Отчет по лабораторной работе №8

Элементы криптографии. Шифрование различных исходных текстов одним ключом

Евсеева Дарья Олеговна

29 октября, 2022

Содержание

# Цель работы

Целью данной работы является освоение на практике применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Задание

Разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

Приложение должно:

1. Определить вид шифротекстов двух открытых текстов при известном ключе.
2. Не зная ключа и не стремясь его определить прочитать оба текста.

# Теоретическое введение

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

# Выполнение лабораторной работы

Выполнять работу будем в среде Jupyter Notebook на языке Python.

Для начала определим вспомогательные функции для дальнейшей работы.



Вспомогательные функции

Далее определим основные функции. Первая функция ciphers\_define будет использоваться для определения вида шифротекстов при известном ключе и двух открытых текстах. Сразу проверим результат работы функции на исходных данных.



Функция определения шифротекстов

Как мы видим, мы получили шифротексты для двух открытых текстов с помощью одного ключа.

Далее реализуем определение неизвестного открытого текста по двум шифротекстам и второму открытому тексту. Напишем вспомогательную функцию для осуществления умножения по модулю два между тремя значениями, а также основную функцию text\_define для определения неизвестного открытого текста. Проверим результат работы функции.



Функция определения открытого текста

Мы видим, что полученный открытый текст совпадает с исходными данными, а значит функцию успешно работает.

# Выводы

В результате проделанной работы мы освоили на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Список литературы

* Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” https://esystem.rudn.ru/