Отчет по лабораторной работе 1

По предмету мат. основы защиты информации

Дидусь Кирилл Валерьевич

Содержание

# Цель работы

* Изучить простейшие методы шифрования
* Рассмотреть функционирование шифров простой замены

# Задание

* Реализовать шиф Цезаря с произвольным ключом k
* Реализовать шифр Атбаш

# Теоретическое введение

* Атба́ш (ивр. ‏אתבש‏‎) — простой шифр подстановки для алфавитного письма. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером n−i+1 {n-i+1}, где n — число букв в алфавите. Впервые встречается в древнееврейском тексте Библии / Танаха.
* 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 вправо на 3, А была бы заменена на Г, Б станет Д, и так далее. Шифр назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

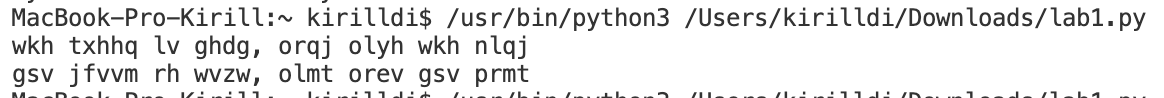
# Выполнение лабораторной работы

Выполнил программную реализацию шифров простой замены. Реализация выполнена в среде разработки Visial Studio Code на языке python (рис.1 [-@fig:001])



Программа

Сообщение ‘the queen is dead, long live the king’ было закодирована двумя шифрами. Зашифрованное сообщение представлено на рисунке (рис.2 [-@fig:002])



Вывод

# Выводы

Изучил реализацию шифров простой замены

# Список литературы