Отчёт по лабораторной работе №7

*дисциплина: Информационная безопасность*

Морозова Ульяна

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования

# 2 Выполнение лабораторной работы

Для выполнения лабораторной работы я написала программу на языке программирования Python.

1. Для начала импортируем необходимые для работы библиотеки (рис. 1).

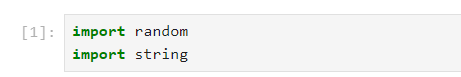


Рис. 1: Импорт

1. Создадим функцию для генерации ключа (рис. 2).

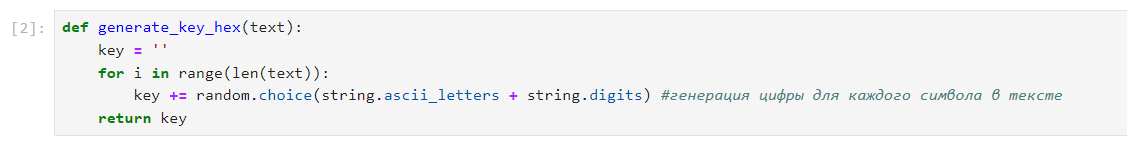


Рис. 2: Генерация ключа

1. Затем напишем функцию для (де)шифрования (рис. 3).



Рис. 3: (Де)шифрование

1. Нужно определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. Для этого создаю функцию для нахождения возможных ключей для фрагмента текста (рис. 4).

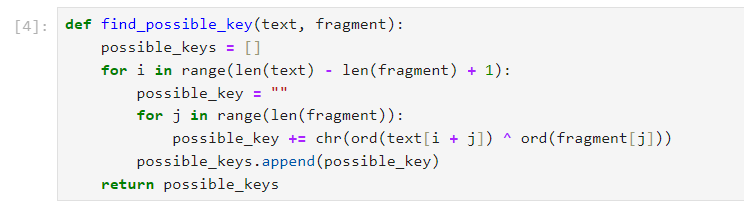


Рис. 4: Функция нахождения всех возможных ключей

1. Проверка работы всех функций. Шифрование и дешифрование происходит верно, как и нахождение ключей, с помощью которых можно расшифровать верно только кусок текста (рис. 5).



Рис. 5: Проверка работы программы

# 3 Выводы

Мы освоили на практике применение режима однократного гаммирования

# Список литературы