# Отчет о практических заданиях по курсу «Математические основы защиты информации и информационной безопасности»

Ссылка на репозиторий: <https://github.com/viktorharlov74/information-security-Labs>

## Задание 1.

Напишите функцию конвертации текста, представленном в 16ричном виде, в base64.

Пример:

Входные данные:

49276d207374756479696e672043727970746f677261706879206c696b6520436c6175646520456c776f6f64205368616e6e6f6e21

Выходные данные:

SSdtIHN0dWR5aW5nIENyeXB0b2dyYXBoeSBsaWtlIENsYXVkZSBFbHdvb2QgU2hhbm5vbiE=

Решение (файл <https://github.com/viktorharlov74/information-security-Labs/blob/master/task1.ipynb> ).

Решением задачи является функция DecodeBase64FromHex, которая принимает строку представленном в шестнадцатеричном виде, и переводит в base64.

Тесты:  
  


## Задание 2.

Напишите функцию, которая принимает в качестве параметров два буфера одинаковой длины и производит операцию XOR над ними.

Решение: (<https://github.com/viktorharlov74/information-security-Labs/blob/master/task2%2Bxor.ipynb> )

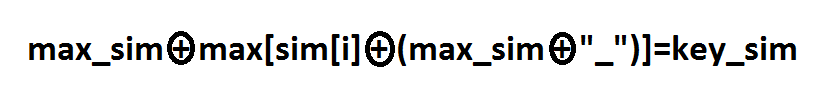
Решением задачи является функция XORbuffer она принимает в себя два 16ричных числа одинаковой длины

Тесты:

## Задание 3.

Решение: (<https://github.com/viktorharlov74/information-security-Labs/blob/master/task_3_final.ipynb> )

Решением задачи является функция ConvertShifrStrFromHex она принимает в качестве аргумента зашифрованную hex строку,

 переводит hex строку в строку utf-8. Затем в этой строке она находит ключ,т.е символ с помощью которого шифровали, делает она это по следующей формуле.  
 , где max\_sim- самый часто встречающийся символ в исходной строке,

max[]-функция поиска самого частого элемента в строке, которая вышла с помощью XOR

Sim[i]-элемент исходной строки.

“\_”-символ пробела

После того как ключ найден, происходит посимвольный xor с элементами исходной зашифрованной строки.

Другие используемые функции:

convert\_base-функция перевода из одной системы счисления в другую,

XORbin-бинарный ксор

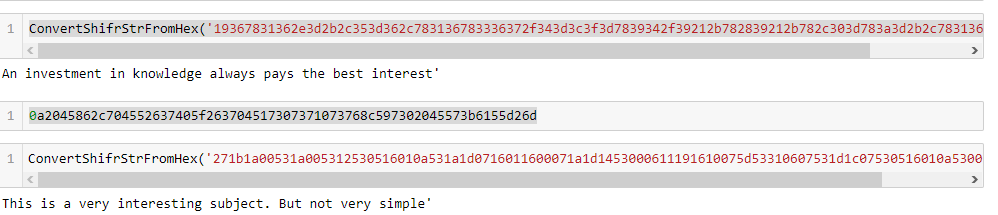
ConvertCharsStrToHex -перевод символа в 16ричную систему счисления

FindKeySimbFromHex вспомогательная функция выполняет эту формулу:



 Результат:

Тесты:



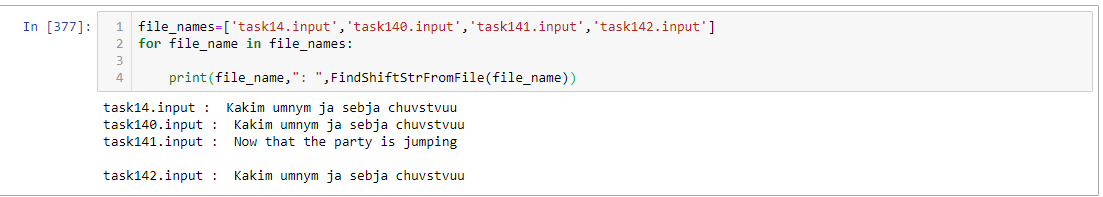
Задание 4.

В качестве входных данных дается файл со строками в hex. Одна из этих строк зашифрована с помощью XOR на одно-символьном ключе. Найдите и расшифруйте эту строку.

Решение:

Решением задачи является функция FindShiftStrFromFile.

Она на вход принимает имя файла и возвращает первую зашифрованную строку или -1 если такой строки нету. Внутри себя функция для каждой строки выполняет функцию ConvertShifrStrFromHex из 3го задания и проверяет результат на соответсвие строке, если строка не похожа на «что-то внятное», то он переходит к следующей строке,до тех пор пока не найдет зашифрованную строку. (За этот функционал отвечает функция CheckDedhifrStr)

Тесты:

## Задание 5.

Реализуйте шифрование XOR'ом с повторяющимся ключом.

Решение:

Решением задачи является функция ShifrXorWithRepeatKey которая принимает два параметра: имя файла с текстом и ключ.



Тесты:

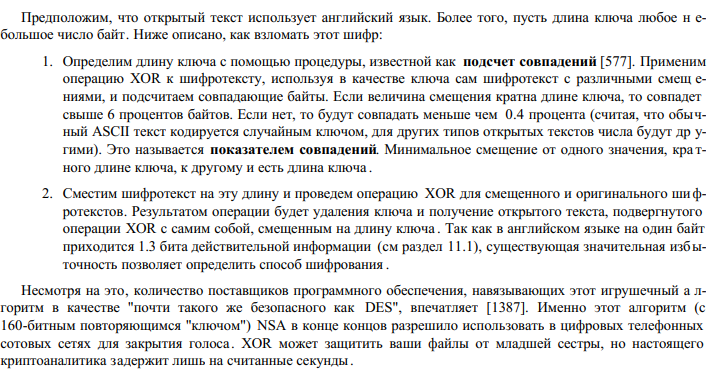


## Задание 6.

Задание: Расшифруйте данные зашифрованные XOR'ом с повторяющимся ключом.

Входные данные: ссылка

Решение.  
1. Найти длину ключа.

2. Расшифровать сообщение