Отчёта по лабораторной работе №4

дисциплина: Информационная безопасность

Кашкин Иван Евгеньевич

Содержание

[Цель работы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202532)

[Задание](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202533)

[Теоретическое введение](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202534)

[Выполнение лабораторной работы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202535)

[Выводы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202536)

[Список литературы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202537)

# Цель работы

Изучение алгоритма шифрования гаммированием

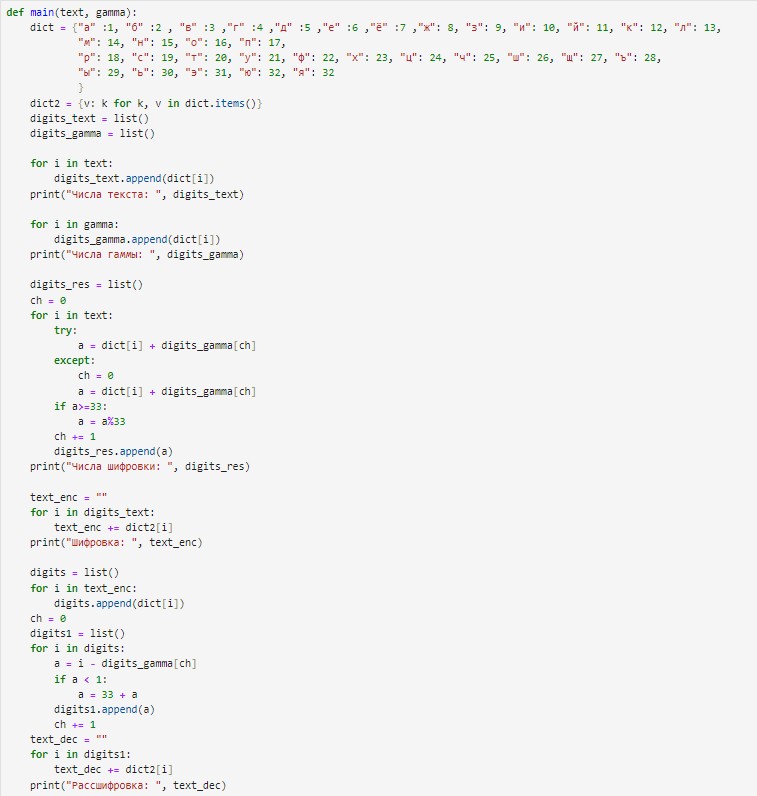
# Теоретические сведения

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

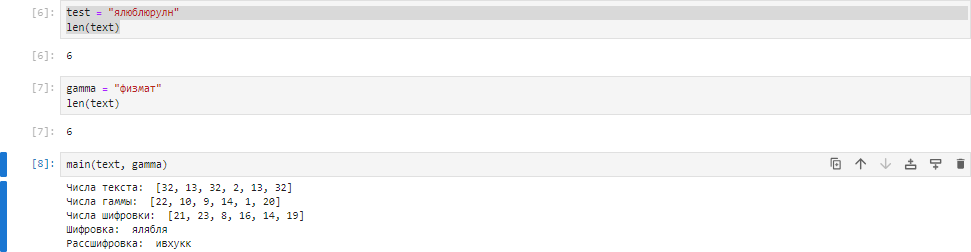
Метод гаммирования становится бессильным, если известен фрагмент исходного текста и соответствующая ему шифрограмма. В этом случае простым вычитанием по модулю 2 получается отрезок псевдослучайной последовательности и по нему восстанавливается вся эта последовательность.

# Выполнение работы

**Реализация шифратора и дешифратора Python**



# Контрольный пример



**Выводы**

Изучили алгоритмы шифрования на основе гаммирования

# Список литературы{.unnumbered}

1. [Шифрование методом гаммирования](http://altaev-aa.narod.ru/security/XOR.html)
2. [Режим гаммирования в блочном алгоритме шифрования](https://kabinfo.ucoz.ru/index/shifr_reshetka_kardano/0-374)