|  |  |
| --- | --- |
| **Gerb-BMSTU_01** | **Министерство науки и высшего образования Российской Федерации**  Калужский филиал  федерального государственного бюджетного  образовательного учреждения высшего образования  ***«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»***  ***(КФ МГТУ им. Н.Э. Баумана)*** |

**ФАКУЛЬТЕТ** ***ИУК «Информатика и управление»***

**КАФЕДРА** \_\_***ИУК4 «Программное обеспечение ЭВМ, информационные технологии»***

**ЛАБОРАТОРНАЯ РАБОТА №1**

**«Основы шифрования данных»**

**ДИСЦИПЛИНА: «Защита информации»**

|  |  |  |
| --- | --- | --- |
| Выполнил: студент гр. ИУК4-72Б | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ( Карельский М.К. )  (Подпись) |
| Проверил: | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ( Ерохин И.И. )  (Подпись) |
| Дата сдачи (защиты):  Результаты сдачи (защиты): | | |
|  | - Балльная оценка:  - Оценка: | |

Калуга, 2023

**Цель:** изучить основные принципы шифрования информации, ознакомиться с широко известными алгоритмами шифрования, приобрести навыки их программной реализации.

**Задачи:** изучить предложенный теоретический материал для получения информации об основных понятиях шифрования информации и освоения принципов действия алгоритмов шифрования. Выявить особенности данных алгоритмов, их эффективность и надежность. В соответствии с вариантом задания программно реализовать простейший алгоритм шифрования. Подготовить ответы на контрольные вопросы.

**Вариант 7**

Реализовать шифрование и дешифрацию содержимого файла по методу Гронсфельда с ключом произвольной длины. Ключ вводится с клавиатуры.

**Листинг:**

key = input("input key: ")

d = len(key)

n = 26

i = 0

file = open('input.txt', 'r')

text = file.read()

mode = int(input('input mode (0 - encrypt, 1 - decrypt): '))

if mode == 0:

    cypher = ""

    for l in text:

        if l.isalpha():

            m = ord(l.lower()) - 97

            k = int(key[i % d])

            cypher += chr((m + k) % n + 97)

        else:

            cypher += l

    print('cypher:', cypher)

elif mode == 1:

    source = ""

    for l in text:

        if l.isalpha():

            m = ord(l.lower()) - 97

            k = int(key[i % d])

            source += chr((m - k) % n + 97)

        else:

            source += l

    print('source:', source)

else:

    print('error')

**Результат:**



**Рис. 1.** Исходный текст



**Рис. 2.** Шифрование



**Рис. 3.** Дешифрация

**Вывод:** в ходе выполнения лабораторной работы были изучены основные принципы шифрования информации, широко известные алгоритмы шифрования, приобретены навыки их программной реализации.