Отчет по лабораторной работе №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Бурдина Ксения Павловна

2022 Oct 19th

Содержание

# 1 Цель работы

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

# 2 Теоретическое введение

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой:

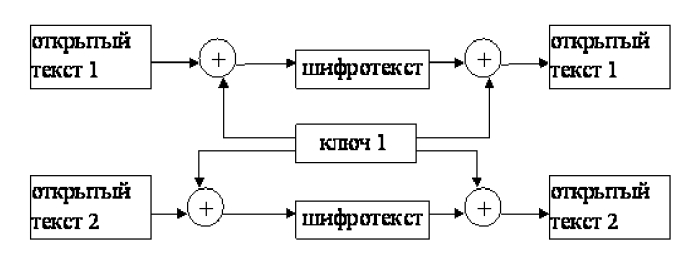


Схема шифрования одним ключом

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для этого оба равенства складываются по модулю 2. Тогда с учетом операции XOR получаем:

Предположим, что одна из телеграмм является шаблоном, т.е. имеет текст фиксированный формат, в который вписываются значения полей [[1]](https://esystem.rudn.ru/pluginfile.php/1651895/mod_resource/content/2/008-lab_crypto-key.pdf). Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар (известен вид обеих шифровок). Тогда зная и учитывая свойства операции XOR, имеем:

Таким образом, злоумышленник получает возможность определить те символы сообщения , которые находятся на позициях известного шаблона сообщения . В соответствии с логикой сообщения , злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения . Затем вновь используется формула с подстановкой вместо полученных на предыдущем шаге новых символов сообщения . И так далее. Действуя подобным образом, злоумышленник даже если не прочитает оба сообщения, то значительно уменьшит пространство их поиска.

# 3 Ход выполнения лабораторной работы

Задача ставится следующая: Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты и в режиме однократного гаммирования. Приложение должно определить вид шифротекстов и обоих текстов и при известном ключе. Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

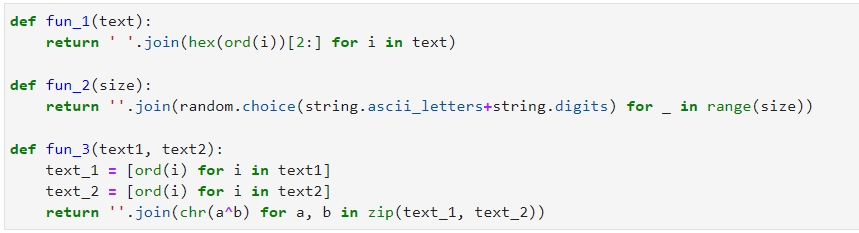
Для написания приложения будем использовать среду Jupyter. Выполним необходимую задачу.

1. Начнем с того, что введем необходимые нам для работы импорты:

Ввод необходимых импортов

Ввод необходимых импортов

1. Далее определим функции, которые мы будем использовать:



Функции для работы

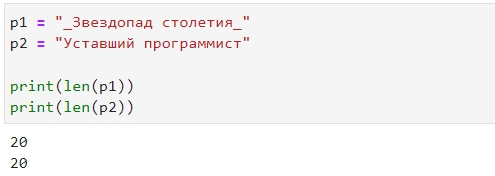
Первая функция у нас преобразует символьное представление текста в шестнадцатиричный вид.

Вторая отвечает за назначение каждому символу введенного текста определенного значения из символов Unicode.

А в третьей функции мы прописываем нахождение шифров обоих текстов по одному ключу и далее их расшифровка.

1. Теперь пропишем листинг нашей программы.

Вводим два текста и выводим для проверки их длину (потому что нам требуются тексты с одинаковой длиной для подбора шаблонного ключа):



Ввод текстов и вывод их длины

1. Пропишем нахождение ключа для одного из текстов, чтобы потом использовать его в качестве шаблона:



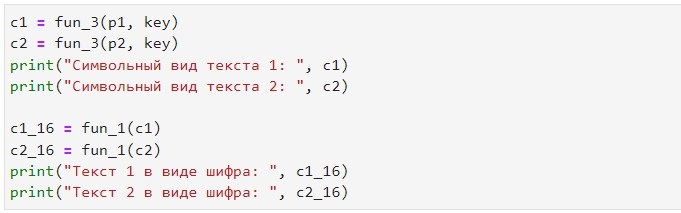
Нахождение ключа для текста 1

При нахождении ключа используем функцию 2 для составления символьного шифра, после чего преобразуем каждый выявленный символ в шестнадцатиричный вид с помощью функции 1 и выводим рещультат на экран:

Результат нахождения ключа

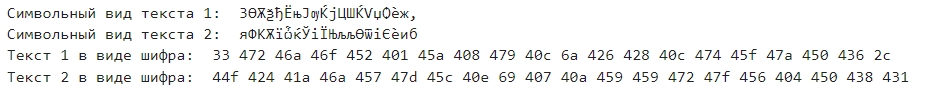
Результат нахождения ключа

1. Далее найдем шифр для каждого из текстов:



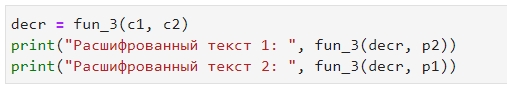
Определение видов шифровок для тектов

Используем функцию 3, которая помогает сделать шифровку для наших текстов. Сначала выводим тексты в символьном виде, после чего преобразуем их в шифр шестнадцатиричного вида и выводим на экран результат:



Результат шифрования текстов

1. Теперь, используя опять же функцию 3, сделаем преобразование шифра в символы необходимого алфавита. При этом заменяем текст сообщения 1 на текст сообщения 2, так как при подстановке шаблона ключа у нас изменился порядок текстов:



Расшифровка текстов

И в итоге получим наши изначальные тексты:

Результат расшифровки текстов

Результат расшифровки текстов

# 4 Листинг программы

import string  
import random  
  
def fun\_1(text):  
 return ' '.join(hex(ord(i))[2:] for i in text)  
def fun\_2(size):  
 return ''.join(random.choice(string.ascii\_letters+string.digits) for \_ in range(size))  
def fun\_3(text1, text2):  
 text\_1 = [ord(i) for i in text1]  
 text\_2 = [ord(i) for i in text2]  
 return ''.join(chr(a^b) for a, b in zip(text\_1, text\_2))  
  
p1 = "\_Звездопад столетия\_"  
p2 = "Уставший программист"  
print(len(p1))  
print(len(p2))  
  
key = fun\_2(len(p1))  
print("Ключ в символьном виде: ", key)  
key\_16 = fun\_1(key)  
print("Ключ в шестнадцатиричном виде: ", key\_16)  
  
c1 = fun\_3(p1, key)  
c2 = fun\_3(p2, key)  
print("Символьный вид текста 1: ", c1)  
print("Символьный вид текста 2: ", c2)  
  
c1\_16 = fun\_1(c1)  
c2\_16 = fun\_1(c2)  
print("Текст 1 в виде шифра: ", c1\_16)  
print("Текст 2 в виде шифра: ", c2\_16)  
  
decr = fun\_3(c1, c2)  
print("Расшифрованный текст 1: ", fun\_3(decr, p2))  
print("Расшифрованный текст 2: ", fun\_3(decr, p1))

# 5 Выводы

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

# 6 Контрольные вопросы

1. Как, зная один из текстов ( или ), определить другой, не зная при этом ключа?

Необходимо попытаться определить длину ключа, а затем разделить сообщение на несколько частей. Если правильно определить ключ, то перед пользователем будет вариант из определенного количества простых криптограмм с заменой Цезаря, которые нужно будет разгадать.

1. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой:

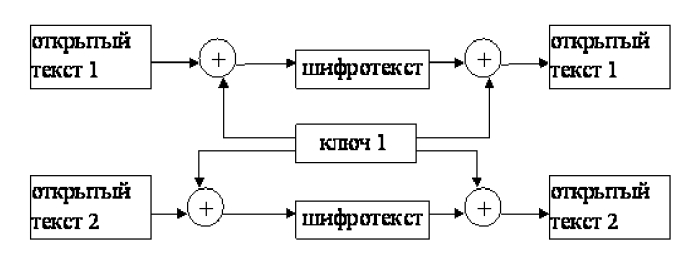


Схема шифрования одним ключом

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для этого оба равенства складываются по модулю 2. Тогда с учетом операции XOR получаем:

1. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Преимущества открытых тектов:

* Не нужно предварительно передавать секретный ключ по надёжному каналу;
* Только одной стороне известен ключ дешифрования, который нужно держать в секрете;
* В больших сетях число ключей в открытой криптосистеме значительно меньше, чем в симметричной.

1. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Недостатки алгоритма открытого шифрования:

* В алгоритм сложнно внести изменения;
* При открытом алгоритме используются порой слишком длинные ключи, которые тяжело подобрать;
* Шифрование-расшифровывание с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом;
* Требуются существенно большие вычислительные ресурсы, поэтому на практике открытые криптосистемы нужно использовать в сочетании с другими алгоритмами.