Лабораторная работа № 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Ильин Никита Евгеньевич, НФИбд-01-19

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом [1].

# 2 Задание

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

# 3 Выполнение работы

1. Была написана программа, которая соответствует требованиям задачи, и проверяет полученный ключ с изначально сгенерированным.

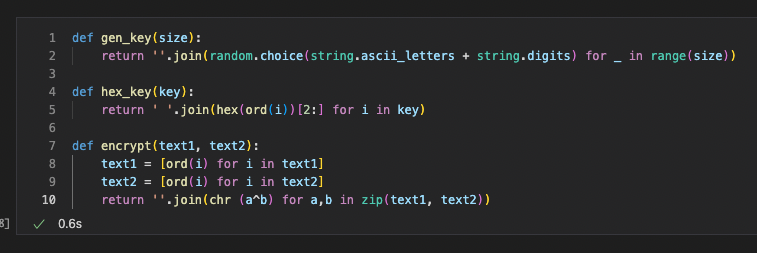


Figure 1: функции

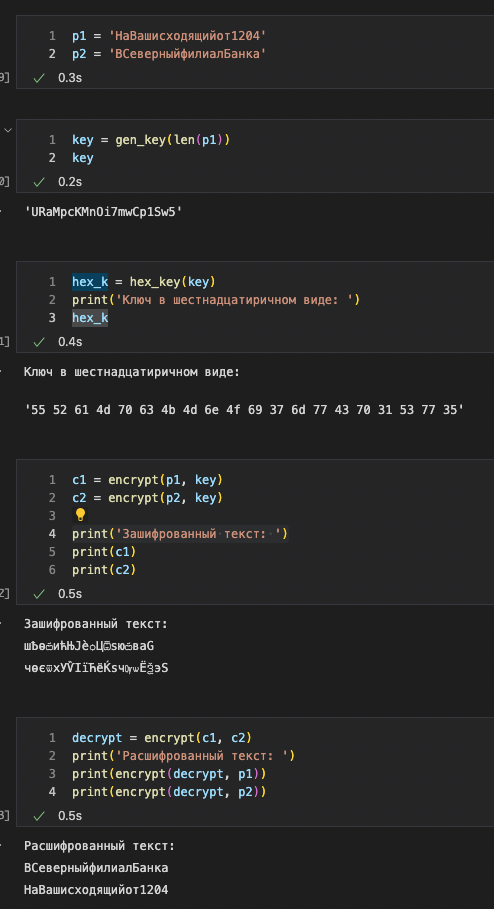


Figure 2: работа программы

# 4 Выводы

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

# 5 Библиография

1. Методические материалы курса