Министерство образования и науки РФ

ФГБОУ ВО «Тамбовский государственный технический университет»

Кафедра САПР

Отчет по лабораторной работе №1.1

по дисциплине «Защита информации»

Выполнил: студент группы БВТ-191

Глушков Н.Р.

Проверил: Евдокимов А.А.

# Тамбов 2022

**Задание:**

Составить программу реализующую шифрование по алгоритму "Шифр Плейфера".

Вариант: зашифровать.

Исходное сообщение: «зашифрованное сообщение».

Ключ: «как написать диплом».

Полученное зашифрованное сообщение: «йкънхуьёнпиджпд2тё1упсг1».

**Листинг:**

cyrillic\_str = **'абвгдеёжзийклмнопрстуфхцчшщъыьэюя'**key = open(**'key.txt'**,**'r'**, encoding=**'utf-8'**).read()  
message = open(**'message.txt'**, **'r'**, encoding=**'utf-8'**).read()  
  
**def** get\_matrix(key, cyrillic\_str):  
 matrix = [[**"0"**,**"0"**,**"0"**,**"0"**,**"0"**,**"0"**],  
 [**"0"**,**"0"**,**"0"**,**"0"**,**"0"**,**"0"**],  
 [**"0"**, **"0"**, **"0"**, **"0"**, **"0"**, **"0"**],  
 [**"0"**,**"0"**,**"0"**,**"0"**,**"0"**,**"0"**],  
 [**"0"**,**"0"**,**"0"**,**"0"**,**"0"**,**"0"**],  
 [**"0"**,**"0"**,**"0"**,**"0"**,**"0"**,**"0"**],]  
 dictionary = (**" "**.join(dict.fromkeys(key + cyrillic\_str))).replace(**" "**,**""**)+**"123"** print(**"Алфавит: "**,dictionary)  
 k = 0  
 print(**"Полученная матрица:"**)  
 **for** i **in** range(len(matrix)):  
 **for** j **in** range(len(matrix[i])):  
 matrix[i][j] = dictionary[k]  
 k+=1  
 print(matrix[i][j], end=**" "**)  
 print()  
 **return** matrix  
  
**def** get\_bigramm(message):  
 bi = []  
 i = 0  
 print(**"Исходное сообщение: "**, message)  
 mess = message.replace(**" "**,**""**)  
 **while** i < (len(mess)-1):  
  
 buff = mess[i]+mess[i+1]  
 **if**(mess[i]==mess[i+1]):  
 buff = mess[i]+**"я"** i += 1  
 **else**: i+=2  
 bi.append(buff)  
  
 **if** i == len(mess)-1:  
 buff = mess[i] + **"я"** bi.append(buff)  
 print(**"Биграмма: "**, bi)  
 **return** bi  
  
  
**def** encryption():  
 str = **''  
 def** search\_coor(n1, n2):  
 **for** i **in** range(len(matrix)):  
 **for** j **in** range(len(matrix[i])):  
 **if** (matrix[i][j]==n1):  
 x1,y1 = i,j  
 **if** (matrix[i][j]==n2):  
 x2,y2 = i,j  
 coor = {**'x1'**: x1, **'y1'**: y1, **'x2'**: x2, **'y2'**: y2}  
 **return** coor  
  
 matrix = get\_matrix(key, cyrillic\_str)  
 bi = get\_bigramm(message)  
  
 **for** i **in** range(len(bi)):  
 b1, b2 = bi[i][0], bi[i][1]  
 cr = search\_coor(b1, b2)  
 *#если на одной строке* **if**(cr[**'x1'**]==cr[**'x2'**]):  
 **if**(cr[**'y1'**]==5):  
 b1 = matrix[cr[**'x1'**]][0]  
 **else**:  
 b1 = matrix[cr[**'x1'**]][cr[**'y1'**]+1]  
 **if**(cr[**'y2'**] == 5):  
 b2 = matrix[cr[**'x2'**]][0]  
 **else**:  
 b2 = matrix[cr[**'x2'**]][cr[**'y2'**]+1]  
 str += b1 + b2  
  
 *#если в одном столбце* **elif**(cr[**'y1'**]==cr[**'y2'**]):  
 **if**(cr[**'y1'**]==5):  
 b1 = matrix[0][cr[**'y1'**]]  
 **else**:  
 b1 = matrix[cr[**'x1'**]+1][cr[**'y1'**]]  
 **if** (cr[**'y2'**] == 5):  
 b2 = matrix[0][cr[**'y2'**]]  
 **else**:  
 b2 = matrix[cr[**'x2'**] + 1][cr[**'y2'**]]  
  
 str += b1 + b2  
  
  
 *#если в разных* **else**:  
 b1 = matrix[cr[**'x1'**]][cr[**'y2'**]]  
 b2= matrix[cr[**'x2'**]][cr[**'y1'**]]  
 str += b1 + b2  
 *#print(str)* **return** str

print(**'Зашифрованное сообщение: '**,encryption())

**Вывод в консоль:**

