Лабораторная работа №1

Логинов Сергей

Цели и справочная информация

Шифрование – это такое преобразование исходного сообщения, которое не позволит всяким нехорошим людям прочитать данные, если они это сообщение перехватят. Делается это преобразование по специальным математическим и логическим алгоритмам.

Атбаш — простой шифр подстановки.

Правило шифрования состоит в замене i-й буквы алфавита буквой с номером n − i + 1, где n — число букв в алфавите.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3 А была бы заменена на Г, Б станет Д, и так далее.

- `y = (x + k) mod n`
- `x = (y - k + n) mod n`
- где *x — символ открытого текста,* y — символ шифрованного текста *n — мощность алфавита* k — ключ.

Результаты

```
(base) lalogin@MacBook-Air-Sergej work % /opt/homebrew/bin/python3 /Users/lalogin/work/work/2022-2023/cyber_sec/lab_1/lab1
Enter step: 3
Enter text: Road so far
UrdgCvrCidu
Enter step: 3
Enter text: UrdgCvrCidu
Road so far
Enter text: Road so far
jMaXAIMAVaJ
Enter text: jMaXAIMAVaJ
Road so far
(base) lalogin@MacBook-Air-Sergej work %
```

Вывод

Изучили алгоритмы шифрования Цезаря и Атбаш

Реализовали алгоритмы шифрования и дешифровки на языке Python