

Лабораторная работа №1

Шифры простой замены

Доборщук В.В.

17 сентября 2022

Российский университет дружбы народов, Москва, Россия

Информация

- Доборщук Владимир Владимирович
- студент группы НФИмд-02-22, студ. билет 1132223451
- учебный ассистент кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- 1132223451@rudn.ru



Цели и задачи

Цель работы — изучить и программно реализовать шифры простой замены.

Задачами являются:

- Реализовать шифр Цезаря с произвольным ключом k ;
- Реализовать шифр Атбаш.

Теоретическое введение

В основе функционирования шифров простой замены лежит следующий принцип: для получения шифртекста отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита.

Шифр Цезаря является моноалфавитной подстановкой, т.е. каждой букве открытого текста ставится в соответствие одна буква шифротекста.

Математическая процедура шифрования описывается как

$$T_m = \{T^j\}, j = 0, 1, \dots, m - 1,$$

$$T^j(a) = (a + j) \mod m,$$

Сам же Цезарь обычно использовал подстановку T^3 .

Шифр Атбаш является сдвигом на всю длину алфавита. Правило шифрования состоит в замене i -й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите.

Выполнение лабораторной работы

Для реализации шифров мы будем использовать Python, так как его синтаксис позволяет быстро реализовать необходимые нам алгоритмы.

Реализация шифра Цезаря с произвольным ключом k

```
# --- Ceasar's Cipher ---
```

```
def ceasar(letter: chr, key: int, alphabet: list):
```

```
    def ceasar(letter: chr, key: int):
```

```
        return alphabet.index(letter) + key
```

```
    if letter.lower() not in alphabet:
```

```
        return letter
```

```
    t_letter = alphabet[ceasar(letter.lower(), key) % len(alphabet)]
```

```
    if letter.isupper():
```

```
        t_letter = t_letter.upper()
```

```
    return t_letter
```

```
# --- Atbash's Cipher ---
```

```
def atbash(letter: chr, alphabet: list):
```

```
    if letter.lower() not in alphabet:
```

```
        return letter
```

```
    t_letter = alphabet[len(alphabet) - alphabet.index(letter.lower()) - 1]
```

```
    if letter.isupper():
```

```
        t_letter = t_letter.upper()
```

```
    return t_letter
```

Для тестирования мы создали следующие функции:

```
# --- Tests ---
```

```
def test_caesar(message: str, key: int, alphabet: list):  
    ciphered_message = list(map(  
        lambda letter: caesar(letter, key, alphabet), message)  
    )  
    return "".join(ciphered_message)
```

```
def test_atbash(message: str, alphabet: list):  
    ciphered_message = list(map(  
        lambda letter: atbash(letter, alphabet), message)  
    )  
    return "".join(ciphered_message)
```

```
(base) wdoborschuk@wxcore ~/work/2022-2023/МО3ИИИБ/infosec/laboratory/lab01 (develop)$ python task.py

CEASAR'S CIPHER TEST 1
Original: Veni, vidi, vici
Ciphered: Yhql, ylgf, ylfj

CEASAR'S CIPHER TEST 2
Original: Happy New Year, my darling friend!
Ciphered: Kdssb Qhz Bhdz, pb gduolqj iulhqg!

ATBASH'S CIPHER TEST STRING OUTPUT
Original: абвгдезийклмнопрстуфхцщъыъэя
Ciphered: яюзыщцхцфутсрпоникизждгёба

ATBASH'S CIPHER TEST LIST OUTPUT
Original: ['a', 'б', 'в', 'г', 'д', 'е', 'з', 'и', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'щ', 'ъ', 'ы', 'э', 'я', ' ', '']
Ciphered: [' ', 'я', 'ю', 'э', 'б', 'м', 'в', 'щ', 'ш', 'ч', 'ц', 'х', 'ф', 'у', 'т', 'с', 'р', 'п', 'о', 'н', 'и', 'л', 'к', 'я', 'ж', 'з', 'ж', 'е', 'д', 'г', 'в', 'б', 'а']
```

Рис. 1: Вывод программы с реализованными шифрами простой замены

Для шифра Цезаря с ключом $k = 3$ получаем следующий результат:

CEASAR'S CIPHER TEST 1

Original: Veni, vidi, vici

Ciphered: Yhql, ylgf, ylfj

Дополнительно проверим механизм шифрования, передав другую строку из букв латинского алфавита:

CEASAR'S CIPHER TEST 2

Original: Happy New Year, my darling friend!

Ciphered: Kdssb Qhz Bhdu, pb gduolqj iulhqg!

Шифр Атбаш мы проверяем на кириллическом алфавите, содержащим также в себе символ пробела. Для проверки, передадим в него также весь русский алфавит с пробелом в виде одной строки:

ATBASH'S CIPHER TEST STRING OUTPUT

Original: абвгдежзийклмнопрстуфхцчщъыьэюя

Ciphered: яюэыъщчцхфутсрпонмлкйизжедгвба

Выведем полученный результат в формате списка, где сможем рассмотреть каждый обработанный символ отдельно:

ATBASH'S CIPHER TEST LIST OUTPUT

Original: ['a', 'б', 'в', 'г', 'д', 'е', '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', ' ']

Ciphered: [' ', 'я', 'ю', 'э', 'ь', 'ы', 'ъ', 'щ', 'ш', 'ч', 'ц', 'х', 'ф',
 'у', 'т', 'с', 'р', 'п', 'о', 'н', 'м', 'л', 'к', 'й', 'и', 'з',
 'ж', 'е', 'д', 'г', 'в', 'б', 'а']

Выводы

В рамках выполненной лабораторной работы мы изучили и реализовали следующие шифры простой замены: шифр Цезаря (с произвольным ключом k) и шифр Атбаш.