Отчет по лабораторной работе №7

-

Овениязов Артур

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: 1. Определить вид шифротекста при известном ключе и известном открытом тексте. 2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# 3 Теоретическое введение

Гамми́рование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. [1]

# 4 Выполнение лабораторной работы

Написал следующий код в файле kripto.py.

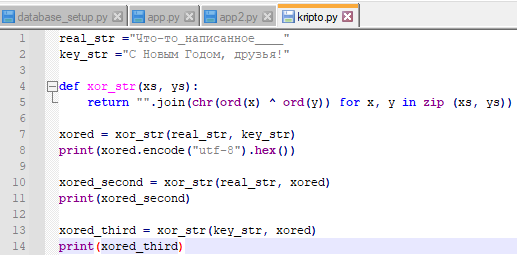


Figure 1: Код kripto.py

Полученный результат работы приложения: первая строка соответствует зашифрованной информации, вторая строка – расшифрованному тексту, а третья – ключу.

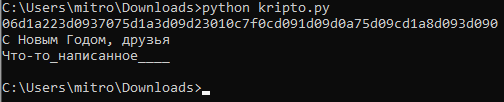


Figure 2: Результат выполнения kripto.py

## 4.1 Ответы на вопросы

1. Поясните смысл однократного гаммирования. Принцип гаммирования представляет собой процедуру наложения, при помощи некой функции G, на входную информационную последовательность гаммы шифра, т.е. псевдослучайной последовательности.
2. Перечислите недостатки однократного гаммирования. Недостатки однократного гаммирования заключается в необходимости иметь огромные объемы данных, которые можно было бы использовать в качестве гаммы.
3. Перечислите преимущества однократного гаммирования. Преимущества однократного гаммирования в том, что не может сказать о дешифровке, верна она или нет из-за равных априорных вероятностей криптоаналитик. Информация о вскрытом участке гаммы не дает информации об остальных ее частях.
4. Почему длина открытого текста должна совпадать с длиной ключа? Так должно быть, потому что мы используем поэлементное перемножение, чтобы размерность шифртекста была равна размерности открытого текста и ключа. Также это ее необходимость заключается в том, чтобы шифрование и расшифрование выполнялось одной и той же программой.
5. Какая операция используется в режиме однократного гаммирования, назовите её особенности? В режиме однократного гаммирования используется операция сложения по модулю 2 (XOR). Двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение.
6. Как по открытому тексту и ключу получить шифротекст? Задача нахождения шифротекста при известном ключе и открытом тексте состоит в применение следующего правила к каждому символу открытого текста: Ci = Pi (+) Ki.
7. Как по открытому тексту и шифротексту получить ключ? Обе части равенства сложим по модулю 2 с Pi. Ci (+) Pi = Pi (+) Ki (+) Pi = Ki, Ki = Ci (+) Pi.
8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра? Необходимые и достаточные условия абсолютной стойкости шифра включают в себя полную случайность ключа, равенство длин ключа и открытого текста, однократное использование ключа.

# 5 Выводы

В ходе данной лабораторной работы я освоил применение режима однократного гаммирования на практике, разработал приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

# Список литературы

1. Дискреционное разграничение доступа Linux [Электронный ресурс]. Сайт, 2021. URL: <http://debianinstall.ru/diskretsionnoe-razgranichenie-dostupa-linux/>.