Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Румянцева Александра Сергеевна

11 декабря, 2021

Цели и задание на лабораторную работу

Цель: Освоить на практике применение режима однократного гаммирования.

Задание: Лабораторная работа подразумевает освоение граммирования опытным путем.

Выполнение лабораторной работы

1. Изучила теорию и указание к лабораторной работе.
2. Написала программу, которая подобирает ключ, чтобы получить сообщение «С Новым Годом, друзья!»

Целью написанной программы является разработка приложения, позволяющего 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.

Я написала программу, состоящую из 2ух функций: функция генерации ключа шифрования, и функция граммирования. Затем я проверила корректность выполняемых действий программой (рис. 1).

```
In [1]:
1 import random
2 import string

In [3]:
1 def key_generate(length, simbols = string.ascii_letters + string.digits):
2     return ''.join(random.choice(simbols) for i in range (length))
3
4 def gramming(text, key):
5     new_text = [ord(i) for i in text]
6     new_key = [ord(i) for i in key]
7     return ''.join(chr(t^k) for t,k in zip(new_text, new_key))

In [4]:
1 text ='test'
2 key = key_generate(4)
3 key

Out[4]: 'UeEL'

In [5]:
1 gramming(text, key)

Out[5]: '!\x0068'

In [6]:
1 gramming(gramming(text, key), key)

Out[6]: 'test'
```

Figure 1: рис.1. Программа для шифрования и дешифрования. Проверка её работы.

1) Определила вид шифротекста при известном ключе и открытом тексте. Текст использовала из задания «С Новым Годом, друзья!» (рис. 2).

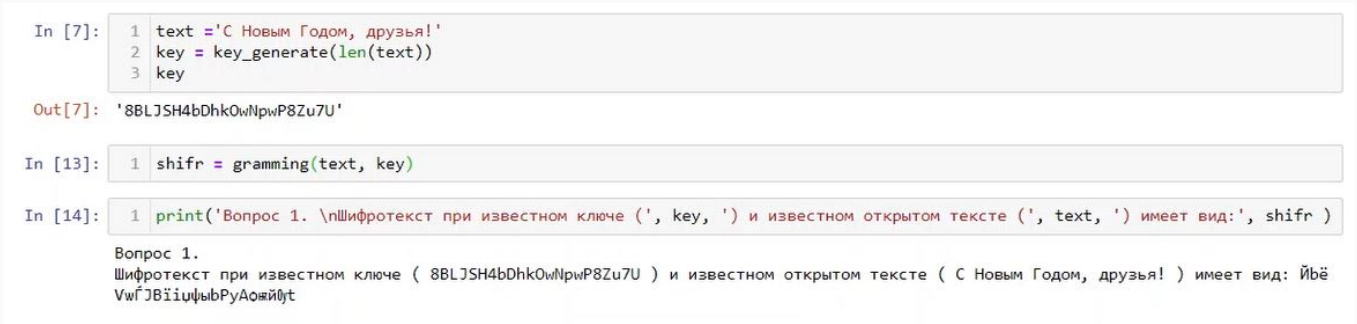

Figure 2: рис.2. Определение шифротекста для «С Новым Годом, друзья!».

2) Определила ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста (рис. 3).

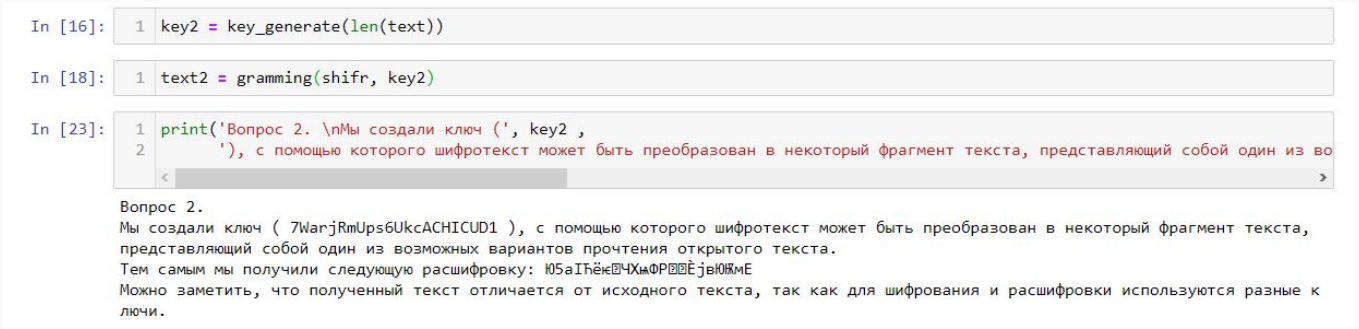

Figure 3: рис.3. Расшифровка текста с помощью иного ключа.

Как видно на рисунке 3, мы создали ключ key2, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.Тем самым мы получили расшифровку, которая отличается от исходного текста, так как для шифрования и расшифровки используются разные ключи.

Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Гаммирование – это наложение/снятие на открытые/зашифрованные данные криптографической гаммы, то есть последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных/открытых данных. Однократное гаммирование – это когда каждый символ попарно с символом ключа складываются по модулю 2 (XOR).

2. Перечислите недостатки однократного гаммирования.

Размер ключевого материала должен совпадать с размером передаваемых сообщений.

```
In [24]:  1 text ='С Новым Годом, друзья!'
          2 key = key_generate(len(text)-1)
          3 key
Out[24]: 'mZUYVeGFyDDP27CvkVYxx'

In [25]:  1 shifr = gramming(text, key)

In [27]:  1 gramming(shifr, key)
Out[27]: 'С Новым Годом, друзья'
```

Figure 4: рис.4. Пример шифрования и расшифровки, если длина ключа меньше длины текста.

Контрольные вопросы

Необходимо иметь эффективные процедуры для выработки случайных равновероятных двоичных последовательностей и специальную службу для развоза огромного количества ключей. Если одну и ту же гамму использовать дважды для разных сообщений, то шифр из совершенно стойкого превращается в «совершенно нестойкий» и допускает дешифрование практически вручную.

3. Перечислите преимущества однократного гаммирования.

С точки зрения теории криптоанализа метод шифрования случайной однократной равновероятной гаммой той же длины, что и открытый текст, является невскрываемым. Кроме того, даже раскрыв часть сообщения, информация о вскрытом участке гаммы не дает информации об остальных ее частях. К достоинствам также можно отнести простоту реализации и удобство применения.

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

Потому что каждый символ открытого текста складывается с символом ключа попарно. Иначе можно получить неполный текст, как рассматривали пример на рисунке 4.

Контрольные вопросы

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

В режиме однократного гаммирования используется сложение по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. Особенность заключается в том, что этот алгоритм шифрования является симметричным. Поскольку двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, шифрование и расшифрование выполняется одной и той же программой.

6. Как по открытому тексту и ключу получить шифротекст?

Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении сложения по модулю 2 между каждым символом открытого текста и ключа. То есть выполняем однократное граммирование.

7. Как по открытому тексту и шифротексту получить ключ?

Если известны открытый текст и шифротекст, то задача нахождения ключа заключается в применении сложения по модулю 2 между каждым символом открытого текста и шифра. Пример рассмотрен на рисунке 5:

```
In [33]:  1 text ='С Новым Годом, друзья!'
          2 key = key_generate(len(text))
          3 key
Out[33]: 'skHSVOdZ9STWIRn49WC92S'

In [34]:  1 shifr = gramming(text, key)

In [36]:  1 gramming(shifr, text)
Out[36]: 'skHSVOdZ9STWIRn49WC92S'
```

Figure 5: рис.5. Нахождение ключа, если известны открытый текст и шифротекст.

8. 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

Я освоила на практике применение режима однократного гаммирования.