Отчет по лабораторной работе № 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

дисциплина: Информационная безопасность

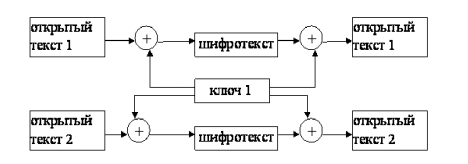
Смирнова Мария Александровна

# Цель работы

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

# Теоретические сведения

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования. Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой, приведённой на рисунке (рис. -@fig:001)



Общая схема шифрования двух различных текстов одним ключом

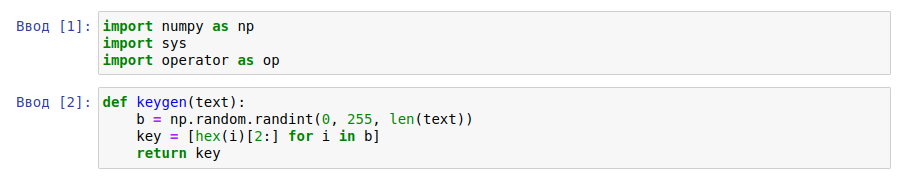
Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования: C1 = P1 ⊕ K, C2 = P2 ⊕ K. Открытый текст можно найти в соответствии с приведенными формулами, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства складываются по модулю 2. Тогда с учётом свойства операции XOR: 1 ⊕ 1 = 0, 1 ⊕ 0 = 1 получаем: C1 ⊕ C2 = P1 ⊕ K ⊕ P2 ⊕ K = P1 ⊕ P2 . 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 C1 ⊕ C2 (известен вид обеих шифровок). Тогда зная P1 и учитывая свойство операции XOR, имеем: C1 ⊕ C2 ⊕ P1 = P1 ⊕ P2 ⊕ P1 = P2 . Таким образом, злоумышленник получает возможность определить те символы сообщения P2 , которые находятся на позициях известного шаблона сообщения P1 . В соответствии с логикой сообщения P2, злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения P2. Затем вновь используется та же формула с подстановкой вместо P1 полученных на предыдущем шаге новых символов сообщения P2 . И так далее. Действуя подобным образом, злоумышленник даже если не прочитает оба сообщения, то значительно уменьшит пространство их поиска.

# Задание

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 P 1 и P 2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

# Выполнение лабораторной работы

1. Подключим необходимые библиотеки и напишем функцию для генерации ключа (рис. -@fig:002).



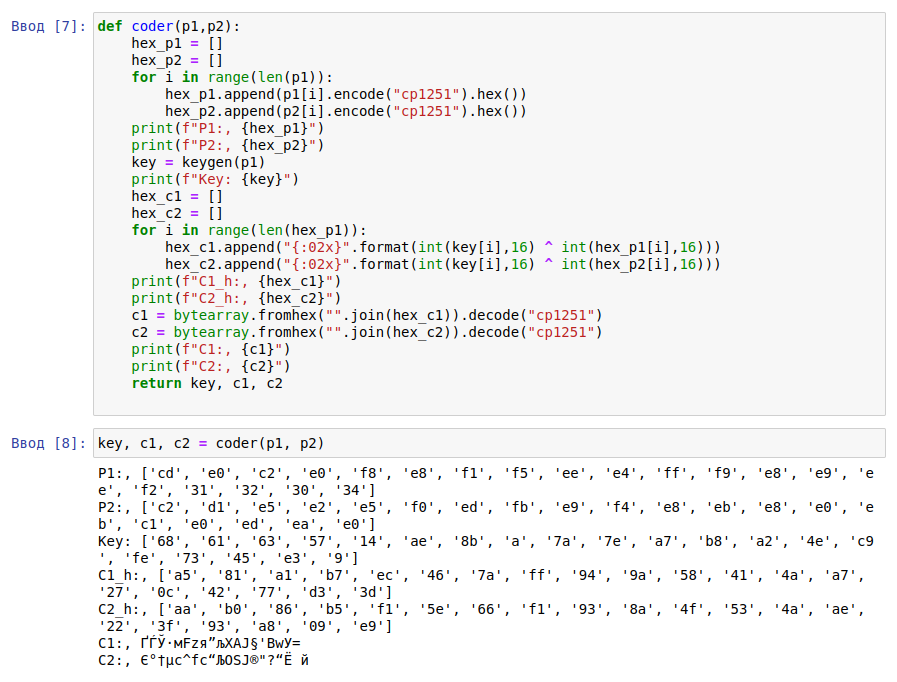
Подключение библиотек и генерация ключа

1. Зададим исходные тексты (рис. -@fig:003).

Тексты P1 и P2

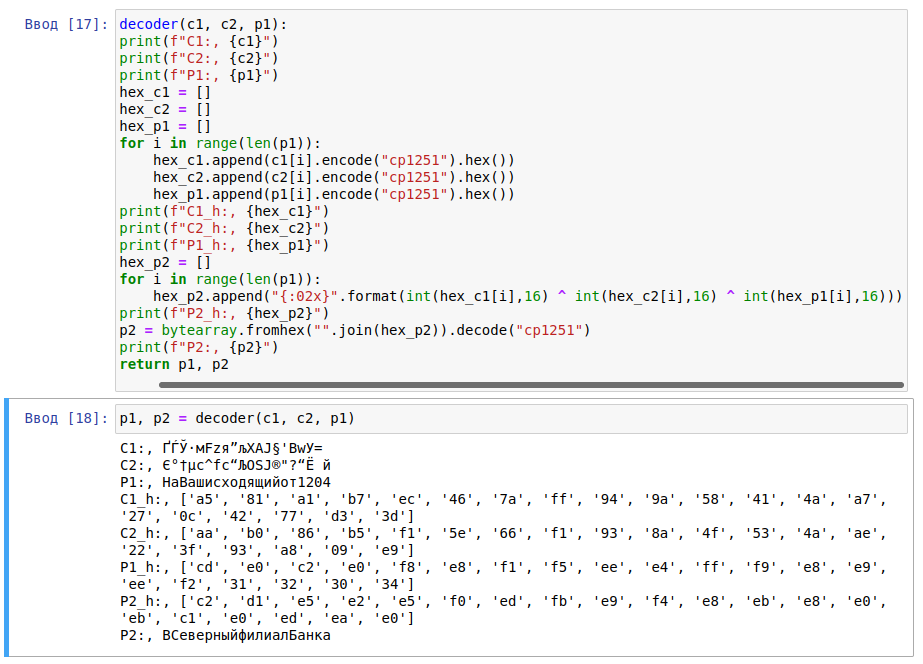
Тексты P1 и P2

1. Напишем функцию coder, которая с помощью операции XOR будет шифровать открытый текст. Проверим ее работу (рис. -@fig:004).



Шифрование

1. Напишем функцию decoder, которая будет с помощью операции XOR при известных шифротекстах и открытом тексте определит второй исходный текст. Проверим ее работу (рис. -@fig:005).



Дешифрование

# Контрольные вопросы

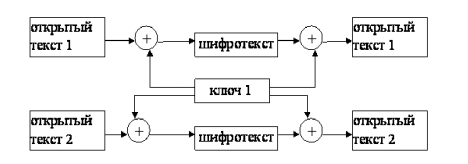
### 1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

Это наглядно показано в 4 пункте работы.

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

Исходный текст может быть восстановлен с помощью статистического анализа двух вариантов зашифрованного текста. Важнейшим правилом криптозащиты является достаточно частая смена ключей. Причем частота может определяться исходя из длительности использования ключа или исходя из объема зашифрованного текста.

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

Ответ представлен на схеме (рис. -@fig:006) 

### 4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

В алгоритм сложнее внести изменения и более длинные ключи. Так же снижается безопасность обоих текстов.

### 5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Небольшое число ключей для передачи, простота алгоритма, удобство для обеих сторон.

# Выводы

В процессе выполнения лабораторной работы мы освоили на практике применение режима однократного гаммирования одним ключом на языке python.