Лабораторная работа № 8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Форис Анастасия Дмитриевна

25.10.2024

Российский университет дружбы народов, Москва, Россия

Цель лабораторной работы

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

Создание программы

Я начала с импорта необходимых библиотек. Затем я реализовала функцию для сложения по модулю два двух строк. Открытые или исходные тексты имели одинаковую длину. После этого я создала ключ такой же длины, что и открытые тексты. С использованием ранее созданной функции я получила шифротексты, предполагая знание как открытых текстов, так и ключа. Точно так же я извлекла открытые тексты с использованием ранее созданной функции, предполагая знание как шифротекстов, так и ключа.

Выполнение лабораторной работы 2

Кроме того, я выполнила сложение по модулю два двух шифротекстов с использованием ранее определенной функции. Кроме того, я получила открытые тексты при условии знания как обоих шифротекстов, так и одного из открытых текстов. Также я извлекла сегмент первого открытого текста с помощью среза. Наконец, я получила сегмент второго текста, расположенный на позициях символов сегмента первого открытого текста, с использованием ранее созданной функции, предполагая знание как обоих шифротекстов, так и части первого открытого текста.

Выполнение лабораторной работы 3

Рис. 1: Приложение, реализующее режим однократного гаммирования для двух текстов одним ключом, Часть 1

Рис. 2: Код

Выполнение лабораторной работы 4

Рис. 3: Приложение, реализующее режим однократного гаммирования для двух текстов одним ключом, Часть 2

Рис. 4: Код

Вывод

Вывод

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.