

Лабораторная работа 1

Попов Дмитрий Павлович, НФИмд-01-23

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра математического моделирования и искусственного интеллекта

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

дисциплина: Математические основы защиты информации и информационной безопасности

Преподаватель: Кулябов Дмитрий Сергеевич

Студент: Попов Дмитрий Павлович

Группа: НФИмд-01-23

МОСКВА

2023 г.

Прагматика выполнения лабораторной работы

Прагматика выполнения лабораторной работы

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

Цель работы

Цель работы

Приобретение практических навыков шифрования простой замены.

Выполнение лабораторной работы

1. Реализовал программу для шифра
Цезаря (1/2)

1. Реализовал программу для шифра Цезаря (1/2)

```
lab_1_cesar.py x lab_1_atbash.py x
1 import sys
2
3 print("-----")
4 print(" Шифр Цезаря")
5 print("-----")
6
7 alphabet = "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"
8 alphabet = alphabet.split()
9 password = list(input("Введите пароль (неповторяющиеся буквы): ").lower())
10 k = int(input("Введите сдвиг k: "))
11 k = k % len(alphabet)
12
13 uniq_letters = list()
14 for letter in alphabet:
15     if letter not in password:
16         uniq_letters.append(letter)
17 if k == 0:
18     cypher = password + uniq_letters
19 elif k <= len(alphabet) - len(password):
20     cypher = uniq_letters[-k:] + password + uniq_letters[:len(uniq_letters)-k]
21 else:
22     print("Сдвиг неверный, нельзя поместить пароль полностью")
23     sys.exit()
```

1. Реализовал программу для шифра
Цезаря (2/2)

1. Реализовал программу для шифра Цезаря (2/2)

```
24
25 print("Таблица шифрования")
26 print(alphabet)
27 print(cypher)
28
29 while True:
30     mess = str(input("Введите предложение, которое нужно зашифровать (0 - для завершения шифрования): "))
31     if mess == '0':
32         print("Выход из шифрования...")
33         break
34
35     cypher_mess = str()
36     for symbol in mess:
37         if symbol == ' ':
38             cypher_mess += ' '
39         else:
40             cypher_mess += cypher[alphabet.index(symbol)]
41
42     print("    Введенное предложение: ", mess)
43     print("    Зашированное предложение: ", cypher_mess)
```

Figure 2: cesar2

2. Вывод работы первой программы

2. Вывод работы первой программы

```
lab_1_cesar
C:\Users\79119\AppData\Local\Programs\Python\Python310\python.exe C:\Users\79119\PycharmProjects\Inform_security_labs\src\lab_1_cesar.py
-----
Шифр Цезаря
-----
Введите пароль (неповторяющиеся буквы): пароль
Введите сдвиг k: 3
Таблица шифрования
['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']
['ы', 'э', 'ю', 'я', 'п', 'а', 'р', 'о', 'л', 'ь', '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']
Введите предложение, которое нужно зашифровать (0 - для завершения шифрования): я люблю помидоры
    Введенное предложение: я люблю помидоры
    Зашированное предложение: ь гцзгц жёдлпёзц
Введите предложение, которое нужно зашифровать (0 - для завершения шифрования): 0
Выход из шифрования...

Process finished with exit code 0
```

Figure 3: cesar_out

3. Реализовал программу для шифра
Атбаш

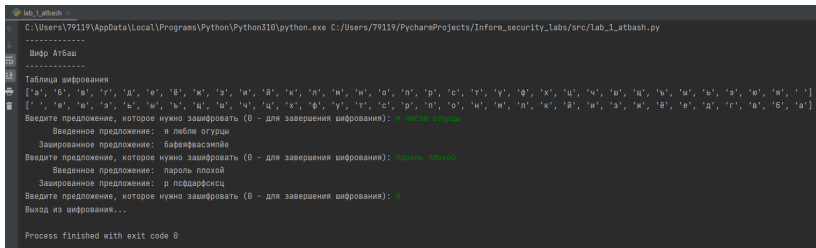
3. Реализовал программу для шифра Атбаш

```
lab_1_cesar.py x lab_1_atbash.py x
1 print("-----")
2 print(" Шифр Атбаш")
3 print("-----")
4
5 alphabet = "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"
6 alphabet = alphabet.split()
7 alphabet.append(' ')
8 cypher = alphabet.copy()
9 cypher.reverse()
10
11
12 print("Таблица шифрования")
13 print(alphabet)
14 print(cypher)
15
16 while True:
17     mess = str(input("Введите предложение, которое нужно зашифровать (0 - для завершения шифрования): "))
18     if mess == '0':
19         print("Выход из шифрования...")
20         break
21
22     cypher_mess = str()
23     for symbol in mess:
24         cypher_mess += cypher[alphabet.index(symbol)]
25
26     print("    Введенное предложение: ", mess)
27     print("    Зашированное предложение: ", cypher_mess)
```

Figure 4: atbash

4. Вывод работы второй программы

4. Вывод работы второй программы



```
Lab_1_atbash
C:\Users\79119\AppData\Local\Programs\Python\Python310\python.exe C:/Users/79119/PycharmProjects/Inform_security_labs/src/Lab_1_atbash.py
-----
Шифр Атбаш
-----
Таблица шифрования
['a', 'б', 'в', 'г', 'д', 'е', 'в', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ь', 'ы', 'я', 'э', 'ю', 'я', ' ' ]
[' ' , 'я', 'ю', 'э', 'ь', 'ы', 'щ', 'ш', 'ч', 'ц', 'х', 'ф', 'у', 'т', 'с', 'р', 'п', 'о', 'н', 'м', 'л', 'к', 'й', 'ж', 'з', 'и', 'я', 'б', 'а', 'в', 'г', 'д', 'е', 'ф', 'д', 'р', 'в', 'б', 'а']
Введите предложение, которое нужно зашифровать (0 - для завершения шифрования): я люблю огурцы
Зашированное предложение: бафявфваасзмйле
Введите предложение, которое нужно зашифровать (0 - для завершения шифрования): пароль плохой
Введенное предложение: лароль плохой
Зашированное предложение: р псфдарфскц
Введите предложение, которое нужно зашифровать (0 - для завершения шифрования): 0
Выход из шифрования...

Process finished with exit code 0
```

Figure 5: atbash_out

Вывод

Вывод

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

