# Лабораторная работа №8

# Дисциплина: информационная безопасность

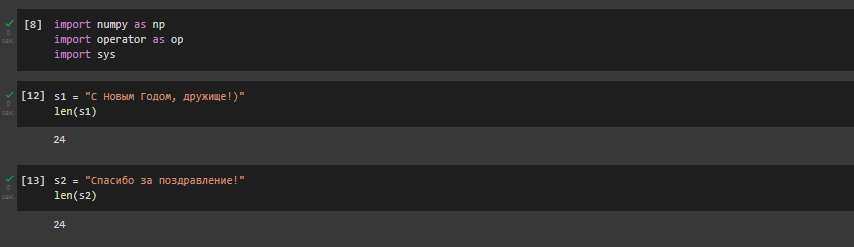
# Студент: Подорога Виктор Александрович

# Цель работы

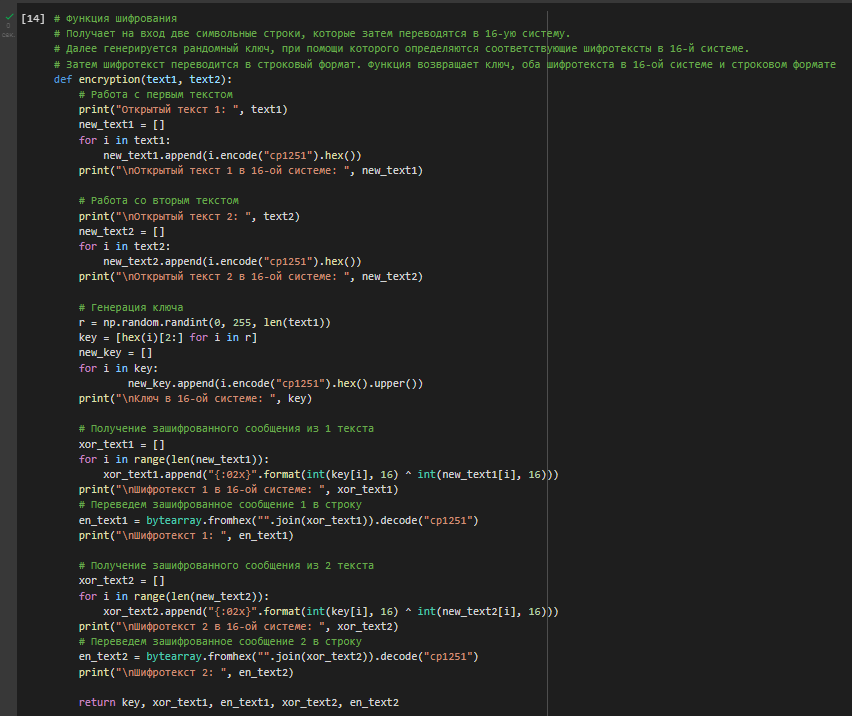
Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Выполнение лабораторной работы

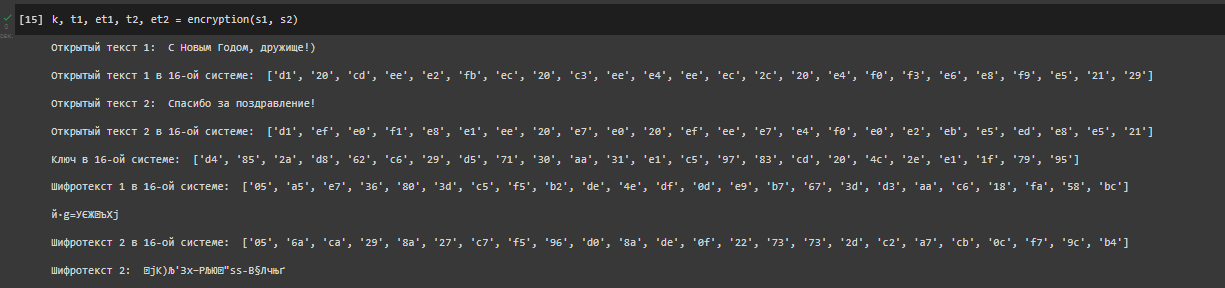
1. Импортируем необходимые библиотеки и введем исходные текстовые сообщения:

* 
* *Рис. 1. Импорт библиотек и исходные данные*

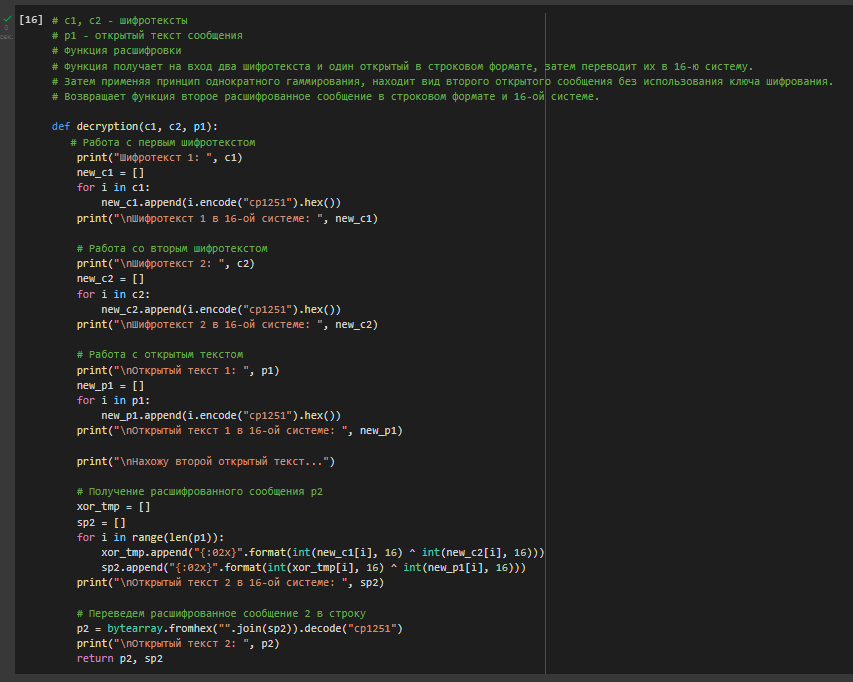
1. Опишем функцию шифрования:

* 
* *Рис. 2. Код функции шифрования*

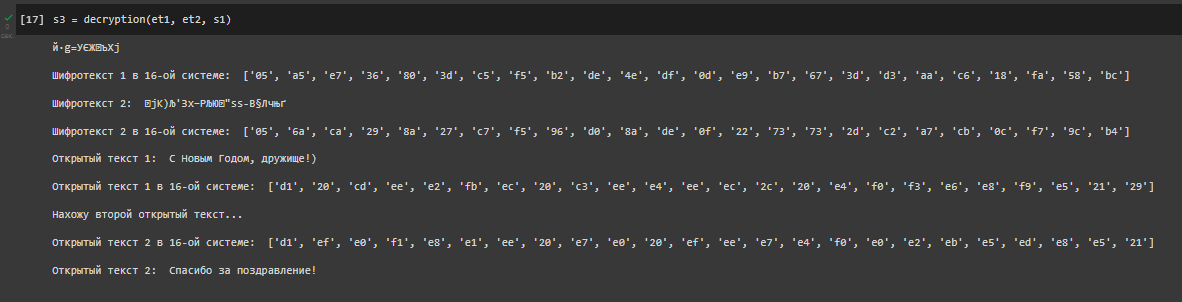
1. Выведем результат работы функции шифрования:

* 
* *Рис. 3. Результат работы функции шифрования*

1. Опишем функцию дешифровки:

* 
* *Рис. 4. Код функции дешифровки*

1. Выведем результат работы функции дешифровки:

* 
* *Рис. 5. Результат работы функции дешифровки*
* **Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?**
* Для этого надо воспользоваться формулой:
* C1 ⊕ C2 ⊕ P1 = P1 ⊕ P2 ⊕ P1 = P2, где *С1* и *С2* – шифротексты. Как видно, ключ в данной формуле не используется.
* **Что будет при повторном использовании ключа при шифровании текста?**
* В таком случае мы получим исходное сообщение.
* **Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?**
* Он реализуется по следующей формуле:
* C1 = P1 ⊕ K, C2 = P2 ⊕ K, где *Сi* – шифротексты, *Pi* – открытые тексты, *K* – единый ключ шифрования.
* **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 *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*. Таким образом, применяя формулу из пункта 1, с подстановкой вместо *P1* полученных на предыдущем шаге новых символов сообщения *P2*, злоумышленник если не прочитает оба сообщения, то значительно уменьшит пространство их поиска.
* Наконец, зная ключ, злоумышленник сможет расшифровать все сообщения, которые были закодированы при его помощи.
* **Перечислите преимущества шифрования одним ключом двух открытых текстов.**
* Такой подход помогает упростить процесс шифрования и дешифровки. Также при отправке сообщений между двумя компьютерами удобнее пользоваться одним общим ключом для передаваемых данных.

# Вывод

В ходе лабораторной работы я получил практические навыки применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.