Отчёт по лабораторной работе №7

Дисциплина: Основы информационной безопасности

Набережных Дарина Денисовна, НПМбд-01-19

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования

# 2 Теоретическое введение

Гаммирование - наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученных с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

# 3 Выполнение лабораторной работы

Необходимо подобрать ключ, чтобы получить сообщение “С Новым Годом, друзья!”. Сначала напишем функцию шифрования. Для этого зададим алфавит из заглавных, строчных букв русского алфавита и нескольких символов. (рис. 1).



Рис. 1: Создание функции шифрования

Создадим функцию расшифрования, которая работает аналогично. (рис. 2).



Рис. 2: Функция расшифрования

Теперь создадим фукнцию, определяющую ключ, с помощью которого шифротекст можно преобразовать в некоторый фрагмент текста, который представляет собой один из возможных вариантов прочтения открытого текста. (рис. 3).



Рис. 3: Определение ключа

# 4 Выводы

Я освоила на практике применение режима однократного гаммирования.

# Список литературы