Лабораторная работа №1

Презентация

Миличевич Александра

15 февраля 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель работы

Познакомиться с шифрами Цезаря и Атбаш.

Задание

Задание

1. Реализовать шифр Цезаря с произвольным ключом k.
2. Реализовать шифр Атбаш.

Выполнение лабораторной работы

Шифр Цезаря

Шифр Цезаря — это один из самых простых и известных методов шифрования, который основан на сдвиге букв алфавита на фиксированное количество позиций. Например, при сдвиге на 3 буква “A” становится “D”, “B” — “E” и так далее, что делает его легко реализуемым, но уязвимым для криптоанализа. Несмотря на свою простоту, шифр Цезаря служит основой для более сложных методов шифрования и часто используется в образовательных целях для объяснения принципов криптографии.

1) Этот код реализует шифр Цезаря для шифрования текста. Он сдвигает каждую букву на указанное число позиций в алфавите, сохраняя регистр (заглавные или строчные). Все остальные символы, такие как цифры или знаки препинания, остаются без изменений. Формула `(ord(char) - ord('a') + shift) % 26 + ord('a')` используется для преобразования букв: она вычисляет позицию буквы в алфавите, добавляет сдвиг, возвращает результат в диапазон от 0 до 25 (циклично) и преобразует обратно в символ.

```python
# Шифр Цезаря: простой алгоритм шифрования сдвигом

def caesar_cipher(text, shift):
    """
    Функция для шифрования текста с использованием шифра Цезаря.
    :param text: исходный текст
    :param shift: сдвиг (целое число)
    :return: зашифрованный текст
    """
    result = ""  # Строка для хранения результата

    for char in text:
        # Проверяем, является ли символ буквой
        if 'a' <= char <= 'z':
            # Сдвиг для строчных букв
            new_char = chr((ord(char) - ord('a') + shift) % 26 + ord('a'))
            result += new_char
        elif 'A' <= char <= 'Z':
            # Сдвиг для заглавных букв
            new_char = chr((ord(char) - ord('A') + shift) % 26 + ord('A'))
            result += new_char
        else:
            # Если символ не буква, оставляем его без изменений
            result += char

    return result
```

Рис. 1: Шифр Цезаря

Этот код запрашивает у пользователя текст и значение сдвига, затем вызывает функцию `caesar_cipher` для шифрования текста и выводит результат на экран.

```
# Ввод текста от пользователя
input_text = input("Введите текст для шифрования: ")
shift_value = int(input("Введите значение сдвига: "))

# Шифруем текст
result = caesar_cipher(input_text, shift_value)
print("Зашифрованный текст:", result)
```

Рис. 2: вывод результата шифра Цезаря

Атбаш

Атбаш — это древний метод шифрования, который заключается в замене каждой буквы алфавита на букву, симметрично расположенную относительно его середины. Например, в латинском алфавите буква “A” заменяется на “Z”, “B” на “Y”, и так далее. Этот шифр использовался в исторических текстах и является одним из простейших методов шифрования.

3) Создание перевернутого алфавита

В строке `reverse_alphabet = alphabet[::-1]` создается перевернутый алфавит, где буквы идут в обратном порядке. Затем с помощью генератора словаря `cipher_dict` для каждой буквы из оригинального алфавита создается пара, сопоставляющая её с буквой из перевернутого алфавита.

```python
def atbash_cipher(text):
    # Создаем словарь для замены букв
    alphabet = "абвгдеёжзийклмнопрстуфхцчшщьыэюя"
    reverse_alphabet = alphabet[::-1]  # перевернутый алфавит

    # Создаем словарь для сопоставления букв
    cipher_dict = {alphabet[i]: reverse_alphabet[i] for i in range(len(alphabet))}
```

Рис. 3: reverse alphabet

4) Основной цикл шифрования

Этот код перебирает каждый символ в строке `text` (приведенной к нижнему регистру). Если символ — буква, она заменяется по словарю `cipher_dict`; если нет (например, пробел или знак препинания), символ остается без изменений. Все измененные символы собираются в список `result`, который затем объединяется в строку и возвращается.

```
# Преобразуем текст
result = []
for char in text.lower():
    if char in cipher_dict:
        result.append(cipher_dict[char])
    else:
        result.append(char)  # Не изменяем символ, если это не буква

# Возвращаем преобразованный текст
return ''.join(result)
```

Рис. 4: цикл главный

5) Вывод результата

Код шифрует строку `text` с помощью функции `atbash_cipher` и выводит исходный и зашифрованный текст.

```
# Пример использования
text = "всем хорошего дня!"
encoded = atbash_cipher(text)
print(f"Исходный текст: {text}")
print(f"Зашифрованный текст: {encoded}")
```

Рис. 5: вывод

Выводы

Реализованы шифр Цезаря и шифр Атбаш.