Отчёт по лабораторной работе 8

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

Румянцева Александра Сергеевна

Содержание

[Цель работы 1](#_Toc90727208)

[Задание 1](#_Toc90727209)

[Теория 1](#_Toc90727210)

[Выполнение лабораторной работы 2](#_Toc90727211)

[Контрольные вопросы 3](#_Toc90727212)

[Библиография 4](#_Toc90727213)

[Выводы 4](#_Toc90727214)

# 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).

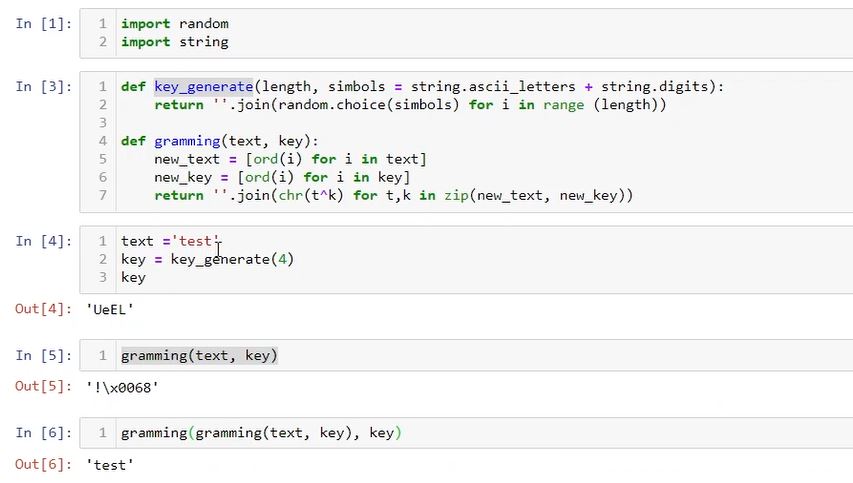
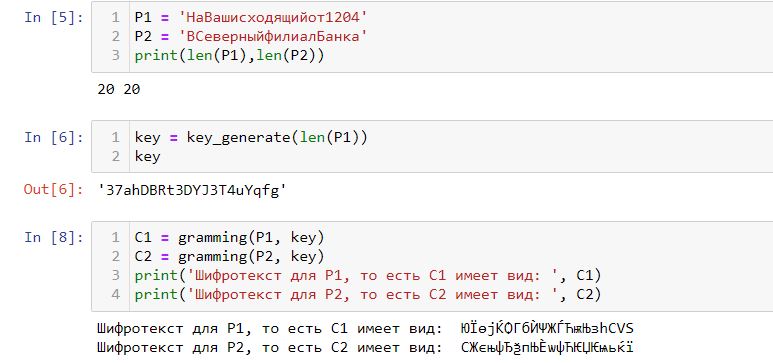


Figure 1: рис.1. Программа для шифрования и дешифрования. Проверка её работы.

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.

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

1. 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).

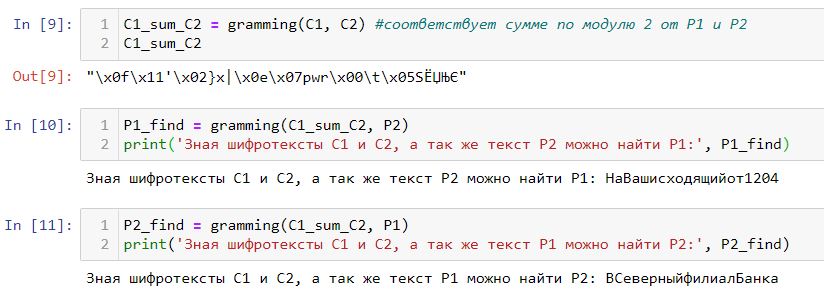


Figure 3: рис.3. Расшифровка текстов без использования ключа.

# 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.

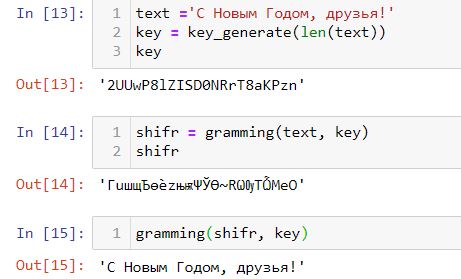


Figure 4: рис.4. Пример шифрования и расшифровки, используя граммирование с одинаковым ключом.

*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.