord(min(text)), ord(max(text))   
 text = text.replace(' ', '')   
 cripting\_table = np.array(list(text)+[chr(np.random.randint(min\_char, max\_char)) for i in range(m\*n-len(text))]).reshape(m, n)   
 p = dict(zip(list(password), range(len(password))))   
 return ''.join([''.join(cripting\_table[:, p[i]]) for i in sorted(p)])

Тут и – размеры кодовой таблицы. Переменная отвечает за пароль, а переменная за исходный текст.

Функциональность данной функции была протестирована в среде jupyter notebook (см. рис. 1).

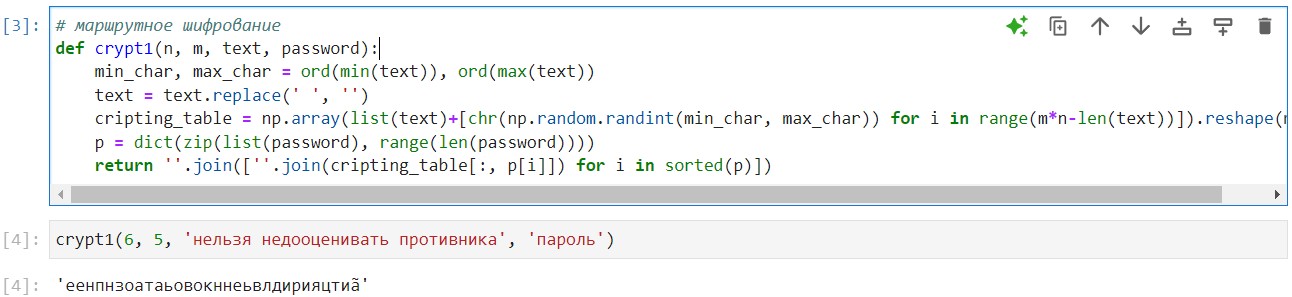


Рис. 1: Тестирование маршрутного шифрования

## 4.2 Шифрование с помощью решеток

Реализовано с помощью функции

def crypt2(k, text, password):   
 text = text.replace(' ', '')   
 text = np.array(list(text)+[chr(np.random.randint(min\_char, max\_char)) for i in range(k\*k-len(text))])   
 base\_square = np.arange(1, k\*\*2 + 1).reshape(k, k)   
 square = base\_square.copy()   
 for i in range(3):   
 base\_square = np.array([i[::-1] for i in base\_square.transpose()])   
 square = np.concatenate([square, base\_square], axis=1)   
 square = np.concatenate([square[:, :2\*k], np.concatenate([square[:, 3\*k:], square[:, 2\*k:3\*k]], axis = 1)])   
 print('Числовой блок из 4 поворотов', '\n', square)   
 bool\_matrix = np.zeros((2\*k, 2\*k))   
 for i in range(1, 2\*k+1):   
 ind = np.random.randint(0, 3)   
 bool\_matrix[np.where(square == i)[0][ind], np.where(square == i)[1][ind]] = 1   
 print('Выбираем k различных чисел', '\n', bool\_matrix)   
 text\_matrix = np.array([['0' for j in range(2\*k)] for i in range(2\*k)])   
 counter = 0   
 for i in range(4):   
 for j in range(2\*k):   
 for m in range(2\*k):   
 if bool\_matrix[j, m]:   
 text\_matrix[j][m] = text[counter]   
 counter += 1   
 print('записываем текст через решето, итерация ', i, '\n', text\_matrix)   
 bool\_matrix = np.array([m[::-1] for m in bool\_matrix.transpose()])   
 p = dict(zip(list(password[:2\*k]), range(len(password[:2\*k]))))   
 return ''.join([''.join(text\_matrix[:, p[i]]) for i in sorted(p)])

Функция была протестирована функции (см. рис. 2).

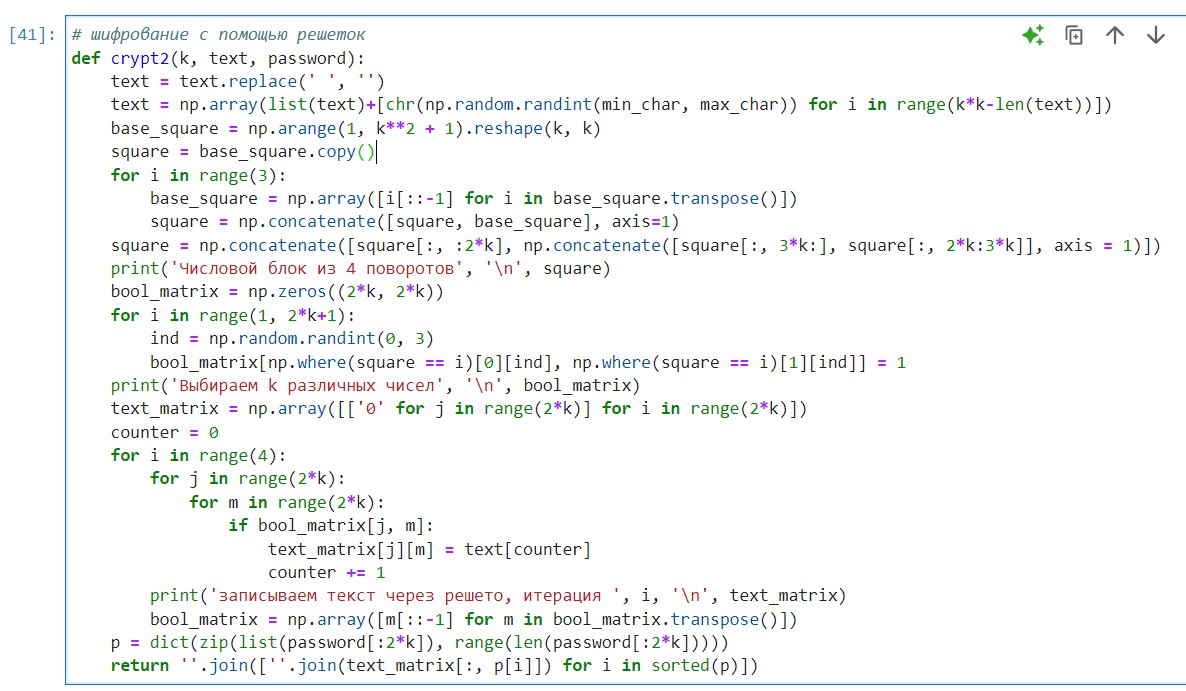


Рис. 2: Тестирование шифрования с помощью решеток

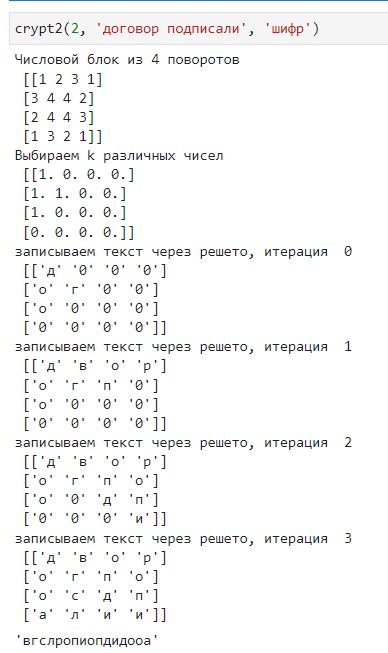


Рис. 3: Тестирование шифрования с помощью решеток

## 4.3 Шифр Вижнера. Тип 1

Реализован с помощью функции

al = 'a b c d e f g h i j k l m n o p q r s t u v w x y z'.split(' ')   
def crypt3(text, password, n):   
 min\_char, max\_char = ord(min(text)), ord(max(text))   
 text = text.replace(' ', '')   
 text = np.array(list(text)+[chr(np.random.randint(min\_char, max\_char))   
 for i in range(n\*(len(text)//n+1\*bool(n%len(text)))-len(text))]).reshape(-1, n)   
 return ''.join([''.join([al[(ord(j)+ord(k))%len(al)]   
 for j in t]) for t, k in zip(text, password)])

Функция была протестирована функции (см. рис. 4).

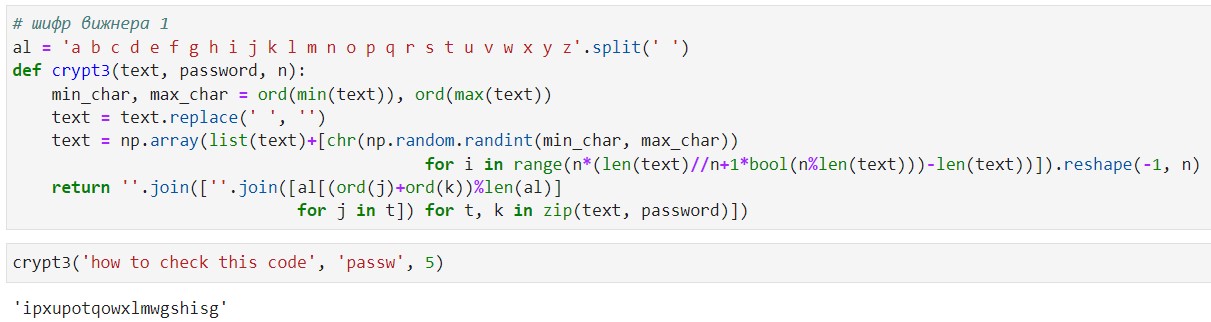


Рис. 4: Тестирование шифрования Виженера типа 1

## 4.4 Шифр Вижнера. Тип 2

Реализован с помощью функции

al = 'а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я'.split(' ')   
def crypt4(text, password):   
 password = [password[i%len(password)].lower() for i in range(len(text))]   
 return ''.join([al[(al.index(i)+al.index(j))%len(al)] for i, j in zip(text.lower().replace(' ', ''), password)])

Функция была протестирована функции (см. рис. 5).

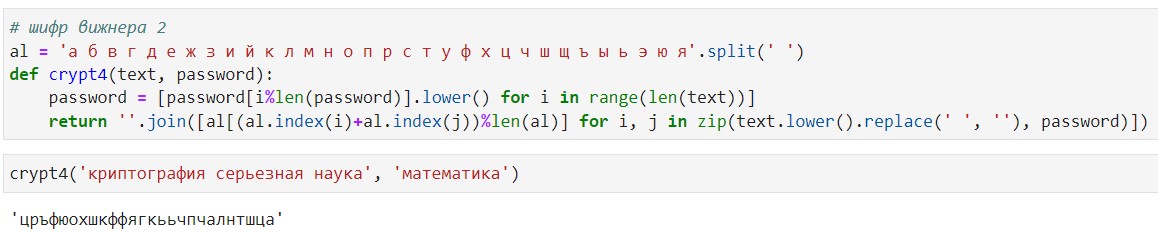


Рис. 5: Тестирование шифрования Виженера типа 2

# 5 Выводы

В данной работе я изучила алгоритмы шифрования с помощью перестановки. Реализовала и протестировала шифрование с помощью маршрутов, шифрование с помощью решеток, и шифрование Виженера.

# Список литературы

1. Kulyabov D., Korolkova A., Gevorkyan M. Информационная безопасность компьютерных сетей: лабораторные работы. 2015.

2. Самуйлов К.Е. и др. Сети и телекоммуникации : Учебник и практикум. Издательство Юрайт, 2019. С. 1–363.