Отчёт по лабораторной работе №8

Дисциплина: Основы информационной безопасности

Паращенко Антонина Дмитриевна

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

1. Функция для генерации ключа. (рис. 1)

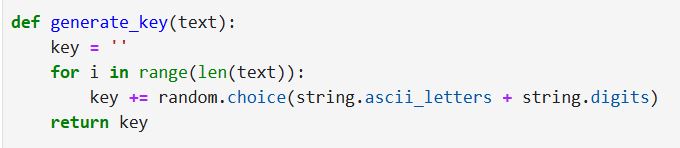


Рис. 1: Генерация ключа

1. Функция для (де)шифрования. (рис. 2)



Рис. 2: Шифрование

1. Код для вывода результатов и результаты. рис. 3) - (рис. 4)



Рис. 3: Подбор ключа

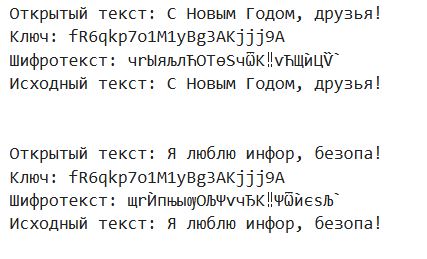


Рис. 4: Результаты

1. Код для расшифровки фразы с помощью второй фразы и результаты. (рис. 5) - (рис. 6)

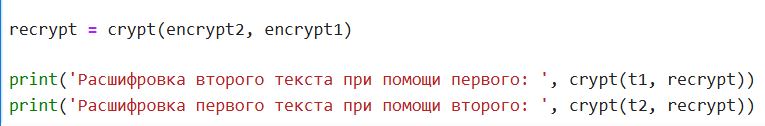


Рис. 5: Код расшифровки

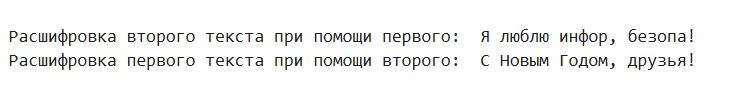


Рис. 6: Результаты расшифровки

1. Листинг программы. (рис. 7)



Рис. 7: Листинг программы

# 3 Вывод

В результате выполнения работы мы научились на практике применять режим однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Список литературы

1. https://esystem.rudn.ru/pluginfile.php/2357159/mod\_resource/content/2/008-lab\_crypto-key.pdf