Отчёт по лабораторной работе 8

Тейшейра Боа Морте Селмилтон

Содержание

[4.1. Цель работы 1](#_Toc149425182)

[4.2. Порядок выполнения работы 1](#_Toc149425183)

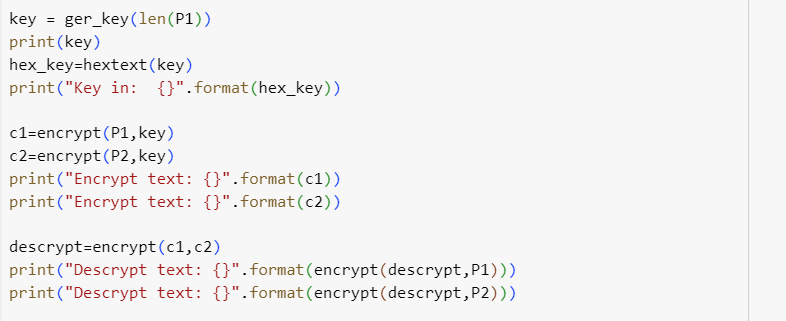
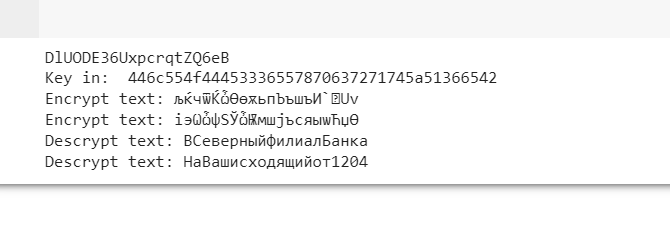
[Выводы 3](#_Toc149425184)

## 4.1. Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

## 4.2. Порядок выполнения работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

## Выводы

Научил как Освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.