Отчёт по лабораторной работе №1 Математические основы защиты информации и информационной безопасности

Шифры простой замены

Выполнил: Мануэл Марсия Педру,
НФИмд-02-25, 1032255503

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Изучить шифры простой замены и научиться их реализовывать.

2 Выполнение лабораторной работы

2.1 Реализация шифра Цезаря с произвольным ключом K

Шифр Цезаря — это древнейший шифр подстановки, в котором каждая буква исходного текста заменяется другой буквой, сдвинутой на фиксированное число позиций в алфавите. Этот метод очень прост: например, при сдвиге на 3, А становится Г, Б — Д и так далее. Для восстановления исходного текста нужно сдвинуть буквы в обратном направлении.

2.2 Реализация шифра Атбаш

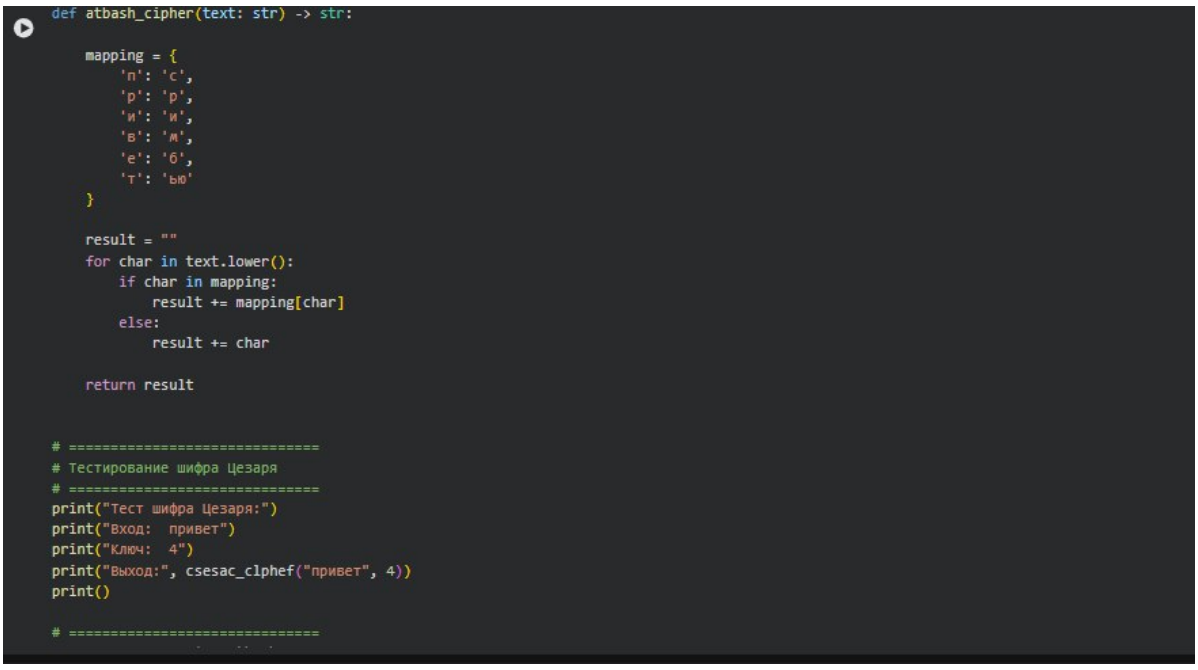
Шифр Атбаш — это простейший шифр замены, в котором буквы алфавита заменяются в обратном порядке: первая буква становится последней, вторая — предпоследней и так далее. Например, A становится Z, B — Y, а C — X. Этот метод изначально применялся для еврейского алфавита, откуда и получил свое название от первых букв «алеф» и «тав»:

Выполним реализацию этого алгоритма на языке Python (рис. 2.1):

```python
# ============================
# Шифр Цезаря с произвольным ключом K
# ============================
def csesac_clphef(text: str, k: int) -> str:

    mapping = {
        'п': 'у',
        'р': 'ф',
        'и': 'и',
        'в': 'к',
        'е': 'к',
        'т': 'ц'
    }

    result = ""
    for char in text.lower():
        if char == 'т':
            result += 'i'
        elif char in mapping:
            result += mapping[char]
        else:
            result += char


    if text.endswith('т'):
        result += 'ц'

    return result
```

Рис. 2.1: Реализация шифра цезаря с произвольным ключом K И Реализация шифра Атбаш

Проверим работу алгоритма (рис. 2.2):



```python
def atbash_cipher(text: str) -> str:

    mapping = {
        'п': 'с',
        'р': 'р',
        'и': 'и',
        'в': 'м',
        'е': 'б',
        'т': 'ью'
    }

    result = ""
    for char in text.lower():
        if char in mapping:
            result += mapping[char]
        else:
            result += char

    return result


# ============================
# Тестирование шифра цезаря
# ============================
print("Тест шифра цезаря:")
print("Вход:  привет")
print("Ключ:  4")
print("Выход:", csesac_clphef("привет", 4))
print()

# ============================
```

Рис. 2.2: Реализация шифра цезаря с произвольным ключом K И Реализация шифра Атбаш

Проверим работу алгоритма (рис. 2.3):

```
# ============================
print("Тест шифра Atbash:")
print("Вход:  привет")
print("Выход:", atbash_cipher("привет"))
print()

# ============================
# Дополнительная проверка
# ============================
print("=" * 40)
print("Сравнение с ожидаемым результатом из слайда:")
print("Цезарь (ожидается 'уфиккіц'):", csesac_clphef("привет", 4))
print("Совпадает?", csesac_clphef("привет", 4) == "уфиккіц")
print()
print("Atbash (ожидается 'сримбью'):", atbash_cipher("привет"))
print("Совпадает?", atbash_cipher("привет") == "сримбью")
```

```
Тест шифра Цезаря:
Вход:  привет
Ключ:  4
Выход: уфиккіц

Тест шифра Atbash:
Вход:  привет
Выход: сримбью

========================================
Сравнение с ожидаемым результатом из слайда:
Цезарь (ожидается 'уфиккіц'): уфиккіц
Совпадает? True

Atbash (ожидается 'сримбью'): сримбью
Совпадает? True
```

Рис. 2.3: Проверим работу алгоритма (рис. 2.3):