Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Асеинова Елизавета

2022 Oct 5th

Содержание

[1 Цель работы 1](#_Toc115901455)

[2 Выполнение лабораторной работы 1](#_Toc115901456)

[3 Контрольные вопросы 2](#_Toc115901457)

[4 Выводы 3](#_Toc115901458)

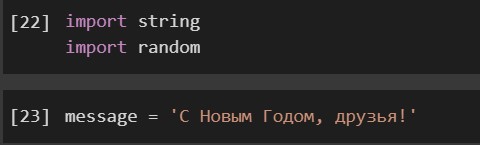
[5 Список литературы 3](#_Toc115901459)

# 1 Цель работы

Целью данной работы является освоение на практике применение режима однократного гаммирования. [1]

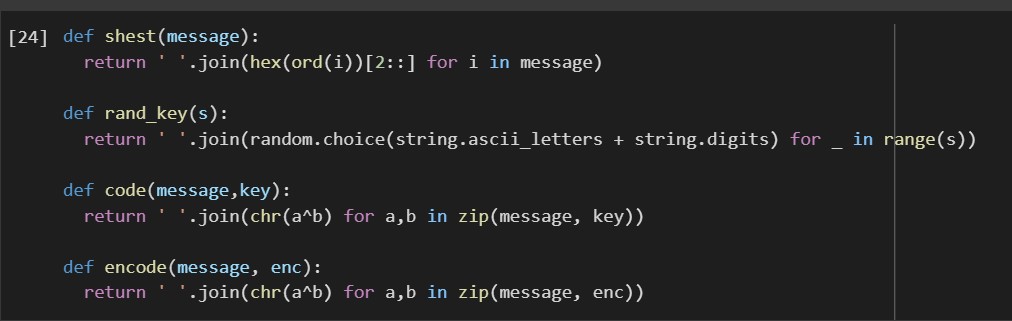
# 2 Выполнение лабораторной работы

1. Импортировала библиотеки, необходимые для работы со строками и рандомными значениями и задала сообщение.



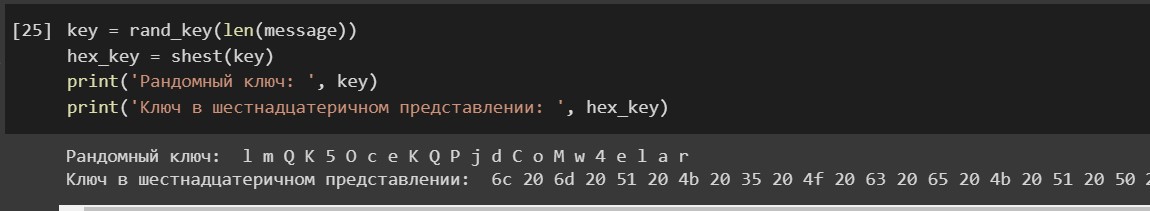
Библиотеки

1. Написала функцию шифрования, которая определяет вид шифротекста при известном ключе и известном открытом тексте. Написала функцию дешифровки, которая определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.



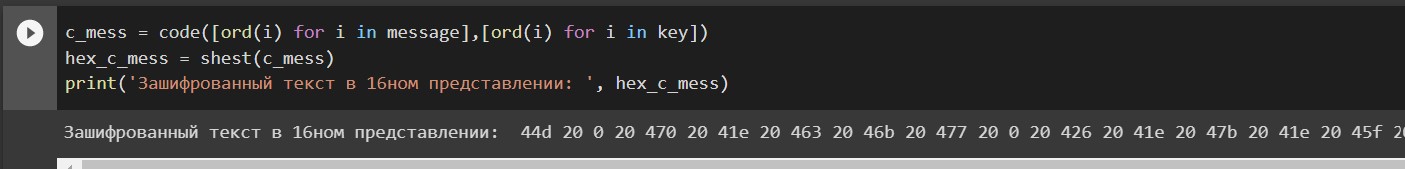
Функции

1. Создала ключ и его шестнадцатеричное представление.



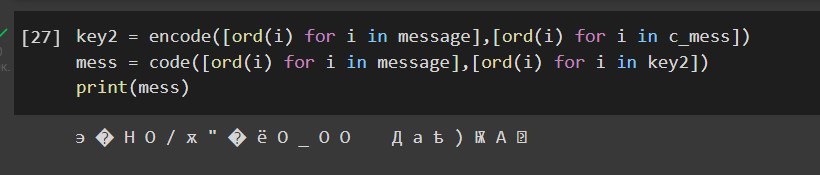
Задание ключа

1. Зашифровала текст в шестнадцатеричном представлении.



Зашифрованный текст

1. Расшифровала сообщение при помощи ключа. Получили один из видов прочтения сообщения. Вывод выглядит таким образом из-за проблем в кодировании у Python.



Расшифрованный текст

# 3 Контрольные вопросы

1. Одократное гаммирование - выполнение операции XOR между элементами гаммы и элементами подлежащего сокрытию текста. 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.
2. Недостатки однократного гаммирования: Абсолютная стойкость шифра доказана только для случая, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения.
3. Преимущества однократного гаммирования: во-первых, такой способ симметричен, т.е. двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение; во-вторых, шифрование и расшифрование может быть выполнено одной и той же программой. Наконец, 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.
4. Длина открытого текста должна совпадать с длиной ключа, т.к. если ключ короче текста, то операция XOR будет применена не ко всем элементам и конец сообщения будет не закодирован, а если ключ будет длиннее, то появится неоднозначность декодирования.
5. Операция XOR используется в режиме однократного гаммирования. Наложение гаммы по сути представляет собой выполнение побитовой операции сложения по модулю 2, т.е. мы должны сложить каждый элемент гаммы с соответствующим элементом ключа. Данная операция является симметричной, так как прибавление одной и той же величины по модулю 2 восстанавливает исходное значение.
6. Получение шифротекста по открытому тексту и ключу:
7. Получение ключа по окрытому тексту и шифротексту:
8. Необходимы и достаточные условия абсолютной стойкости шифра: полная случайность ключа; равенство длин ключа и открытого текста; однократное использование ключа.

# 4 Выводы

В ходе работы мы освоили на практике применение режима однократного гаммирования.

# 5 Список литературы

1. Методические материалы курса