Отчёт по лабораторной работе 8

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

Румянцева Александра Сергеевна

Содержание

Список иллюстраций

Список таблиц

Цель работы

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.

Теория

Граммирование - метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле.

Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы шифра на открытые данные обратимым образом (например, используя операцию сложения по модулю 2). Процесс дешифрования сводится к повторной генерации гаммы шифра при известном ключе и наложении такой же гаммы на зашифрованные данные.

Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей и изменяется случайным образом для каждого шифруемого слова. Если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (подбором ключа). В этом случае криптостойкость определяется размером ключа.

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).

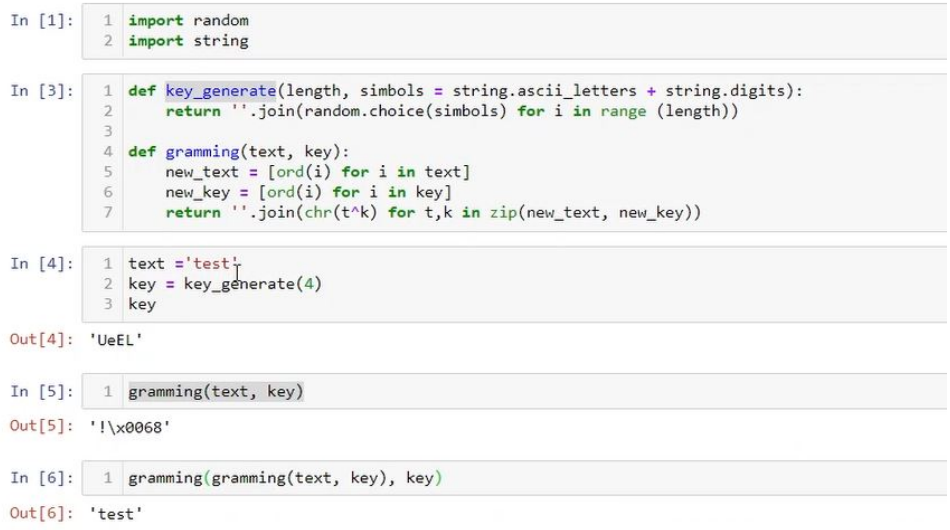

Рис. 0.1: рис.1. Программа для шифрования и дешифрования. Проверка её работы.

Как мы видим из рисунка, программа успешно генерирует ключ нужной длинны, с в его помощью может шифровать и обратно расшифрововать текст.

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.

```
In [5]:
P1 = 'НаВашисходящийот1204'
P2 = 'ВСеверныйфилиалБанка'
print(len(P1),len(P2))

20 20
```

```
In [6]:
key = key_generate(len(P1))
key

Out[6]: '37ahDBRt3DYJ3T4uYqfg'
```

```
In [8]:
C1 = gramming(P1, key)
C2 = gramming(P2, key)
print('Шифротекст для P1, то есть C1 имеет вид: ', C1)
print('Шифротекст для P2, то есть C2 имеет вид: ', C2)

Шифротекст для P1, то есть C1 имеет вид:  ЮЇѳjЌѺГбЍѰЖЃЋѫЊзhCVS
Шифротекст для P2, то есть C2 имеет вид:  СЖєњфЂѮпЊЀwфЋЮЏЮѩьќї
```

Рис. 0.2: 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]:
C1_sum_C2 = gramming(C1, C2) #соответствует сумме по модулю 2 от P1 и P2
C1_sum_C2

Out[9]: "\x0f\x11'\x02}x|\x0e\x07pwr\x00\t\x05SЁЏЊЄ"
```

```
In [10]:
P1_find = gramming(C1_sum_C2, P2)
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]:
P2_find = gramming(C1_sum_C2, P1)
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
```

Рис. 0.3: 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]: 'ГuшщЂѳѐzъыѫѰЎѲ~RѠѲyTѮMeO'

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

Out[15]: 'С Новым Годом, друзья!'
```

Рис. 0.1: рис.4. Пример шифрования и расшифровки, используя граммирование с одинаковым ключом.

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.

Библиография

1. ТУИС РУДН

2. Статья “Принцип шифрования гаммированием” на сайте http://crypto.pp.ua/2010/04/82/

Выводы

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