

Лабораторная работа 1

Серенко Данил Сергеевич, НФИмд-01-23

Содержание

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра математического моделирования и искусственного интеллекта

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

дисциплина: Математические основы защиты информации и информационной безопасности

Преподаватель: Кулябов Дмитрий Сергеевич

Студент: Серенко Данил Сергеевич

Группа: НФИмд-01-23

МОСКВА

2023 г.

Цель работы

Целью данной работы является приобретение практических навыков шифрования простой замены.[1]

Выполнение лабораторной работы

Требуется реализовать шифр Цезаря с произвольным ключом k и Реализовать шифр Атбаш.

Для этого я реализовал две программы на языке Python

Первая программа для шифра Цезаря.

```
##### ЦЕЗАРЬ #####

rus_alp = "а б в г д е ё 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"
rus_alp = rus_alp.split()
shift = 4
password = "пароль"
norm_message = "хочу каникулы и новый год"

def encode_cesar(message: str, pswd=password, alp=rus_alp, shift=shift) -> str:
    uniq_pswd = []
    for let in pswd:
        if let not in uniq_pswd:
            uniq_pswd.append(let)

    left_symbols = [symb for symb in alp if symb not in uniq_pswd]
    new_alp = left_symbols[-shift:] + uniq_pswd + left_symbols[:-shift]
    words = message.lower().split()
    tmp_message = []
    for word in words:
        encoded_word = ""
        for letter in word:
            encoded_word += new_alp[rus_alp.index(letter)]
        tmp_message.append(encoded_word)
    encoded_message = " ".join(tmp_message)
    return encoded_message
```

cesar1

```
def decode_cesar(message: str, pswd=password, alp=rus_alp, shift=shift) -> str:
    uniq_pswd = []
    for let in pswd:
        if let not in uniq_pswd:
            uniq_pswd.append(let)

    left_symbols = [symb for symb in alp if symb not in uniq_pswd]
    new_alp = left_symbols[-shift:] + uniq_pswd + left_symbols[:-shift]
    words = message.lower().split()
    tmp_message = []
    for word in words:
        decoded_word = ""
        for letter in word:
            decoded_word += rus_alp[new_alp.index(letter)]
        tmp_message.append(decoded_word)
    decoded_message = " ".join(tmp_message)
    return decoded_message

print(norm_message)
encoded_message = encode_cesar(norm_message)
print(encoded_message)
decoded_message = decode_cesar(encoded_message)
print(decoded_message + "\n")
```

cesar2

Затем я запустил программу, ввел пароль и сдвиг. Получил таблицу шифрования. Затем ввел предложение, которое нужно закодировать и получил зашифрованное сообщение. Вывод работы программы.

```
C:\Users\Nitro\AppData\Local\Programs\
хочу каникулы и новый год
нётк выеьвкгц ь еёюцб яёп
хочу каникулы и новый год

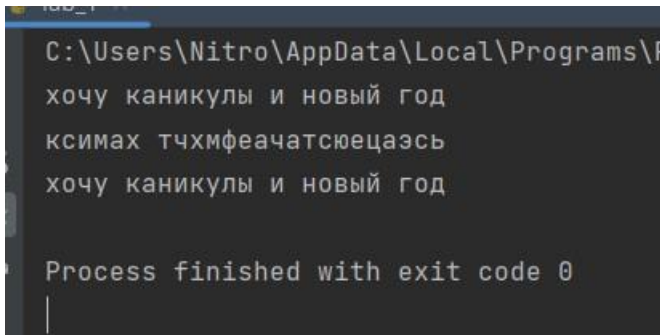
Process finished with exit code 0
```

cesar_out

Вторая программа для шифра Атбаш.

```
54 ##### АТБАШ #####
55
56 rus_alp_with_space = rus_alp.copy()
57 rus_alp_with_space.append(" ")
58
59
60 def encode_atbash(message: str, alp=rus_alp_with_space) -> str:
61     rev_alp = alp.copy()
62     rev_alp.reverse()
63
64     encoded_message = ""
65     for letter in message:
66         encoded_message += rev_alp[alp.index(letter)]
67     return encoded_message
68
69
70 def decode_atbash(message: str, pswd=password, alp=rus_alp_with_space, shift=shift) -> str:
71     rev_alp = alp.copy()
72     rev_alp.reverse()
73
74     decoded_message = ""
75     for letter in message:
76         decoded_message += alp[rev_alp.index(letter)]
77     return decoded_message
78
79
80 def decode_atbash(message: str, alp=rus_alp_with_space) -> str:
81     rev_alp = alp.copy()
82     rev_alp.reverse()
83
84     decoded_message = ""
85     for letter in message:
86         decoded_message += alp[rev_alp.index(letter)]
87     return decoded_message
88
89
90 print(norm_message)
91 encoded_message_atbash = encode_atbash(norm_message)
92 print(encoded_message_atbash)
93 decoded_message_atbash = decode_atbash(encoded_message_atbash)
94 print(decoded_message_atbash)
```

Вывод работы программы.



```
C:\Users\Nitro\AppData\Local\Programs\F
хочу каникулы и новый год
ксимах тчхмфеачатсюецаэсь
хочу каникулы и новый год

Process finished with exit code 0
```

atbash_out

Выводы

В результате выполнения работы я освоил на практике шифрование простой замены. Шифр Цезаря и Атбаш.

Список литературы

1. Методические материалы курса