Отчёт по выполнению практического занятия №2
Повышение криптостойкости шифров подстановки

1. Введение

В рамках практического занятия была поставлена задача изучения и реализации трёх алгоритмов шифрования, основанных на методах подстановки. Данное занятие направлено на повышение криптостойкости классических шифров посредством использования многобуквенного шифрования и полиалфавитных систем.

2. Цели занятия

Основными целями работы являются:

- Изучение принципов работы шифра Плейфейера, шифра Хилла и шифра Виженера.
- Реализация алгоритмов шифрования и расшифрования для каждого из методов на языке Python.
- Анализ преимуществ и недостатков каждого шифра с точки зрения криптостойкости.
- Формирование навыков работы с алгоритмами, основанными на подстановке, и их реализации в виде программного проекта.

3. Описание реализованных шифров

3.1. Шифр Плейфейера

Шифр Плейфейера использует матрицу 5×5, в которой буквы I и J считаются одинаковыми.
Основные этапы алгоритма:

- Генерация матрицы на основе ключевого слова (английское слово не менее 7 букв).
- Разбиение исходного текста на биграммы (пары букв) с учетом правил: если в паре повторяются буквы, между ними вставляется буква-заполнитель (например, X).
- Применение правил замены: если буквы находятся в одной строке или столбце, производится циклический сдвиг, иначе – происходит замена по пересечению строк и столбцов.

3.2. Шифр Хилла

Шифр Хилла является блочным шифром, основанным на использовании матричного умножения по модулю 26.
Основные этапы алгоритма:

- Преобразование исходного текста (фамилия, имя, отчество на английском) в числовой вектор, где A=0, B=1, …, Z=25.

- Разбиение текста на блоки по 3 символа. При необходимости блок дополняется символом (например, X).
- Шифрование каждого блока с помощью умножения на произвольную матрицу-ключ (размером 3×3, определитель которой не равен нулю) по модулю 26.
- Для расшифрования вычисляется обратная матрица (также по модулю 26), после чего происходит обратное преобразование.

3.3. Шифр Виженера

Шифр Виженера – это полиалфавитный шифр, использующий принцип циклического повторения ключевого слова, которым в данном задании является полное имя пользователя.
Основные этапы алгоритма:

- Форматирование исходного текста (приведение к верхнему регистру, удаление пробелов).
- Расширение ключа до длины исходного текста путём циклического повторения.
- Шифрование: для каждой буквы исходного текста вычисляется сумма её порядкового номера и номера соответствующей буквы ключа по модулю 26.
- Аналогичным образом производится расшифрование, вычитая значения букв ключа.

4. Структура проекта

Проект реализован на языке Python и состоит из нескольких модулей, каждый из которых отвечает за определённый алгоритм шифрования. Структура проекта следующая:

```
project/
├── main.py          # Точка входа, меню выбора шифрования/расшифрования
├── playfair.py      # Реализация алгоритма шифра Плейфейера
├── hill.py          # Реализация алгоритма шифра Хилла (операции с матрицами)
├── vigenere.py      # Реализация алгоритма шифра Виженера
└── README.md        # Документация проекта
```

В файле `main.py` реализовано меню, позволяющее выбрать режим работы (шифрование или расшифрование) и соответствующий алгоритм. Каждый модуль содержит функции для шифрования и расшифрования, а также вспомогательные функции (например, генерация матрицы для шифра Плейфейера, преобразование текста в числовой вектор для шифра Хилла).

5. Тестирование и результаты

В процессе тестирования проекта были выполнены следующие шаги:

- **Плейфейер:**
  - Введён ключевое слово (например, «monarchy»).

    - Протестированы случаи с повторяющимися символами и корректность обработки биграмм.
- **Хилл:**
    - Введён тестовый ключ (матрица 3×3 с ненулевым определителем).
    - Проверена корректность шифрования и обратного преобразования посредством вычисления обратной матрицы по модулю 26.
- **Виженер:**
    - Использовано полное имя пользователя в качестве ключа.
    - Проведена проверка корректного циклического повторения ключа и правильного сдвига букв.

Все тесты показали, что реализованные алгоритмы работают корректно, а исходный текст можно восстановить из зашифрованного сообщения с использованием соответствующего ключа.

6. Заключение

В результате выполнения практического занятия были получены следующие итоги:

- Изучены принципы работы трёх классических шифров, основанных на подстановке.
- Реализованы алгоритмы шифрования и расшифрования для шифров Плейфейера, Хилла и Виженера.
- Проект структурирован по принципам модульности, что позволяет легко расширять функциональность и добавлять новые алгоритмы.
- Полученные навыки могут быть использованы для дальнейших исследований в области криптографии и разработки более сложных систем защиты информации.