Отчет по лабораторной работе №7

Информационная безопасноть

Астафьева Анна Андреевна НПИбд-01-18

Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Теоретическое описание

Предложенная Г. С. Вернамом так называемая «схема однократного использования (гаммирования)» является простой, но надёжной схемой шифрования данных. *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. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ) между элементами гаммы и элементами подлежащего сокрытию текста. Напомним, как работает операция XOR над битами: . Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходноезначение, а шифрование и расшифрование выполняется одной и той же программой. Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении к каждому символу открытого текста следующего правила:

где — i-й символ получившегося зашифрованного послания, — i-й символ открытого текста, — i-й символ ключа, i = 1, m. Размерности открытого текста и ключа должны совпадать, и полученный шифротекст будет такой же длины. Если известны шифротекст и открытый текст, то задача нахождения ключа решается также, а именно, обе части равенства необходимо сложить по модулю 2 с :

Открытый текст имеет символьный вид, а ключ — шестнадцатеричное представление. Ключ также можно представить в символьном виде, воспользовавшись таблицей ASCII-кодов. К. Шеннон доказал абсолютную стойкость шифра в случае, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения. Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении C все различные ключевые последовательности K возможны и равновероятны, а значит, возможны и любые сообщения P. Необходимые и достаточные условия абсолютной стойкости шифра: – полная случайность ключа; – равенство длин ключа и открытого текста; – однократное использование ключа.

# Выполнение лабораторной работы

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

1. Написана функция *encryption*, которая с помощью однократного гаммирования из сообщения и ключа получает шифротекст (рис. 1).

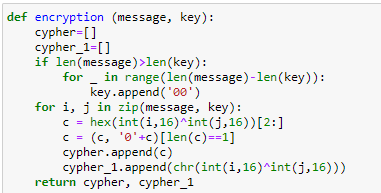


Figure 1: Код функции *encryption*

1. Написана функция *gen\_key*, генерирующая случайный ключ (рис. 2).

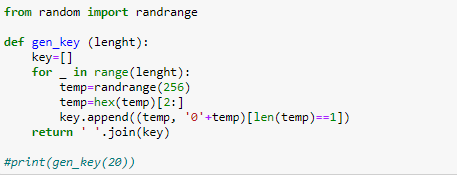


Figure 2: Код функции *gen\_key*

1. Написана функция *to\_hex*, трансформирующая текст в шестнадцатиричное представление (рис. 3).

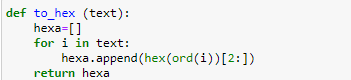


Figure 3: Код функции *to\_hex*

1. Определяю вид шифротекста при известном ключе и известном открытом тексте. Применяю к шифротексту ключ снова, чтобы получить исходное сообщение (рис. 4).

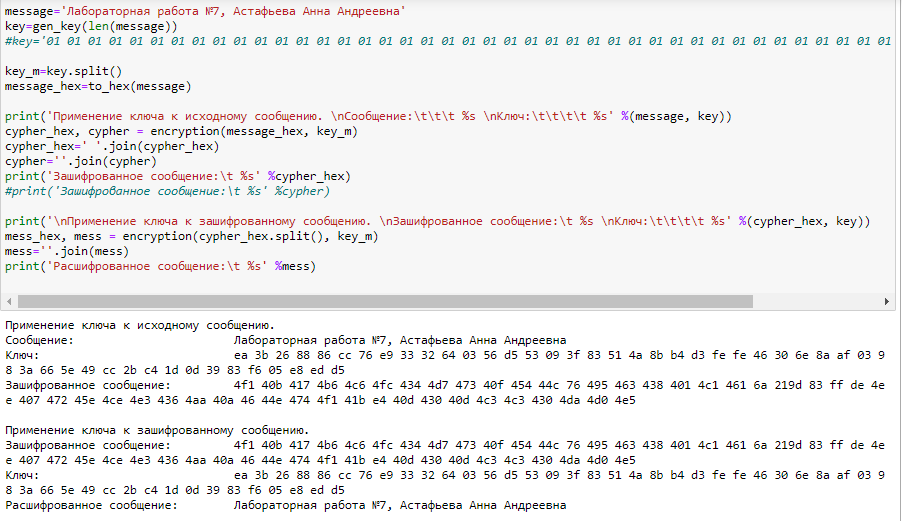


Figure 4: Получение шифротекста

1. Пробую расшифровать шифротекст с помощью неправильного ключа(рис. 5).

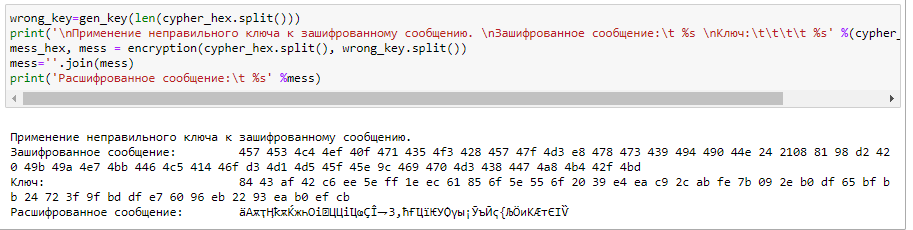


Figure 5: Применение неправильного ключа

1. Определяю ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста (Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!»)(рис. 6).

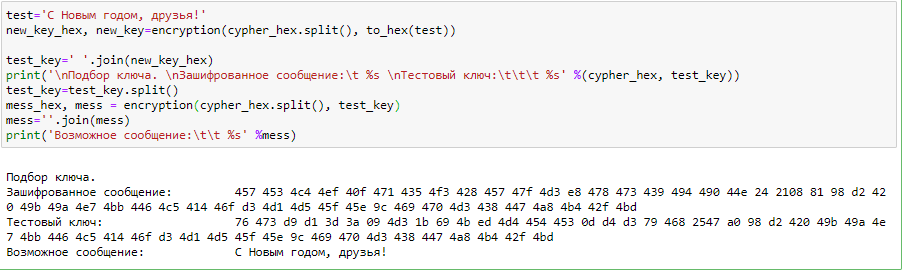


Figure 6: Один из вариантов прочтения шифротекста

# Контрольные вопросы

1. Поясните смысл однократного гаммирования. Смысл однократного гаммирования состоит в том, что каждый символ попарно с символом ключа складываются по модулю.
2. Перечислите недостатки однократного гаммирования. Недостатками является то, что ключ нельзя переиспользовать, а также размер ключа должен быть равен размеру текста.
3. Перечислите преимущества однократного гаммирования. Основными преимуществами являются симметричность и криптостойкость.
4. Почему длина открытого текста должна совпадать с длиной ключа? Каждый символ открытого текста должен попарно складываться с символом ключа.
5. Какая операция используется в режиме однократного гаммирования, назовите её особенности? В режиме однократного гаммирования используется сложение по модулю 2: при сложении чисел с другим получается исходное. Например, 0+0 = 0, 0+1=1, 1+0=1, 1+1=0. Если в методе шифрования используется однократная вероятностная гамма той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть.
6. Как по открытому тексту и ключу получить шифротекст? Для этого необходимо сложить попарно символы текста с ключом по модулю 2.
7. Как по открытому тексту и шифротексту получить ключ? Для этого необходимо сложить попарно по модулю 2 символы открытого текста с символами шифротекста.
8. В чём заключаются необходимые и достаточные условия абсолютной стойкости шифра? Необходимые и достаточные условия абсолютной стойкости шифра заключаются в полной случайности ключа; равенстве длин ключа и открытого текста; использовании ключа однократно.

# Выводы

На основе проделанной работы освоила на практике применение режима однократного гаммирования.