Ощепков Дмитрий Владимирович НКАбд-02-22

Дисциплина: Основы информационной безопасности

Лабораторная работа №8

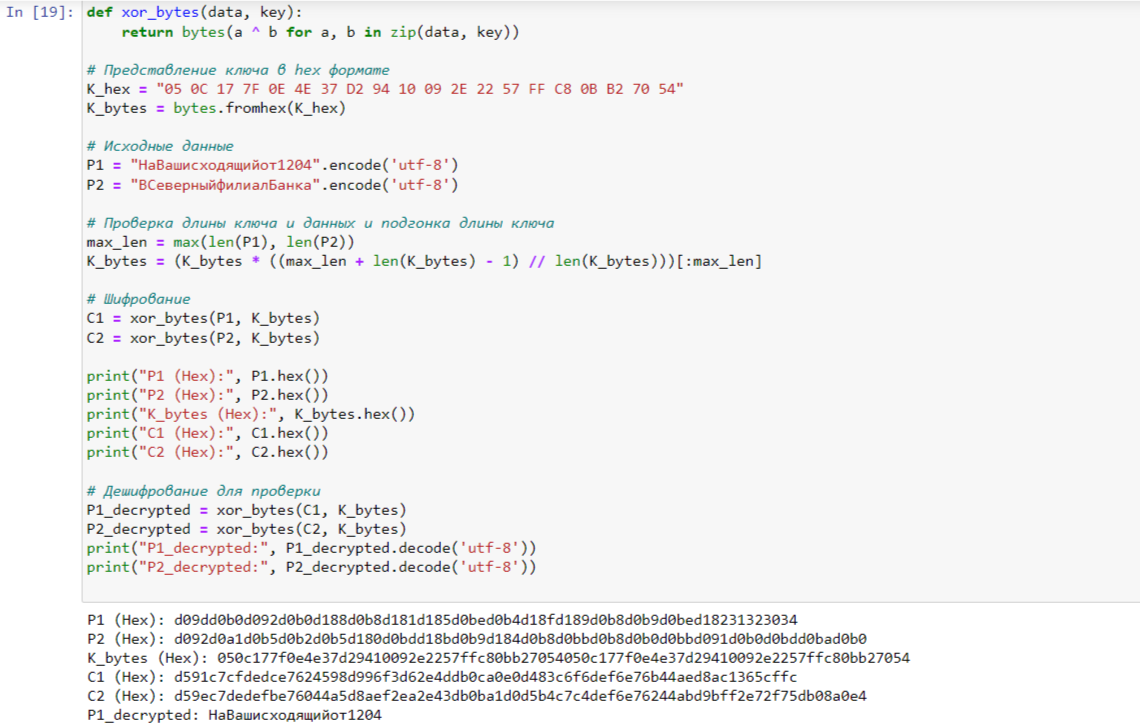
Цель работы: освоить на практике применение режима однократного гаммирования

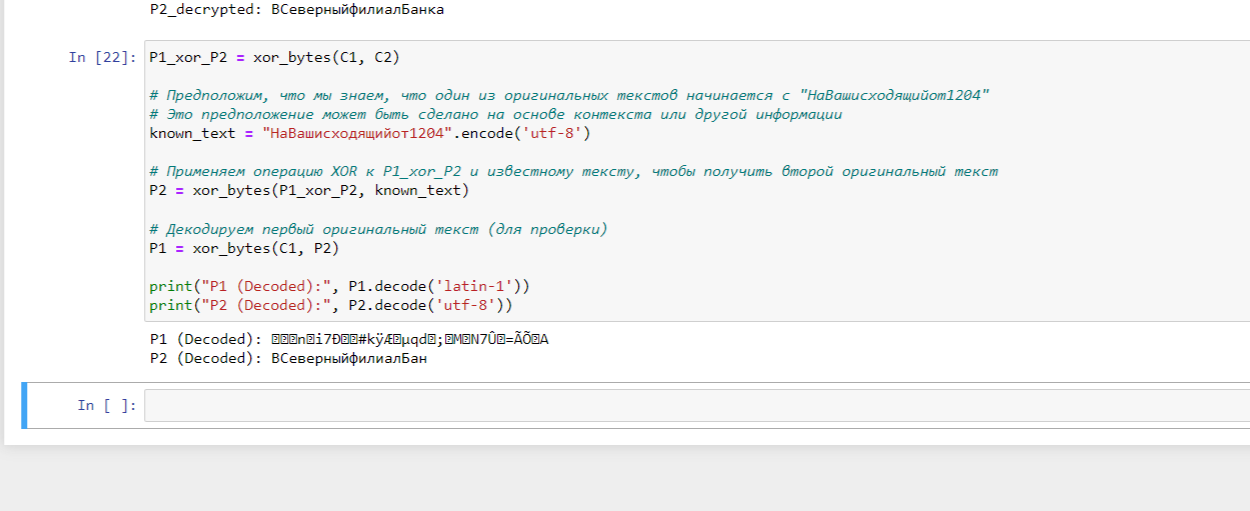
Порядок выполнения работы:

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

Приложение должно:

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.





Вывод: освоил на практике применение режима однократного гаммирования.