Отчет по лабораторной работе №8

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

Смородова Дарья Владимировна

2022 Oct 29th

Содержание

# Цель работы

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

# Задание лаборатоной работы

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.

# Теоретическое введение[[1]](#footnote-22)

Исходные данные: Две телеграммы Центра: P1 = НаВашисходящийот1204 P2 = ВСеверныйфилиалБанка Ключ Центра длиной 20 байт: K = 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 OB B2 70 54 Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой ниже.

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

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

получаем:

Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар (известен вид обеих шифровок). Тогда зная и учитывая формулу выше, 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 последняя формула с подстановкой вместо полученных на предыдущем шаге новых символов сообщения . И так далее.

Действуя подобным образом, злоумышленник даже если не прочитает оба cообщения, то значительно уменьшит пространство их поиска.

# Выполнение лабораторной работы

1. Напишем на Python функцию шифрования (рис. 1):



Figure 1: Функция шифрования данных

1. Посмотрим работу данной функции (рис. 2):

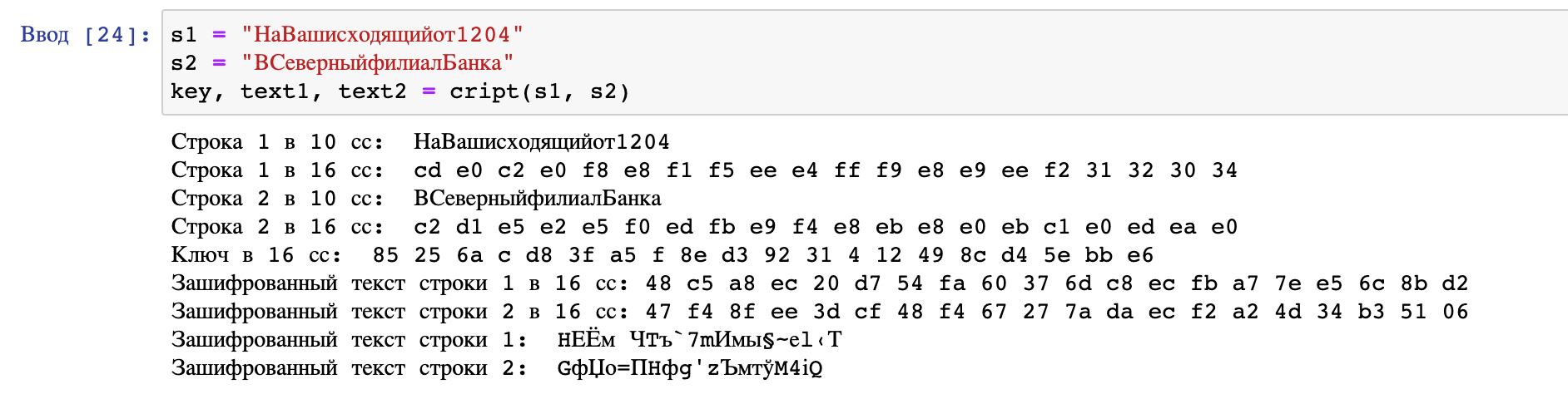


Figure 2: Результат работы функции, шифрующей данные

1. Напишем функцию дешифровки, которая возвращает вторую строку, получив на вход первую строку и обе защифрованные строки (рис. 3):



Figure 3: Функция, дешифрующая данные

1. Посмторим на результаты функции дешифрования(рис. 4):

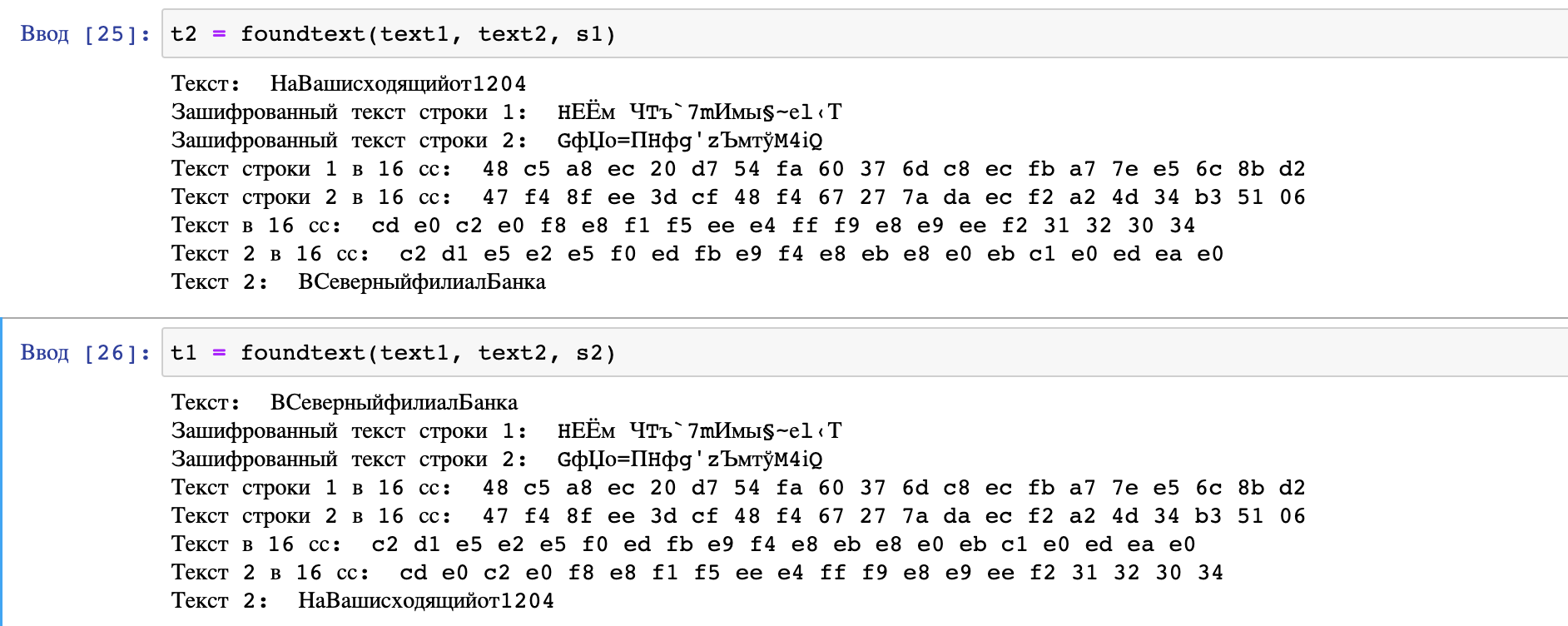


Figure 4: Результат работы функции, дешифрующей данные

# Контрольные вопросы

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

* Чтобы определить один из текстов, зная другой, необходимо вопсользоваться следующей формулой: , где и - шифротексты. Т.е. ключ в данной формуле не используется.

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

* При повторном использовании ключа при шифровании текста получим исходное сообщение.

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

* Режим шифрования однократного гаммирования одним ключом двух открытых текстов реализуется по следующей формуле:
* где - шифротексты, - открытые тексты, - единый ключ шифровки

1. Перечислите недостатки шифрования одним ключом двух открытых текстов.

* Во-первых, имея на руках одно из сообщений в открытом виде и оба шифротекста, злоумышленник способен расшифровать каждое сообщение, не зная ключа. Во-вторых, зная шаблон сообщений, злоумышленник получает возможность определить те символы сообщения , которые находятся на позициях известного шаблона сообщения .

1. Перечислите преимущества шифрования одним ключом двух открытых текстов.

* Такой подход помогает упростить процесс шифрования и дешифровки. Также, при отправке сообщений между 2-я компьютерами, удобнее пользоваться одним общим ключом для передаваемых данных

# Выводы

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

# Список литературы

1. [Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН”](https://esystem.rudn.ru/)

1. Методические материалы к лабораторной работе [↑](#footnote-ref-22)