

Цель работы

Цель данной лабораторной работы заключается в ознакомлении с основами алгоритмов шифрования текста, а именно шифрования Цезаря и Атбаш, а также в их реализации. Целью является изучение принципов работы данных методов шифрования и их практическое применение

Задание

Реализовать алгоритма шифра Цезаря. Реализовать алгоритма шифра Атбаш.

Теоретическое введение

Шифр Цезаря — это один из простейших и наиболее известных методов шифрования текста. Он назван в честь римского полководца Гая Юлия Цезаря, который, согласно легенде, использовал этот метод для секретной переписки.

Принцип работы шифра Цезаря основан на сдвиге букв алфавита на определенное число позиций. Каждая буква заменяется на букву, идущую в алфавите после сдвига на заданное число позиций.

Пример шифрования: сдвиг алфавита на 3 позиции (shift = 3): Оригинальное сообщение: HELLO Зашифрованное сообщение: KNOOR

Шифр Атбаш — это шифр замены, в котором каждая буква заменяется на свою "зеркальную" букву в алфавите. Алфавит разбивается пополам, и каждая буква заменяется на соответствующую букву из противоположной половины алфавита.

Пример шифрования: Оригинальное сообщение: HELLO Зашифрованное сообщение: SV00L

Применение Оба эти метода шифрования используются для простого скрытия содержания текста от посторонних глаз. Они особенно полезны в случаях, когда требуется быстро зашифровать или расшифровать текст без сложных вычислений.

Выполнение лабораторной работы

1. Реализация алгоритма шифра Цезаря Для реализации алгоритма шифра Цезаря потребуется функция, которая принимает на вход текст и количество позиций для сдвига в алфавите. Внутри функции осуществляется итерация по каждому символу входного текста. Если символ является буквой, то он сдвигается на указанное количество позиций в алфавите. Не буквенные символы остаются неизменными.
2. Реализация алгоритма шифра Атбаш Для реализации алгоритма шифра Атбаш потребуется функция, которая принимает на вход текст. Внутри функции осуществляется итерация по каждому символу входного текста. Если символ является буквой, то он заменяется на свое зеркальное отражение в алфавите (например, 'a' заменяется на 'z', 'b' на 'y' и т.д.). Не буквенные символы остаются неизменными.

Таким образом, каждый алгоритм можно реализовать в виде функции, которая принимает входные данные (текст или символы) и возвращает зашифрованный текст согласно

соответствующему алгоритму шифрования

Выводы

Были реализованы алгоритмы шифров Цезаря и Атбаш на языке Kotlin

Список литературы

1. Методические материалы курса