Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

«Техгологии и методы программирования»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5

Выполнил:
Михайлик Антон Денисович, студент группы N3351

(Подпись)

Проверил:
Ищенко Алексей Петрович

(Отметка о выполнении)

(Подпись)

Санкт-Петербург
2024 г.

Содержание

1 Техническое задание

Написать программу, реализующую два исторических примера алгоритмов шифрования. Продумать интерфейс, руководство пользователя и описание работы алгоритмов (их историей и криптоустойчивостью), для демонстрации алгоритмов пользователю со встроенными примерами текстов (шифруем и дешифруем), а также с возможностью ввода произвольного текста с его шифровкой дешифровкой.

Для данной лабораторной работы надо разработать программу для "Шифровка последовательностей нулей и единиц", что было усложнено до XOR шифрования и "Шифр Вижинера (для русских букв)".

Необходимо реализовать следующие этапы для каждого алгоритма:

1. Краткое описание алгоритма шифрования.
2. Определение ограничений на решаемую задачу.
3. Реализация данного алгоритма в виде программного кода.
4. Реализация и описание графического интерфейса.
5. Оформление отчета (включает описание выше и нижеизложенных пунктов со скриншотами работы программы и результатов).

2 Описание шифров

2.1 XOR

XOR (исключающее ИЛИ) — простой симметричный шифр, основанный на применении побитовой операции XOR между символами исходного текста и ключа. Основные особенности:

- Принцип работы: каждый символ текста преобразуется, используя соответствующий символ ключа (или ключ повторяется циклически).
- Шифрование и дешифрование идентичны: повторное применение операции XOR с тем же ключом восстанавливает исходное сообщение.
- Пример: для текста A (01000001 в бинарном виде) и ключа K (01001011), результат будет (00001010), что соответствует символу LF в ASCII.
- Применение: используется в простых системах шифрования, но уязвим для атак, если ключ короче текста или предсказуем.

2.2 Шифр Виженера (для русских букв)

Шифр Вижинера — это полиалфавитный шифр, использующий последовательность разных алфавитов для шифрования текста. Особенности его применения для русского алфавита:

- Принцип работы: каждый символ текста сдвигается по алфавиту на число позиций, соответствующее символу ключа. Русский алфавит насчитывает 33 буквы, поэтому сдвиг выполняется циклически.
- Шифрование:
  - Исходный текст: "ПРИВЕТ".
  - Ключ: "КОД". (повторяется циклически: "КОДКОД").
  - Результат:
    - П + К = Т
    - Р + О = Ф
    - И + Д = Л
    - и т.д.
  - Итоговый текст: "ТФЛЬЗФ".
- Дешифрование: выполняется обратным сдвигом на число позиций ключа.
- Преимущества: стойкость выше, чем у простого шифра Цезаря.
- Недостатки: уязвим к частотному анализу, если ключ короткий.
- Этот шифр часто используется в учебных целях для изучения основ криптографии.

3 Реализация и пример работы

Весь код приведён в приложении к лабораторной работе

3.1 XOR шифрование/дешифрование

Реализация

Функция xor_encrypt_decrypt шифрует или дешифрует текст, используя XOR-операцию. Ключ применяется циклически, чтобы обработать весь текст. Каждая буква преобразуется с помощью побитового исключающего ИЛИ между её кодом ASCII и соответствующим кодом символа ключа.

Пример работы

- Входные данные:

- Текст: hello
- Ключ: key

- Шифрование:
  - ASCII-коды текста: [104, 101, 108, 108, 111]
  - ASCII-коды ключа (циклично): [107, 101, 121, 107, 101]
  - Результат XOR: [3, 0, 21, 3, 10]
  - Итоговая строка: "\x03\x00\x15\x03\n" (защищённая форма текста).

- Дешифрование:
  - Применяя тот же ключ, исходный текст восстанавливается.

3.2 Шифр Виженера

Реализация

Функция vigenere_cipher использует алфавит из русских букв. В зависимости от режима работы (encrypt или decrypt), символы текста сдвигаются на позиции, определяемые соответствующими символами ключа.

Алгоритм шифрования:

1. Для каждого символа текста находится его индекс в алфавите.
2. Индексы символов ключа повторяются циклически.
3. При шифровании символ текста сдвигается вперёд на количество позиций ключа.
4. При дешифровании символ текста сдвигается назад.

Пример работы

- Входные данные:
  - Текст: привет
  - Ключ: ключ

- Шифрование:
  - Индексы текста: [16, 17, 8, 3, 5, 19] (позиции букв в русском алфавите).
  - Индексы ключа (циклично): [10, 11, 23, 10, 11, 23].
  - Результат: [26, 28, 31, 13, 16, 16] → Символы: ьфчкпп.

- Итог: Зашифрованный текст — ьфчкпп.

3.3 Пример работы программы

Программа позволяет выбрать один из алгоритмов, режим работы (шифрование/дешифрование) и способ ввода текста (вручную или из файла). Результат выводится на экран или записывается в указанный файл.

Пример работы программы:

Рис. 1: Создаём файл, который будем кодировать с помощью XOR

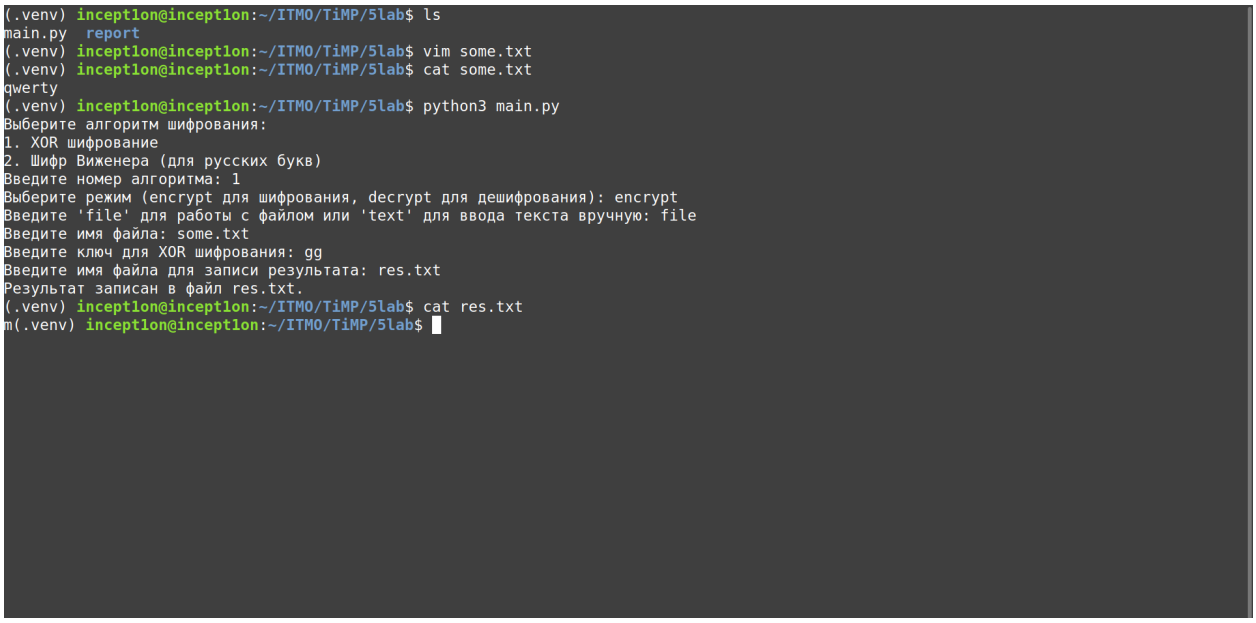

Рис. 2: Шифруем файл

Для сравнения покажем, как выглядят файлы в байтах, чтобы удостовериться, что всё зашифровано правильно.

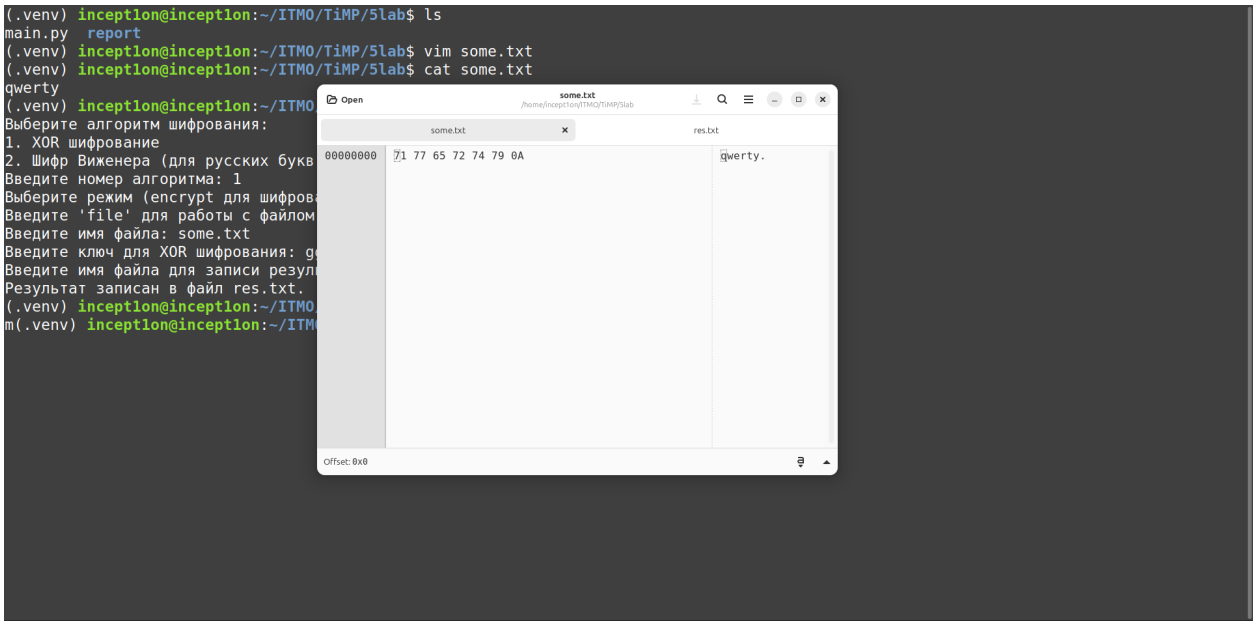

Рис. 3: Файл some.txt

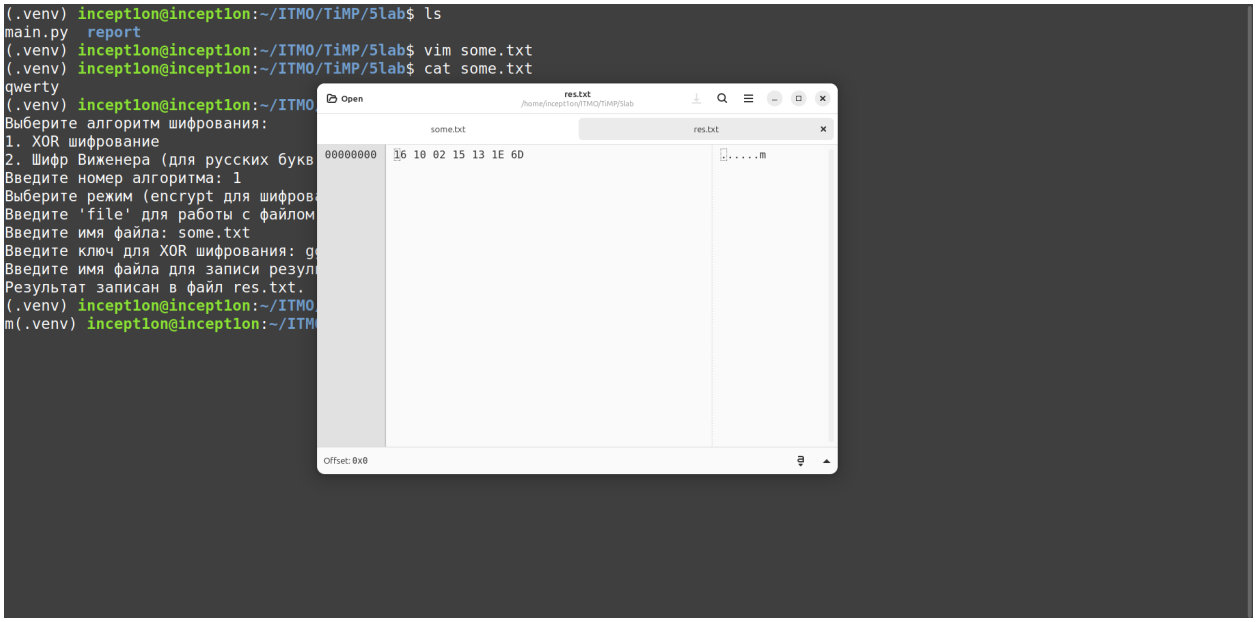

Рис. 4: Файл res.txt

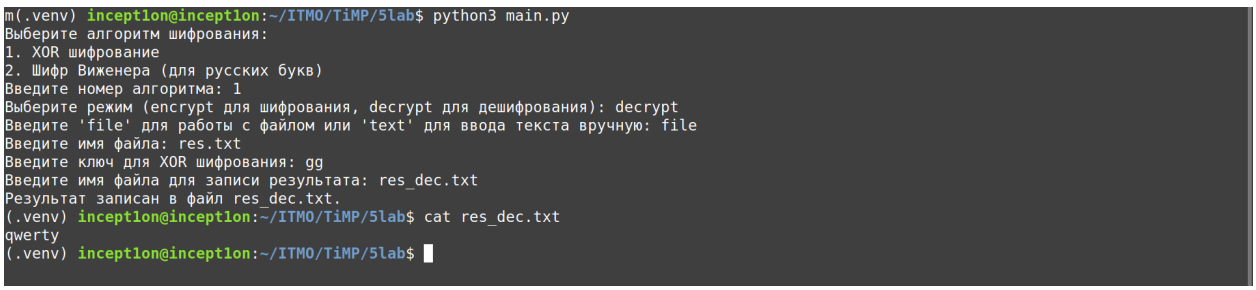

Рис. 5: Расшифровка файла

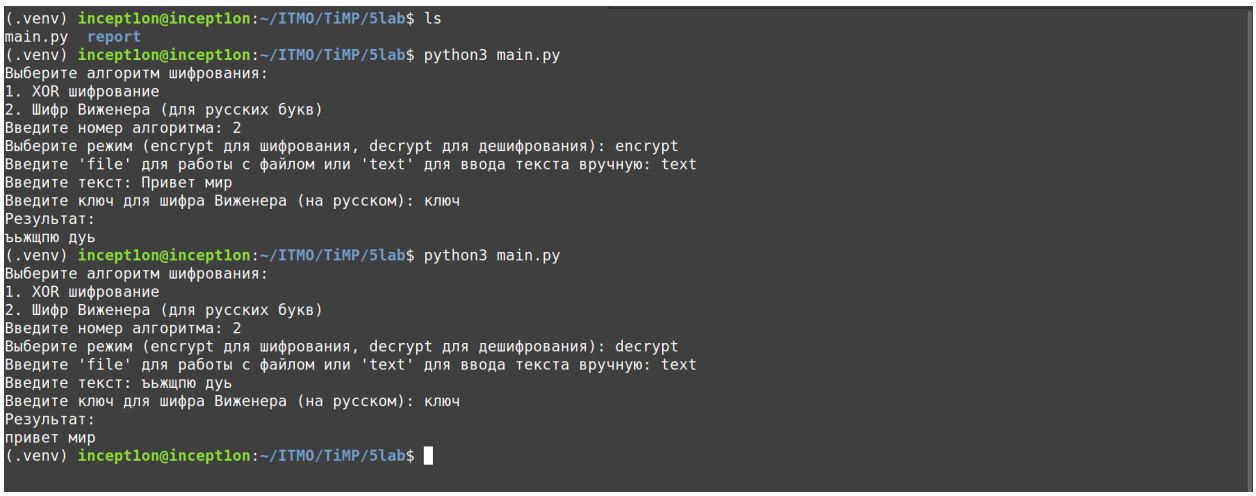

Рис. 6: Шифрование и расшифровка с помощью шифра Виженера

4 Заключение

В ходе выполнения лабораторной работы были реализованы два исторических алгоритма шифрования: XOR и шифр Виженера для русского алфавита. Программа демонстрирует процесс шифрования и дешифрования, позволяя работать как с предустановленными примерами, так и с пользовательскими текстами.

Была проведена работа по следующим направлениям:

1. Изучены принципы работы выбранных алгоритмов, их криптоустойчивость и ограничения. Для XOR характерна простота реализации, но низкая стойкость при использовании короткого или одноразового ключа. Шифр Виженера предоставляет более высокую устойчивость за счёт использования многоалфавитного подхода, но подвержен атаке Касиски при известных длинных текстах.

2. Разработан программный код для шифрования и дешифрования текстов, включая поддержку русского языка.

3. Создан удобный пользовательский интерфейс, обеспечивающий выбор алгоритма, режим шифрования/дешифрования, ввод текста и ключа, а также сохранение результатов в файлы.

4. Реализованы встроенные примеры для демонстрации работы алгоритмов, что облегчает восприятие их принципов.

5. Проведено тестирование программы, продемонстрирована её работоспособность на различных входных данных.

5 Приложение

```python
import os


def xor_encrypt_decrypt(text, key):
    """
    XOR шифрование/дешифрование.
    """
    key_length = len(key)
    key_as_int = [ord(k) for k in key]
    text_as_int = [ord(t) for t in text]
    result = ''.join(chr(t ^ key_as_int[i % key_length]) for i, t in
   enumerate(text_as_int))
    return result


def vigenere_cipher(text, key, mode):
    """
    Шифр Виженера для русских букв.
    """
    alphabet = 'абвгдеёжзийклмнопрстуфхцчшщъыьэюя'
    result = []
    key = key.lower()
    key_indices = [alphabet.index(k) for k in key]

    for i, char in enumerate(text.lower()):
        if char in alphabet:
            char_idx = alphabet.index(char)
            key_idx = key_indices[i % len(key)]
            if mode == "encrypt":
                new_char = alphabet[(char_idx + key_idx) % len(alphabet)]
            elif mode == "decrypt":
                new_char = alphabet[(char_idx - key_idx) % len(alphabet)]
            result.append(new_char)
        else:
            result.append(char)

    return ''.join(result)


def read_from_file(filename):
    with open(filename, 'r', encoding='utf-8') as file:
        return file.read()


def write_to_file(filename, content):
    with open(filename, 'w', encoding='utf-8') as file:
        file.write(content)


def main():
    print("Выберите алгоритм шифрования:")
    print("1. XOR шифрование")
    print("2. Шифр Виженера (для русских букв)")
    choice = input("Введите номер алгоритма: ").strip()

    if choice not in {'1', '2'}:
        print("Неверный выбор. Завершение программы.")
        return
```

```
58
59      mode = input("Выберите режим (encrypt для шифрования, decrypt для деши
        фрования): ").strip().lower()
60      if mode not in {'encrypt', 'decrypt'}:
61          print("Неверный режим. Завершение программы.")
62          return
63
64      source = input("Введите 'file' для работы с файлом или 'text' для ввод
        а текста вручную: ").strip().lower()
65      if source == 'file':
66          filename = input("Введите имя файла: ").strip()
67          if not os.path.exists(filename):
68              print("Файл не найден.")
69              return
70          text = read_from_file(filename)
71      elif source == 'text':
72          text = input("Введите текст: ").strip()
73      else:
74          print("Неверный ввод.")
75          return
76
77      if choice == '1':
78          key = input("Введите ключ для XOR шифрования: ").strip()
79          if not key:
80              print("Ключ не может быть пустым.")
81              return
82          result = xor_encrypt_decrypt(text, key)
83      elif choice == '2':
84          key = input("Введите ключ для шифра Виженера (на русском): ").
        strip()
85          if not key.isalpha() or not all(c in 'абвгдеёжзийклмнопрстуфхцчшщъ
        ыьэюя' for c in key.lower()):
86              print("Ключ должен содержать только русские буквы.")
87              return
88          result = vigenere_cipher(text, key, mode)
89
90      if source == 'file':
91          output_file = input("Введите имя файла для записи результата: ").
        strip()
92          write_to_file(output_file, result)
93          print(f"Результат записан в файл {output_file}.")
94      else:
95          print("Результат:")
96          print(result)
97
98
99  if __name__ == "__main__":
100     main()
```

Листинг 1: Код для работы программы по шифрованию