Лабораторная работа №8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Дисциплина: Информационная безопасность

Манаева Варвара Евгеньевна

Содержание

# 1 Техническое оснащение:

* Персональный компьютер с операционной системой Windows 10;
* Планшет для записи видеосопровождения и голосовых комментариев;
* Microsoft Teams, использующийся для записи скринкаста лабораторной работы;
* Приложение Pycharm для редактирования файлов формата *md*;
* *pandoc* для конвертации файлов отчётов и презентаций.

# 2 Цели и задачи работы

## 2.1 Цель

Изучение механизма шифрования гаммирование как простейшего варианта системы шифрования с закрытым ключом.

## 2.2 Задачи [1]

1. Рассмотреть особенности и особенности кодирование однократного гаммирования с использованием одного ключа.
2. Создать код, который будет показывать принцип работы нескольких шифротекстов с одним ключом и его взлом.
3. изучить способы взлома и декодирование шифротекста без ключа.

# 3 Теоретическое введение

Пример:

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 (смотреть лабораторную).

# 4 Выполнение лабораторной работы

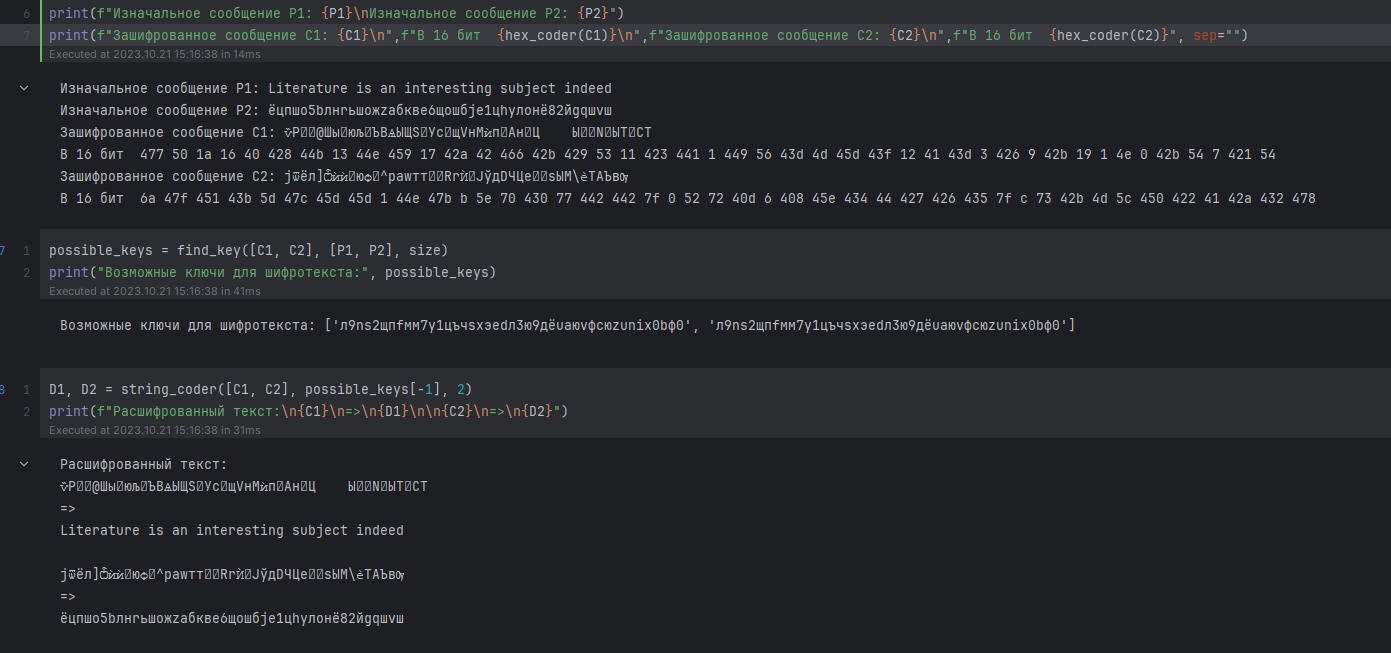
## 4.1 Условие задания

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 P1 и P2 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.

# 5 Выполнение лабораторной работы

1. Код и результат его выполнения (??)

def key\_create(s, alf):  
 k = ''.join(random.choice(alf) for i in range(s))  
 return k



Результат

# 6 Контрольные вопросы

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

Ответ: Это возможно сделать только в том случае если текст P1 и P2 одной длины и имеют общий ключ.

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

Ответ: Из-за одинаковости способа кодирование и декодирование после повторного использование слова и ключа даст нам шифротекст.

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

Ответ: Фактически, следуя схеме 8.1 и принципу “шифра XOR”, мы просто имеем два параллельных кодирования и декодирования с использованием одного ключа.

1. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Ответ: Если вспомнить требования для абсолютной стойкости шифра, рассмотренных в предыдущей лабораторной, можно сразу понять по первому же пункту, что если ключ не будет случайным и каждый раз новым для каждой строки, то, найдя пересечения или аналоги в шифротекстах, можно определить одинаковые символы, что может пошатнуть защиту текста даже если у вас нет ни одного исходного кода. При этом получается, что если есть исходный текст (хотя бы один образец), определить другие слова становится легко.

1. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Ответ:

* требуется передать один ключ, что сделать проще и быстрее
* при передаче большого количества шифротекста нет шанса запутаться в их порядке сочетания с ключами.

# 7 Выводы по проделанной работе

## 7.1 Вывод

В результате выполнения работы мы освоили на практике применение режима однократного гаммирования и возможных способах взлома при отсутствии ключа и наличие исходных текстов и шифротекстов.

Были записаны скринкасты выполнения и защиты лабораторной работы.

Ссылки на скринкасты:

* [Выполнение, Youtube](https://youtu.be/UkINyO_l1Bc)
* [Выполнение, Rutube](https://rutube.ru/video/f8018ffb05bfa7efdb1c0340a22a4cbb/)
* [Защита презентации, Youtube](https://youtu.be/7uqRu-Ntaj0)
* [Защита презентации, Rutube](https://rutube.ru/video/7e5e7f2982dd9e03fd523fd00a9d6027/)

# Список литературы

1. Лабораторная работа № 8 [Электронный ресурс]. Российский Университет Дружбы Народов имени Патрису Лумумбы, 2023. URL: <https://esystem.rudn.ru/mod/resource/view.php?id=1031384>.