Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование

Радикорский Павел Михайлович

НФИбд-03-18

11.12.2021

Содержание

# Цели и задачи

**Цель:** Освоить на практике применение режима однократного гаммирования

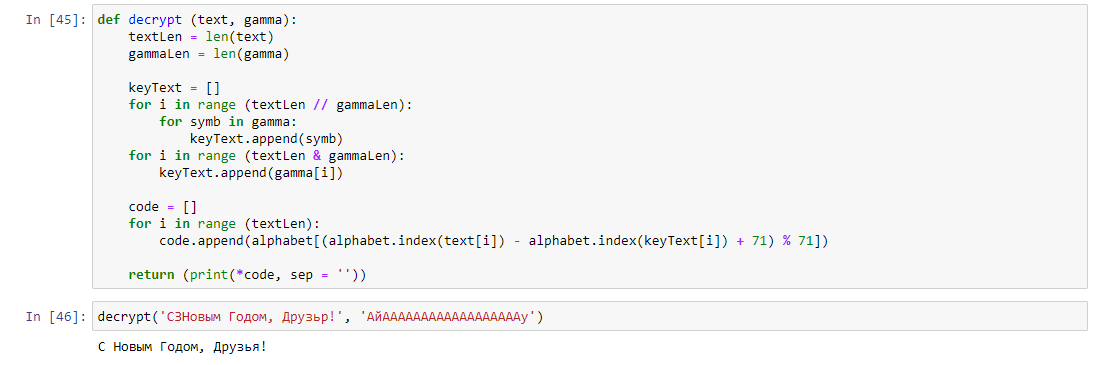
# Выполнение

Функция шифрования. Задаем алфавит из заглавных, строчных букв русского алфавита, !, ?, ., , и пробела. На вход поступает открытый текст, в виде массива символов, и ключ — гамму. Анализируем длину текста, «растягиваем» гамму до нужного размера и выполняем посимвольное сложение.



Функция шифрования

Функция расшифрования Работает аналогично. «Растягиваем» гамму и выполняем посимвольное вычитание ее из текста.



Функция расшифрования

Функция, которая определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. Работает аналогично функции расшифрования, но на вход поступает не зашифрованный текст и ключ, а зашифрованный и открытый текст



Функция получения ключа

# Выводы

В результате выполнения работы я освоил на практике применение режима однократного гаммирования.