Основы информационной безопасности

Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование

Нзита Диатезилуа Катенди

Содержание

# ПЦель работы

Освоить на практике применение режима однократного гаммирования.

# 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:

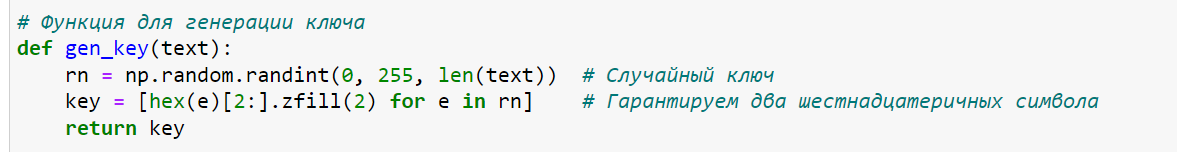
1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста

# Теоретические сведения

Гаммиирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст[@intro\_crypto\_2017]:. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных.

# Выполнение лабораторной работы

Генерация ключа (gen\_key): Функция создает случайный ключ для каждого символа текста. Каждый элемент ключа представлен в шестнадцатеричной системе. (рис. @fig:001)



Генерация ключа (gen\_key)

Шифрование текста (crypt\_message): Для каждого символа текста применяется кодировка в шестнадцатеричное значение, а затем используется операция XOR с ключом для получения зашифрованного текста.(рис. @fig:002)



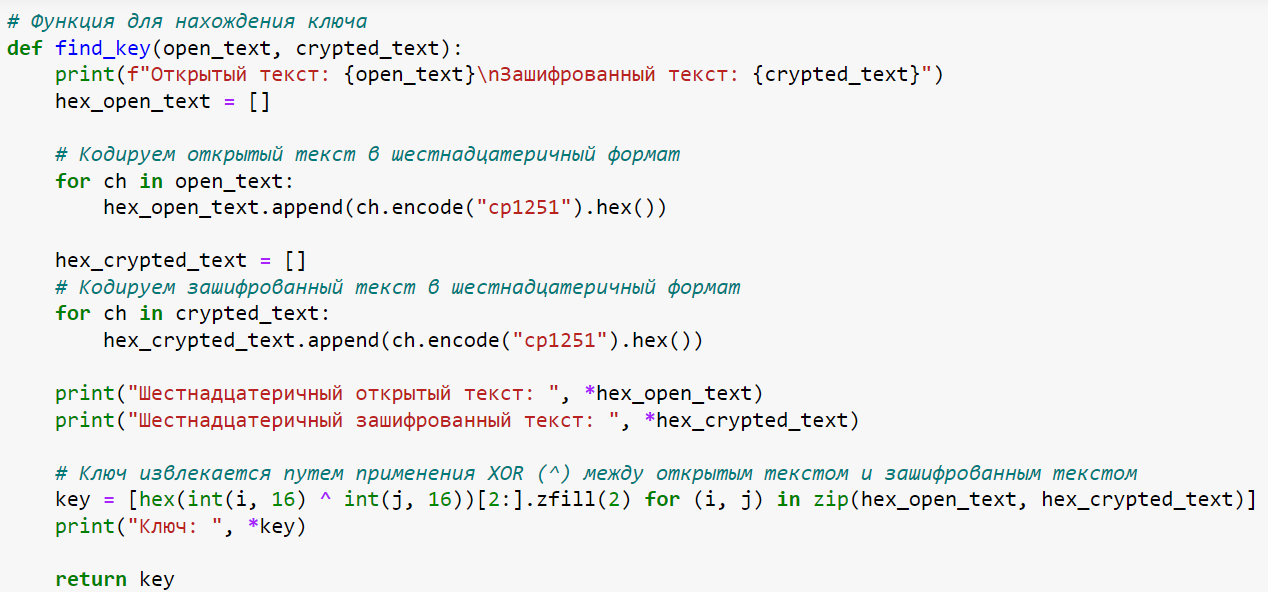
Шифрование текста (crypt\_message)

Расшифровка текста (decrypt\_message): Процесс аналогичен шифрованию, но операция XOR применяется к зашифрованному тексту с ключом для восстановления исходного текста. (рис. @fig:003)



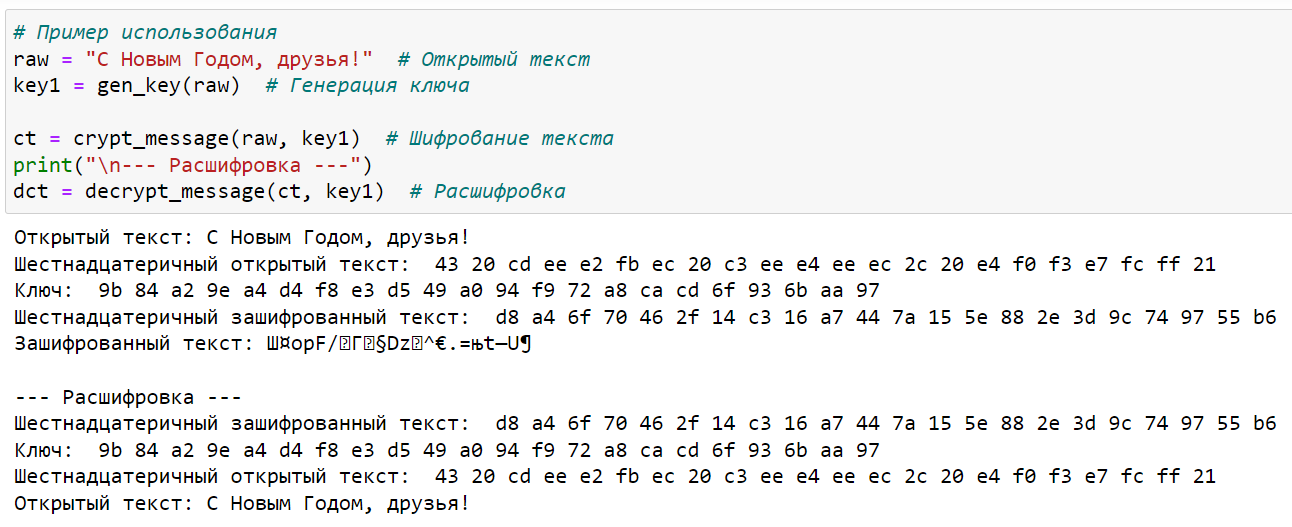
Расшифровка текста (decrypt\_message)

Нахождение ключа (find\_key): Операция XOR между шестнадцатеричными значениями открытого текста и зашифрованного текста позволяет найти ключ.(рис. @fig:004)



Нахождение ключа (find\_key)

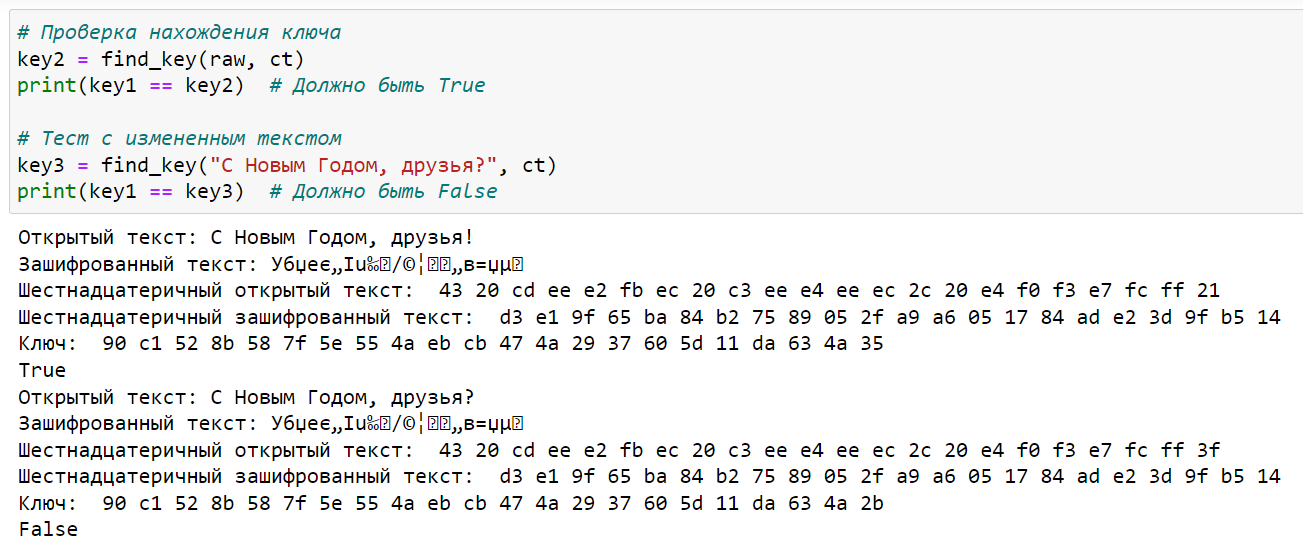
Проверка Шифрования(рис. @fig:005)



Проверка Шифрования

Если используется исходный открытый текст, то ключи key1 и key2 должны совпадать, и результат будет True.

Если изменен открытый текст (например, добавлен вопросительный знак), ключи key1 и key3 будут различаться, и результат будет False.(рис. @fig:006)



Ожидаемый результат

# Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Гаммиирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть.

1. Перечислите недостатки однократного гаммирования.

* Если один и тот же ключ используется для шифрования нескольких сообщений, это может привести к уязвимостям. Например, если злоумышленник узнает открытый текст и соответствующий шифротекст, он может использовать эту информацию для взлома ключа.
* Однократное гаммирование не обеспечивает аутентификацию или целостность данных. Это означает, что злоумышленник может изменить шифротекст без заметных изменений в открытом тексте.

1. Перечислите преимущества однократного гаммирования.

* Однократное гаммирование обеспечивает высокий уровень конфиденциальности, поскольку шифротекст не может быть легко взломан без знания ключа.
* Однократное гаммирование обеспечивает равномерное распределение вероятностей для каждого символа в шифротексте, что делает его статистически неразличимым от случайной последовательности.
* Однократное гаммирование является простым и быстрым методом шифрования.

1. Почему длина открытого текста должна совпадать с длиной ключа?

Если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть.

1. Какая операция используется в режиме однократного гаммирования, назовите её особенности?

В режиме однократного гаммирования используется операция XOR (исключающее ИЛИ). Операция XOR комбинирует биты открытого текста и ключа, чтобы получить шифротекст. Особенностью операции XOR является то, что она возвращает 1 только в том случае, если один из входных битов равен 1, но не оба.

1. Как по открытому тексту и ключу получить шифротекст?

Нужно побитово сложить по модулю численное представление символов в ключе и в открытом тексте.

1. Как по открытому тексту и шифротексту получить ключ?

Нужно побитово сложить по модулю численное представление символов в шифротексте и в открытом тексте.

1. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра?

Необходимые и достаточные условия абсолютной стойкости шифра:

* полная случайность ключа;
* равенство длин ключа и открытого текста;
* однократное использование ключа.

# Выводы

В результаты выполнения работы были освоены практические навыки применения режима однократного гаммирования.

# Список литературы