Отчёт по лабораторной работе №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Кондрашина Мария Сергеевна

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы. Создание программы

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

1. Перевод открытых текстов в шестнадцатеричное представление. (fig. 1)

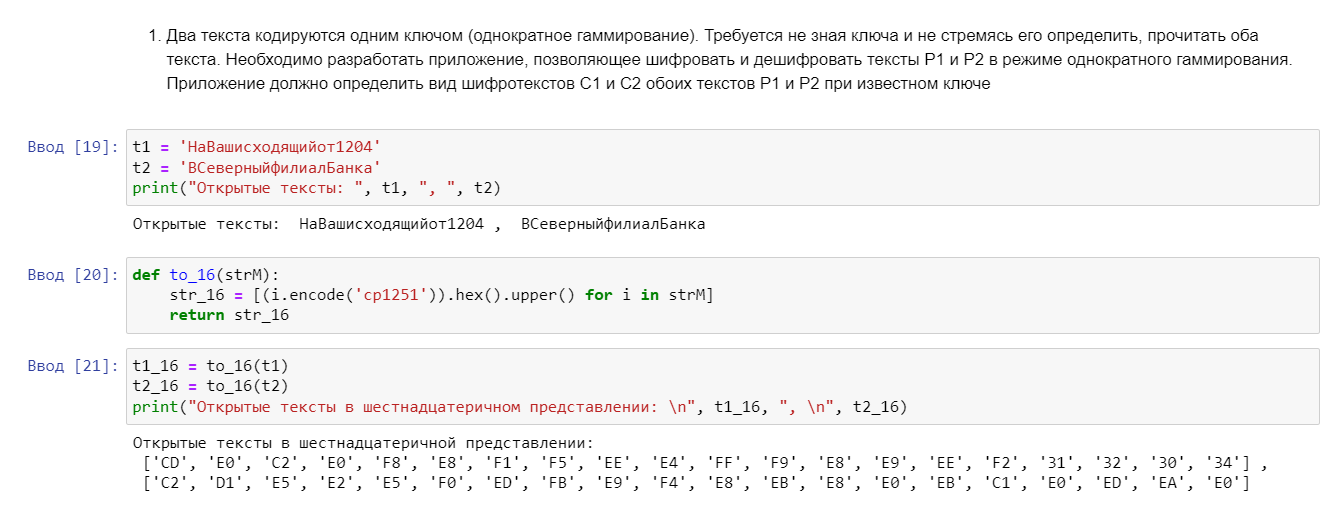


Figure 1: Перевод открытых текстов в шестнадцатеричное представление.

1. Создание ключа и шифрование текстов (шестнадцатеричное представление (fig. 2)

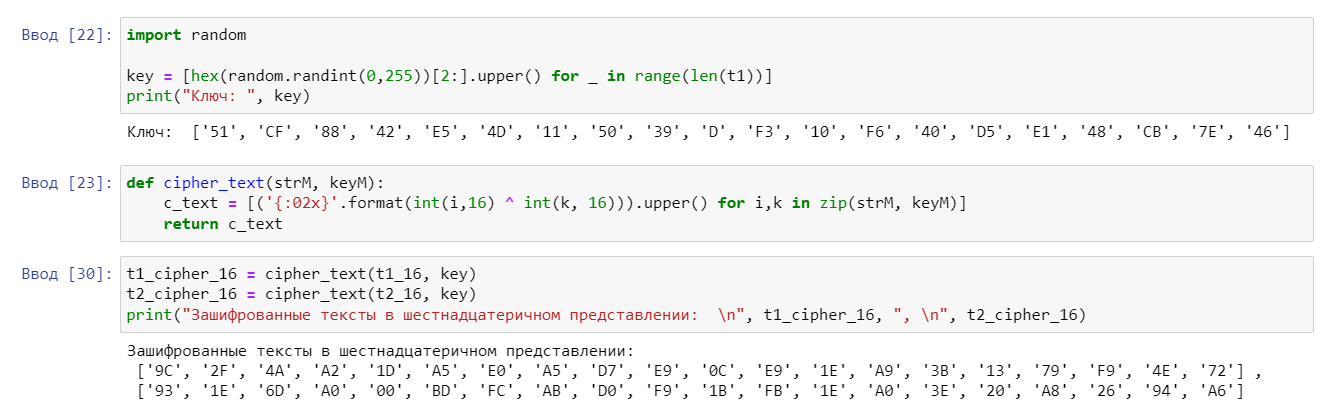


Figure 2: Создание ключа и шифрование текста

1. Зашиврованные тексты. (fig. 3)

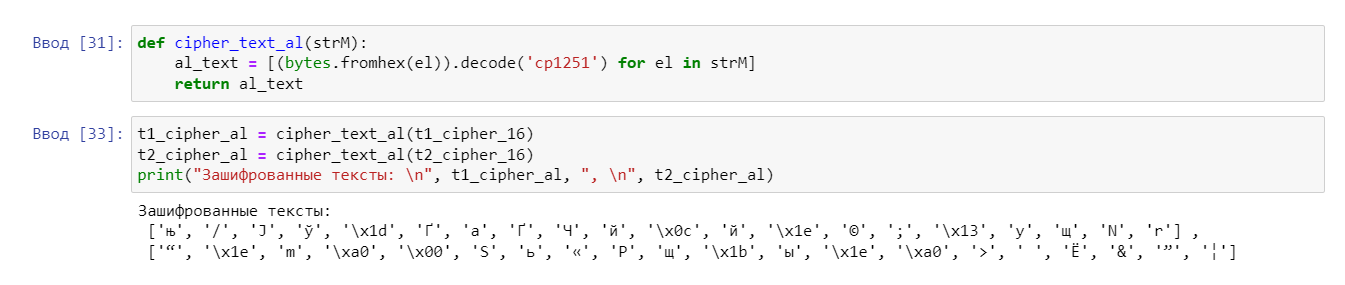


Figure 3: Зашиврованные тексты

1. Определение открытого текста по второму отрытому тексту и зашифрованным текстам (без использования ключа)(fig. **¿fig:004?**)

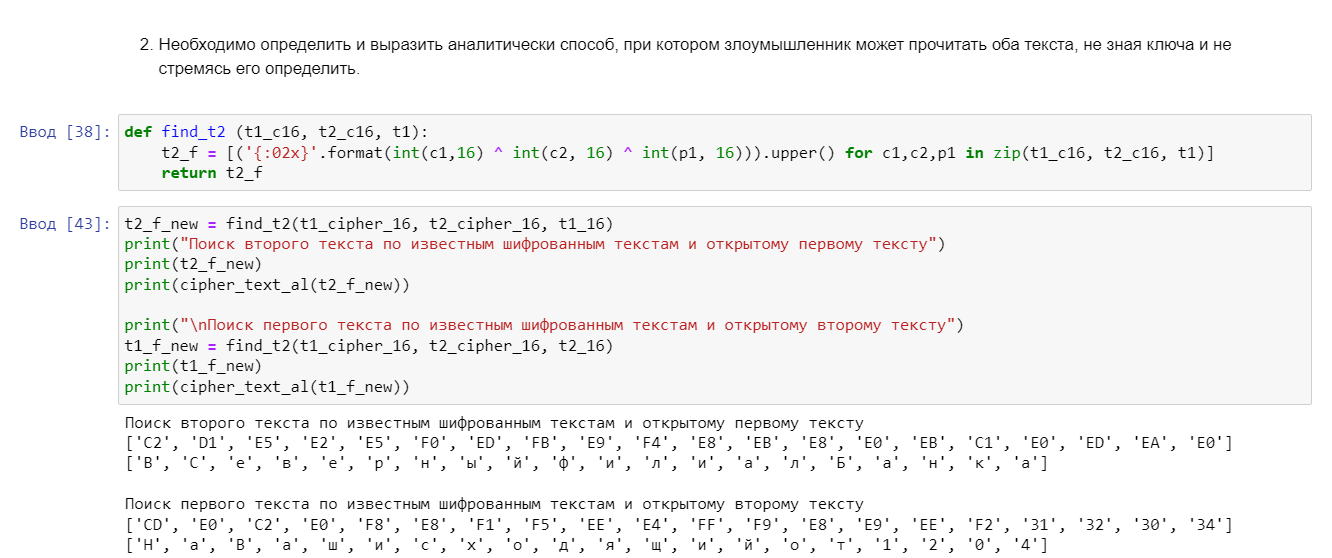


Figure 4: Определение открытого текста по второму отрытому тексту и зашифрованным текстам

# 3 Выводы

* Выполнила лабораторную работу №8.
* Освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

# 4 Список литературы

1. Методические материалы курса. “Информационная безопасность компьютерных сетей” Кулябов Д. С., Королькова А. В., Геворкян М. Н.