Лабораторная работа №8

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

Румянцева Александра Сергеевна

18 декабря, 2021

Цели и задание на лабораторную работу

Цель: Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Задание: Лабораторная работа подразумевает освоение граммирования опытным путем на примере кодирования различных исходных текстов одним ключом.

Выполнение лабораторной работы

1. Изучила теорию и указание к лабораторной работе.
2. Разработала приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования.

С помощью приложения нужно:

1) Определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе;
2) Определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Я написала программу, состоящую из 2ух функций (рис. 1): функция генерации ключа шифрования, и функция граммирования (выполнено в лабораторной 7).

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

In [3]:
def key_generate(length, simbols = string.ascii_letters + string.digits):
    return ''.join(random.choice(simbols) for i in range (length))

def gramming(text, key):
    new_text = [ord(i) for i in text]
    new_key = [ord(i) for i in key]
    return ''.join(chr(t^k) for t,k in zip(new_text, new_key))

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

Out[4]: 'UeEL'

In [5]:
gramming(text, key)

Out[5]: '!\x0068'

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

Out[6]: 'test'
```

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

Выполним пункты задания:

1) Определила вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе. Текста P1 и P2 использовала из задания (рис. 2). При этом обратила внимание на длину текстов, так как важно, чтобы длина ключа совпадала с длиной текстов.

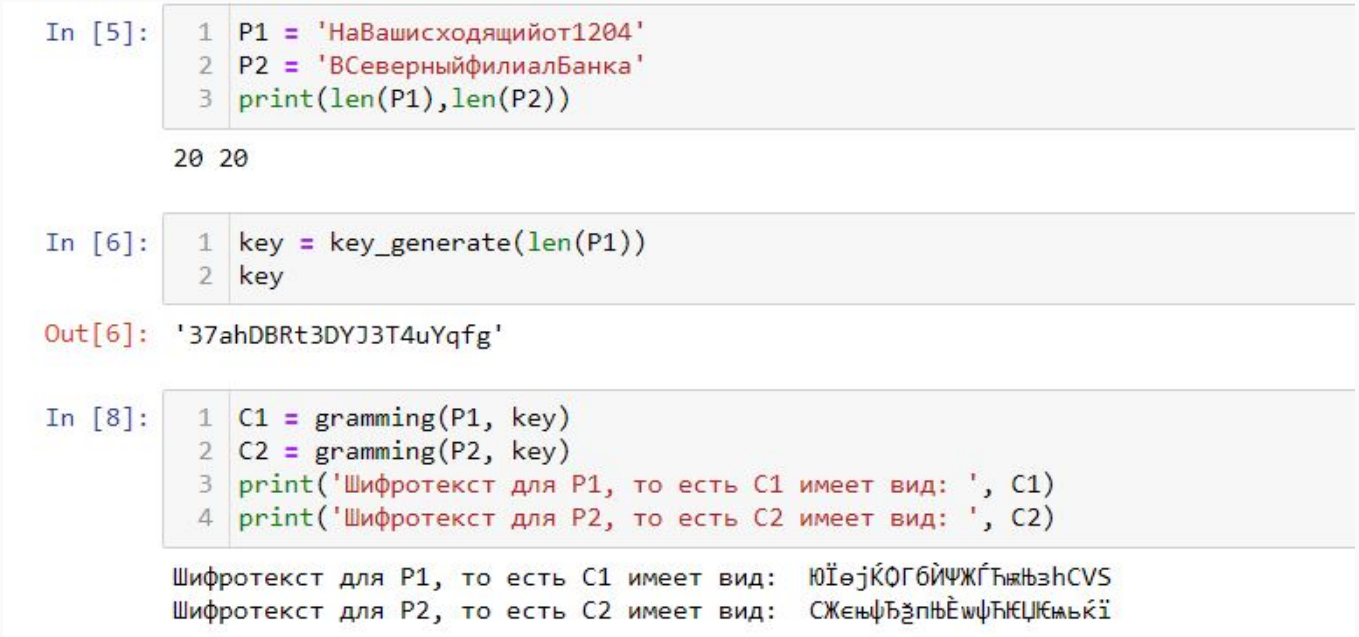

Figure 2: рис.2. Определение шифротекстов для P1 и P2.

2) Определила и выразила аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Для этого необходимо было произвести граммирование суммы по модулю 2 от шифротекстов и одного из исходных текстов, таким образом получаем расшифрованный второй текст (рис. 3).

```
In [9]:
1 C1_sum_C2 = gramming(C1, C2) #соответствует сумме по модулю 2 от P1 и P2
2 C1_sum_C2

Out[9]: "\x0f\x11'\x02}x|\x0e\x07pwr\x00\t\x05SËЏЊЄ"

In [10]:
1 P1_find = gramming(C1_sum_C2, P2)
2 print('Зная шифротексты C1 и C2, а так же текст P2 можно найти P1:', P1_find)

Зная шифротексты C1 и C2, а так же текст P2 можно найти P1: НаВашисходящийот1204

In [11]:
1 P2_find = gramming(C1_sum_C2, P1)
2 print('Зная шифротексты C1 и C2, а так же текст P1 можно найти P2:', P2_find)

Зная шифротексты C1 и C2, а так же текст P1 можно найти P2: ВСеверныйфилиалБанка
```

Figure 3: рис.3. Расшифровка текстов без использования ключа.

Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

Определить неизвестный текст можно с помощью примерения однократного граммирования к сумме по модулю 2 для шифротекстов (т.е. их однократного граммирования) и ко второму известному тексту.

2. Что будет при повторном использовании ключа при шифровании текста?

При повторном использовании ключа для текста (точнее для шифротекста, так как первым испольхованием ключа исходных текст шифруется) мы получаем исходный текст.

```
In [13]:
1 text ='С Новым Годом, друзья!'
2 key = key_generate(len(text))
3 key

Out[13]: '2UUwP8lZISD0NRrT8aKPzn'

In [14]:
1 shifr = gramming(text, key)
2 shifr

Out[14]: 'ГшщЂѳѐzыяΨЎΘ~RѠ0уTŮMeO'

In [15]:
1 gramming(shifr, key)

Out[15]: 'С Новым Годом, друзья!'
```

Figure 4: рис.4. Пример шифрования и расшифровки, используя граммирование с одинаковым ключом.

Контрольные вопросы

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

Если два текста имеют одинаковую длину, то можно их зашифровать одним ключом. Для этого генерируется ключ необходимой длины (длины текстов) и поочерёдно применяется к текстам.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Главный недостаток - возможность расшифровки всех текстов, зашифрованных тем же ключом, что и текст, расшифровать который уже удалось.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Простота использования, так как не нужно генерировать новые ключи для щифрования и знать новые ключи для расшифровки.

Выводы

Я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.