

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

**Лабораторная работа № 2**

по дисциплине «Криптографические методы защиты информации»

на тему «Реализация алгоритма шифрования с использованием систем Цезаря и системы Трисемуса»

Выполнил обучающийся гр. ВКБ41

Деев Д.Д.

(Фамилия, Имя, Отчество)

Проверила:

Доцент Рощина Е.В.

(Должность, Фамилия, Имя, Отчество)

Ростов-на-Дону

2019

**Краткие теоретические сведения**

**1. В чем особенность шифров простой замены?**

В шифрах простой замены (одноалфавитной подстановки) каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста.

**2. Чем отличаются система шифрования Цезаря и аффинная система подстановок Цезаря?**

При шифровании с использованием аффинной системы подстановок Цезаря буква с порядковым номером t в соответствующем алфавите заменяется на букву, порядковый номер которой в этом же алфавите рассчитывается по формуле (at + b) mod m, где a, b – числовые ключи, а m – количество букв в алфавите.

**3. Какие требования предъявляются к выбору ключей для аффинной системы подстановок Цезаря?**

a и m должны быть взаимно простыми числами, то есть наибольший общий делитель a и m должен быть равен 1.

**4. Для каких шифров простой замены используется составной ключ?**

Система шифрования Трисемуса, система шифрования Цезаря с ключевым словом.

**5. Каким образом заполняется таблица подстановок для шифрования с использованием системы Трисемуса?**

В таблицу сначала по строкам вписывается ключевое слово, причем повторно встречающиеся в нем буквы не записываются. Затем эта таблица дополняется не вошедшими в нее буквами алфавита по порядку.

**Цель работы:** формирование умений шифрования с использованием систем Цезаря и системы Трисемуса.

**Ход работы (вариант 8)**

**Задание 1.** Зашифруйте сообщение «МЫ ДОЛЖНЫ ПРИЗНАТЬ ОЧЕВИДНОЕ: ПОНИМАЮТ ЛИШЬ ТЕ, КТО ХОЧЕТ ПОНЯТЬ», используя систему Цезаря со значением ключа соответствующим номеру варианта (например, для варианта 10 – ключ К = 10).

Ключ: 8

Программное средство было реализовано на языке Python 3.6. Результаты работы показаны на рисунке 1.

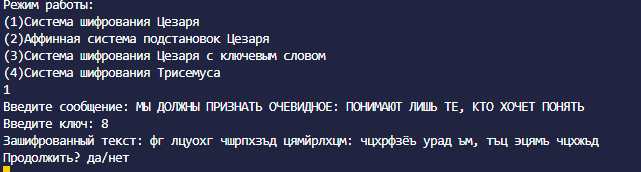


Рисунок 1 – Результат работы системы шифрования Цезаря

**Задание 2.** Зашифруйте сообщение «СМЫСЛ ЖИЗНИ НАШЕЙ – НЕПРЕРЫВНОЕ ДВИЖЕНИЕ», используя аффинную систему подстановок Цезаря с ключами.

Ключ: a = 4 b = 10

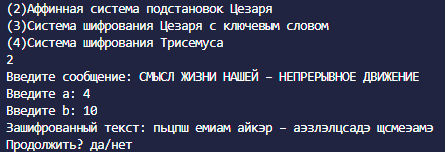


Рисунок 2 – Результат работы аффинной системы шифрования

**Задание 3.** Выполните шифрование сообщения «РАЗУМА ЛИШАЕТ НЕСОМНЕНИЕ, А УВЕРЕННОСТЬ», используя систему шифрования Цезаря с ключами

Ключ: 8

Ключевое слово: алгоритм

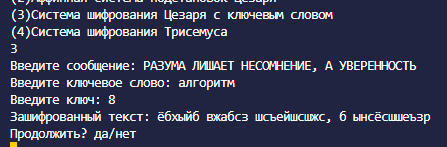


Рисунок 3 – Результат работы системы шифрования Цезаря с ключевым словом

**Задание 4.** Выполните шифрование сообщения «УСПЕХ – ЭТО КОГДА ТЫ ДЕВЯТЬ РАЗ УПАЛ, НО ДЕСЯТЬ РАЗ ПОДНЯЛСЯ», используя систему Трисемуса с ключевым словом из задания 3. Размер таблицы 4 × 8.

Ключевое слово: алгоритм

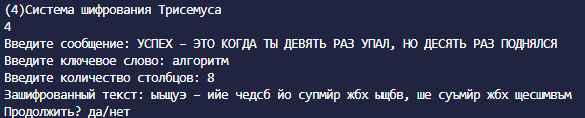


Рисунок 4 – Результат работы системы Трисемуса с ключевым словом

Количество строк находится автоматически из количества столбцов.

Листинг программного средства:

def cat(a, b, text, abc):

"""Цезарь, аффинный, Трисемус"""

list\_abc = []

length = len(abc)

for i in range(length):

list\_abc.append([abc[i], abc[(i \* a + b) % length]])

# print(list\_abc) # output table

print('Зашифрованный текст: ', end='')

for symbol in text:

if 1072 <= ord(symbol) < 1104 or symbol == 'ё':

for row in list\_abc:

if symbol in row[0]:

print(row[1], end="")

else:

print(symbol, end="")

print()

def remove\_duplicates(key, new\_key):

for symbol in key:

if symbol not in new\_key:

new\_key += symbol

return new\_key

def isint(s):

try:

int(s)

return int(s)

except ValueError:

print('Введите числовое значение')

s = isint(input())

return int(s)

def isstring(string):

try:

for i in string:

if i not in "абвгдеёжзийклмнопрстуфхцчшщъыьэюя":

int(None)

return string

except TypeError:

print('Введите строку, состоящую из букв русского алфавита')

strings = isstring(input().lower())

return string

if \_\_name\_\_ == "\_\_main\_\_":

while True:

ABC = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"

print('Режим работы:')

print('(1)Система шифрования Цезаря')

print('(2)Аффинная система подстановок Цезаря')

print('(3)Система шифрования Цезаря с ключевым словом')

print('(4)Система шифрования Трисемуса')

case = input()

if case == '1':

print('Введите сообщение: ', end='')

text = input().lower()

print('Введите ключ: ', end='')

b = isint(input())

cat(1, b, text, ABC)

elif case == '2':

print('Введите сообщение: ', end='')

text = input().lower()

print('Введите a: ', end='')

a = isint(input())

print('Введите b: ', end='')

b = isint(input())

cat(a, b, text, ABC)

elif case == '3':

print('Введите сообщение: ', end='')

text = input().lower()

print('Введите ключевое слово: ', end='')

key = isstring(input().lower())

print('Введите ключ: ', end='')

b = isint(input())

new\_key = ''

new\_key = remove\_duplicates(key, new\_key)

new\_key = remove\_duplicates(ABC, new\_key)

cat(1, b, text, new\_key)

elif case == '4':

print('Введите сообщение: ', end='')

text = input().lower()

print('Введите ключевое слово: ', end='')

key = isstring(input().lower())

print('Введите количество столбцов: ', end='')

b = isint(input())

new\_key = ''

new\_key = remove\_duplicates(key, new\_key)

new\_key = remove\_duplicates(ABC, new\_key).replace('ё', '')

cat(1, b, text, new\_key)

print('Продолжить? да/нет')

fail\_condition = input()

if fail\_condition == 'нет':

break

**Заключение.** В ходе выполнения лабораторной работы были получены навыки шифрования с использованием с использованием систем Цезаря и системы Трисемуса. Таким образом, цель работы была достигнута.