Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование

Лёшьен Стефани, НФИбд-02-19

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Задача

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: 1. Определить вид шифротекста при известном ключе и известном открытом тексте. 2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# 3 Последовательность выполнения работы

1. В новом блокноте в Google Colaboratory я импортировала нужные мне библиотеки.

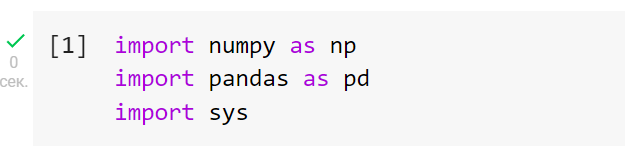


Figure 1: Импорт библиотек

1. Далее, я написала фунцию для определения вида шифротекста при известном ключе и известном открытом тексте. Сначала я перевела наш открытый текст в шестнадцатеричную систему и сгенерировала рандомный ключ. При помощи ключа я получаю зашифрованный текст в шестнадцатеричном формате и шифротекст.

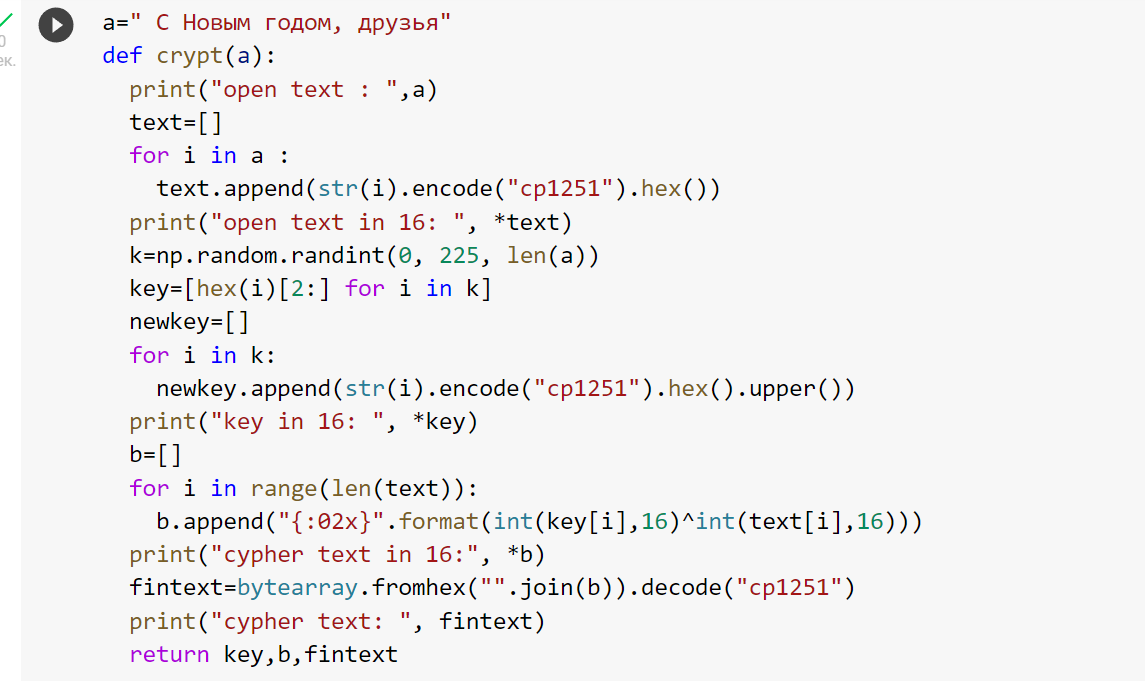


Figure 2: Функция определения шифротекста

1. В результате выполнения этой функции мы получаем на выход открытый текст, ключ в шестнадцатеричной системе счисления.

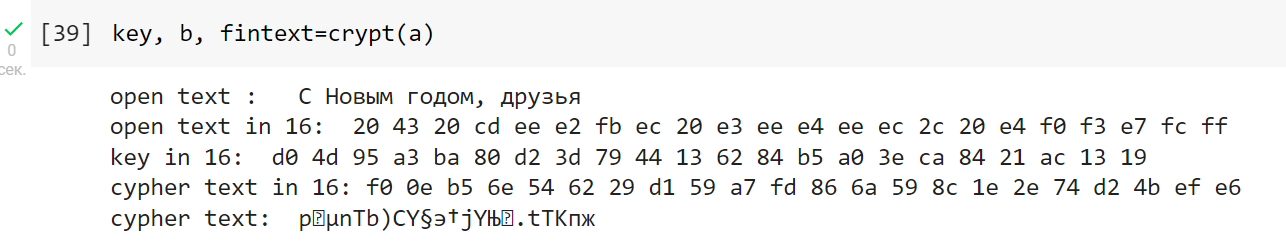


Figure 3: результат

1. вторая фунция

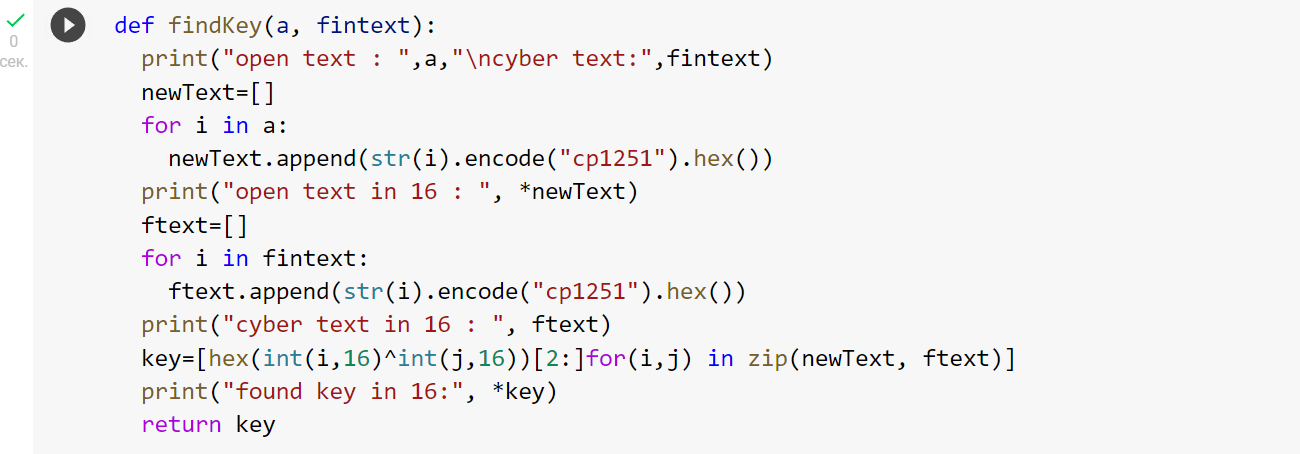


Figure 4: Вторая функция

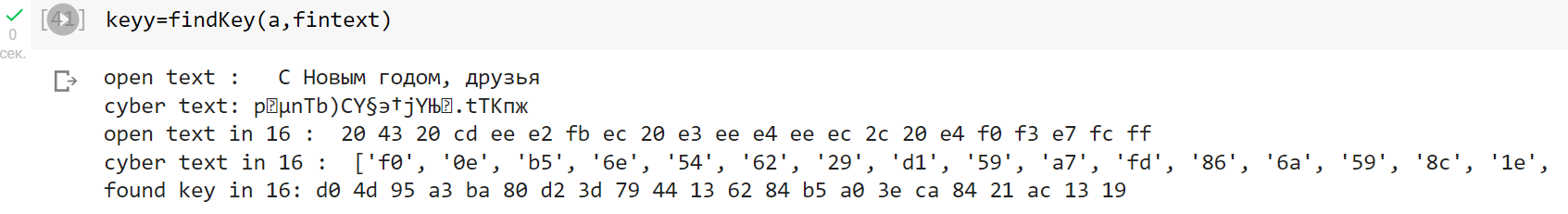
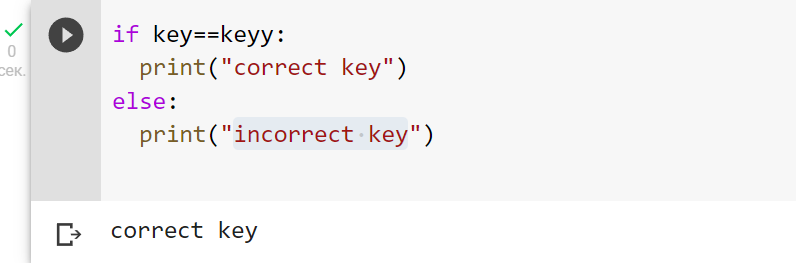


Figure 5: Результат

1. Проверяем если полученный ключ совпадает с тем, который мы получили на предыдущем шаге. 

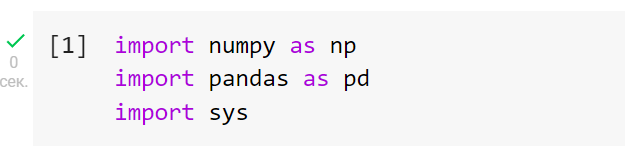


Figure 6: html-файл test.html

# 4 Выводы

Я освоила на практике применение режима однократного гаммирования.

# 5 Библиография

1. Методические материалы курса