# Лабораторная работа №7

# Дисциплина: информационная безопасность

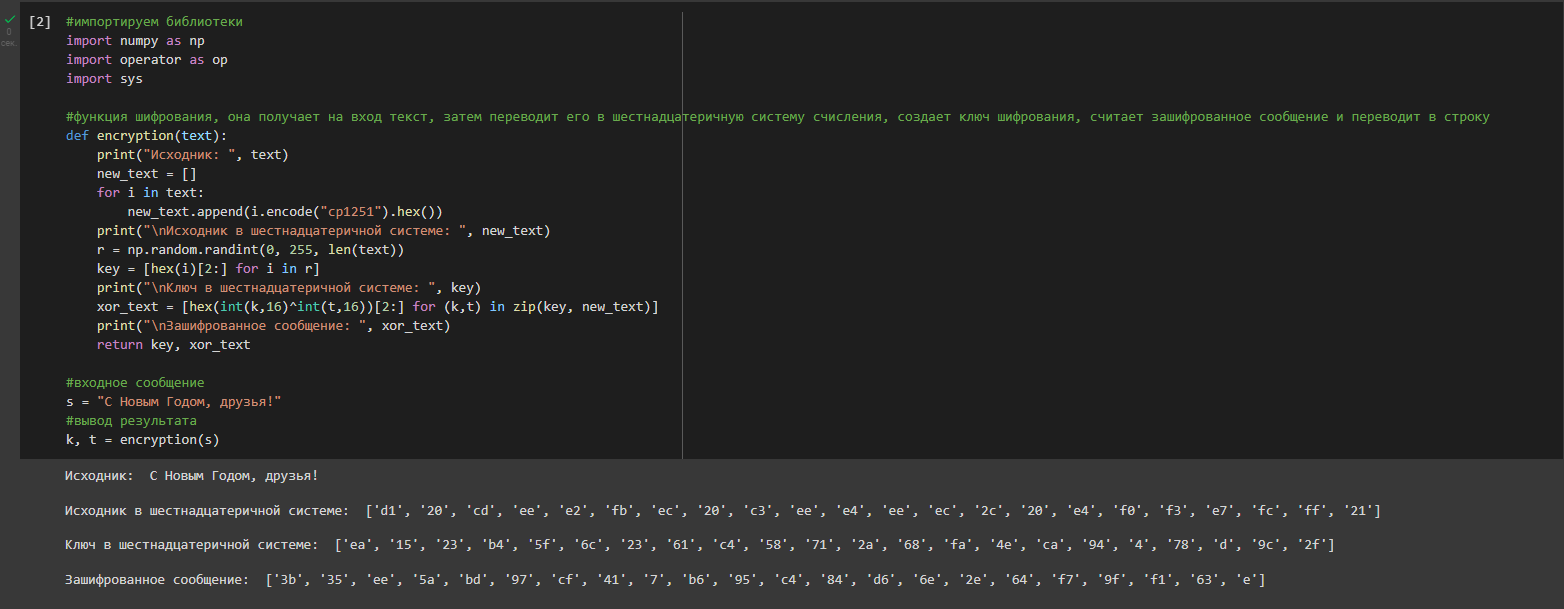
# Студент: Подорога Виктор Александрович

# Цель работы

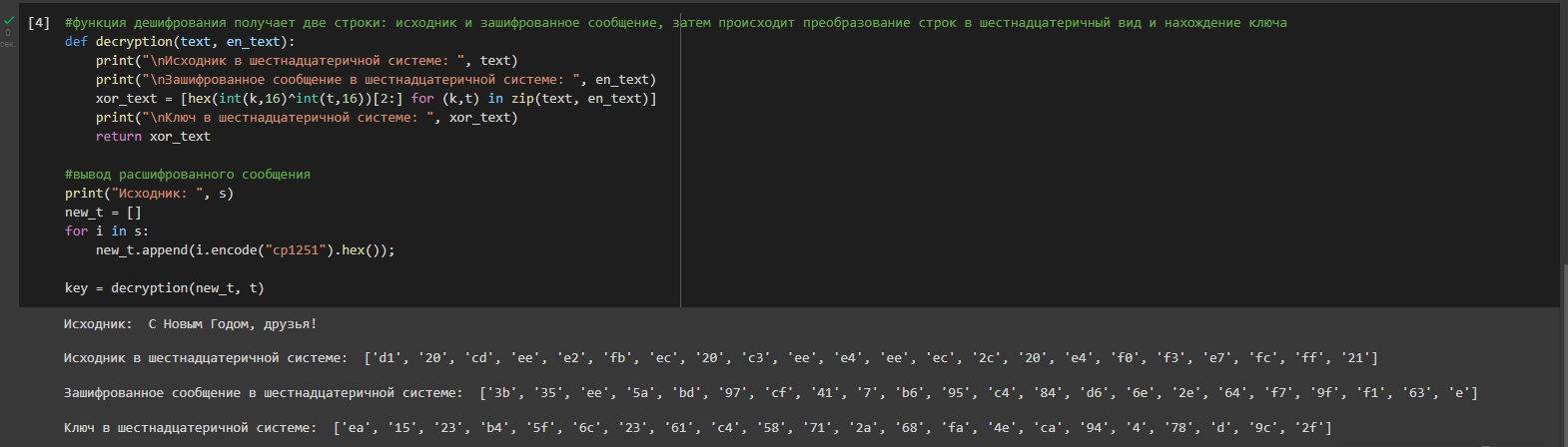
Освоить на практике применение режима однократного гаммирования.

# Выполнение лабораторной работы

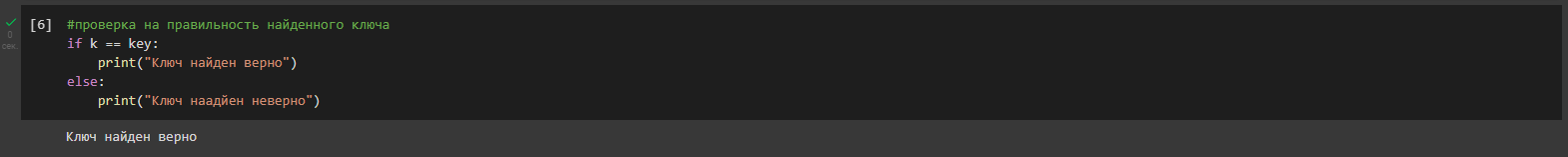
1. Напишем код программы для зашифровки сообщения "С Новым Годом, друзья!":

* 
* *Рис. 1. Программа для зашифровки сообщения*

1. Напишем код программы для расшифровки зашифрованного сообщения и нахождения ключа шифрования:

* 
* *Рис. 2. Программа для расшифровки и нахождения ключа*

1. Проверим правильность нахождения ключа:

* 
* *Рис. 3. Проверка*
* **Поясните смысл однократного гаммирования.**
* Гаммирование – выполнение операции XOR между элементами гаммы и элементами подлежащего сокрытию текста. Если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.
* **Перечислите недостатки однократного гаммирования.**
* Абсолютная стойкость шифра доказана только для случая, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения.
* **Перечислите преимущества однократного гаммирования.**
* Во-первых, такой способ симметричен, т.е. двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение. Во-вторых, шифрование и расшифрование может быть выполнено одной и той же программой. Наконец, криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении C все различные ключевые последовательности K возможны и равновероятны, а значит, возможны и любые сообщения P.
* **Почему длина открытого текста должна совпадать с длиной ключа?**
* Если ключ короче текста, то операция XOR будет применена не ко всем элементам и конец сообщения будет не закодирован. Если ключ будет длиннее, то появится неоднозначность декодирования.
* **Какая операция используется в режиме однократного гаммирования, назовите её особенности?**
* Наложение гаммы по сути представляет собой выполнение побитовой операции сложения по модулю 2, т.е. мы должны сложить каждый элемент гаммы с соответствующим элементом ключа. Данная операция является симметричной, так как прибавление одной и той же величины по модулю 2 восстанавливает исходное значение.
* **Как по открытому тексту и ключу получить шифротекст?**
* В таком случае задача сводится к правилу: Ci = Pi ⊕ Ki, т.е. мы поэлементно получаем символы зашифрованного сообщения, применяя операцию исключающего или к соответствующим элементам ключа и открытого текста.
* **Как по открытому тексту и шифротексту получить ключ?**
* Подобная задача решается путем применения операции исключающего или к последовательностям символов зашифрованного и открытого сообщений: Ki = Pi ⊕ Ci.
* **В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра?**
* Необходимые и достаточные условия абсолютной стойкости шифра: полная случайность ключа; равенство длин ключа и открытого текста; однократное использование ключа.

# Вывод

В ходе лабораторной работы я научился на практике применять режим однократного гаммирования.