Front matter

title: "Отчёт по лабораторной работе № 1" subtitle: "Математические основы защиты информации и информационной безопасности" author: "Надиа Эззакат"

Цель работы

Целью данной лабораторной работы является реализация и тестирование двух шифров на Python: **Цезаря** и **Атбаша**. Мы изучаем их применение для шифрования текста, а также рассматриваем принципы работы данных алгоритмов.

Теоретическое введение

Шифр Цезаря

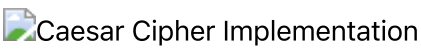
Шифр Цезаря – это один из самых простых и широко известных методов шифрования. Он заключается в замене каждой буквы текста на букву, которая находится на фиксированное количество позиций дальше по алфавиту. Например, если сдвиг составляет 3, то «А» становится «Г», «Б» – «Д» и так далее. Шифрование Цезаря циклично, то есть после «Я» начинается «А».

Шифр Атбаш

Шифр Атбаш – это простой подстановочный шифр, где первая буква алфавита заменяется последней, вторая – предпоследней и так далее. Например, «А» заменяется на «Я», «Б» на «Ю», и так далее. Этот шифр является симметричным, что означает, что для его расшифровки используется тот же алгоритм, что и для шифрования.

Выполнение лабораторной работы

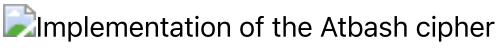
Реализация шифра Цезаря

 Caesar Cipher Implementation

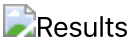
Результаты:

 Results

Реализация шифра Атбаш

 Implementation of the Atbash cipher

Результаты:

 Results

Выводы

В ходе выполнения лабораторной работы были реализованы и протестированы два шифра: Цезаря и Атбаш.

Шифр Цезаря позволяет сдвигать буквы текста на заданное количество позиций, что обеспечивает базовое шифрование. Его реализация проста и может быть адаптирована для различных алфавитов и языков. Шифр Атбаш выполняет зеркальную замену букв, что делает его одним из самых простых шифров с симметричной структурой. Он также легок в реализации и понимании. Оба шифра продемонстрировали свою эффективность в шифровании и расшифровке текста, однако их безопасность на практике достаточно низка, и они могут быть легко взломаны с помощью современных методов криптоанализа.