МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ

КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования   «Московский технический университет связи и информатики»



Кафедра"Системное программирование"

ЛАБОРАТОРНАЯ РАБОТА № 4

Электронно-цифровая подпись и приемы хеширования

По дисциплине “Основы информационной безопасности”

                                      Выполнили: студенты гр. БВТ2201

Шамсутдинов Р.Ф.

Новожилов Д.П.

Титков Д.П.

Москва, 2023 г

Цель работы:

Овладеть практическими навыками закрытия информации электронно-цифровой подписью и приемами хеширования, рассмотрение хеширования методом контрольных сумм и методом наложения кодов — гаммированием.

Ход работы:

1. Ознакомиться с теоретической частью данной работы.

2. Составить программу шифрования методом контрольных сумм.

3. Составить программу шифрования методом хеширования с применением гаммирования.

4. Составить отчет по проделанной работе.

5. Защитить работу.

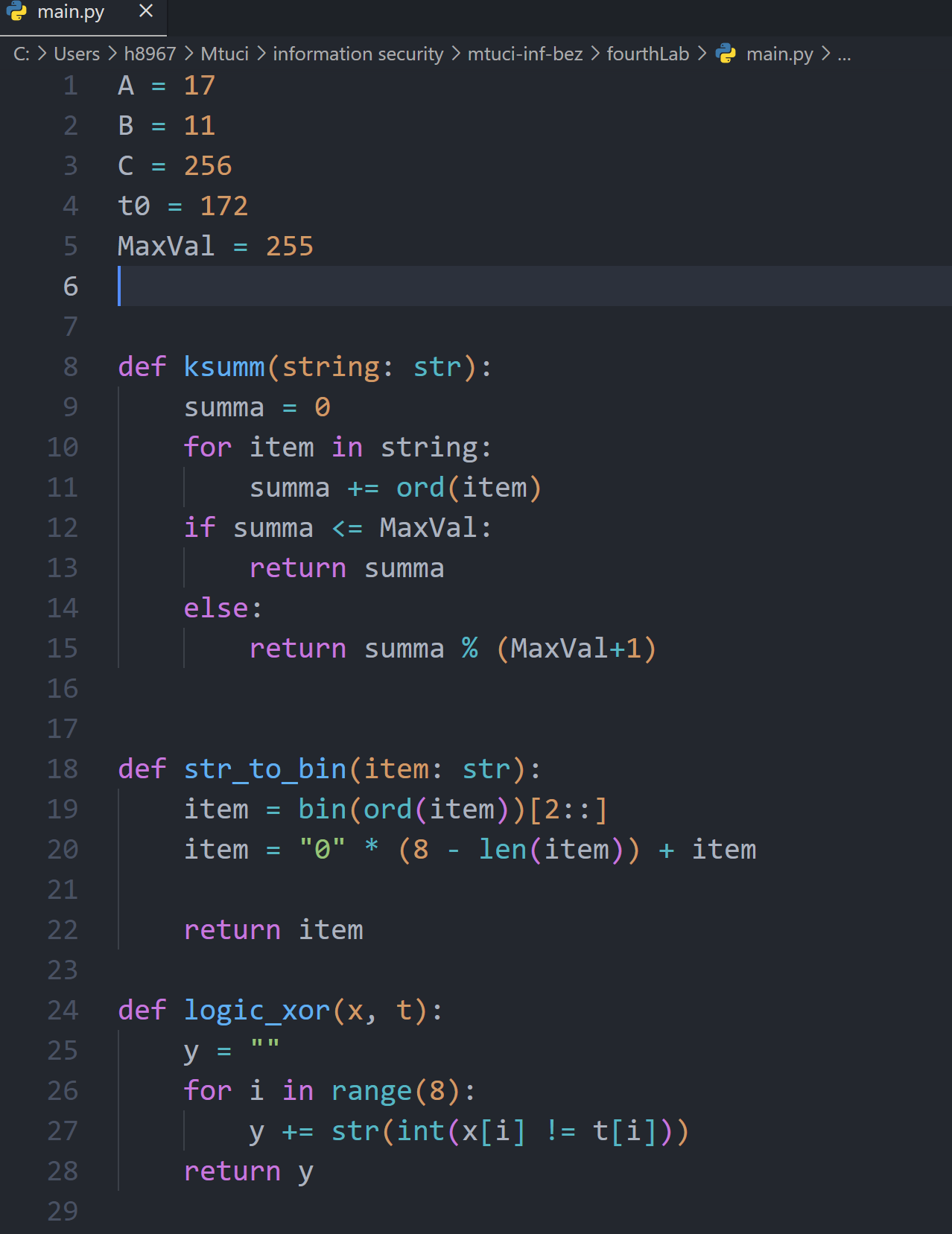
Задание к лабораторной работе № 4

Составить программу шифрования методом контрольных сумм и методом хеширования с применением гаммирования.

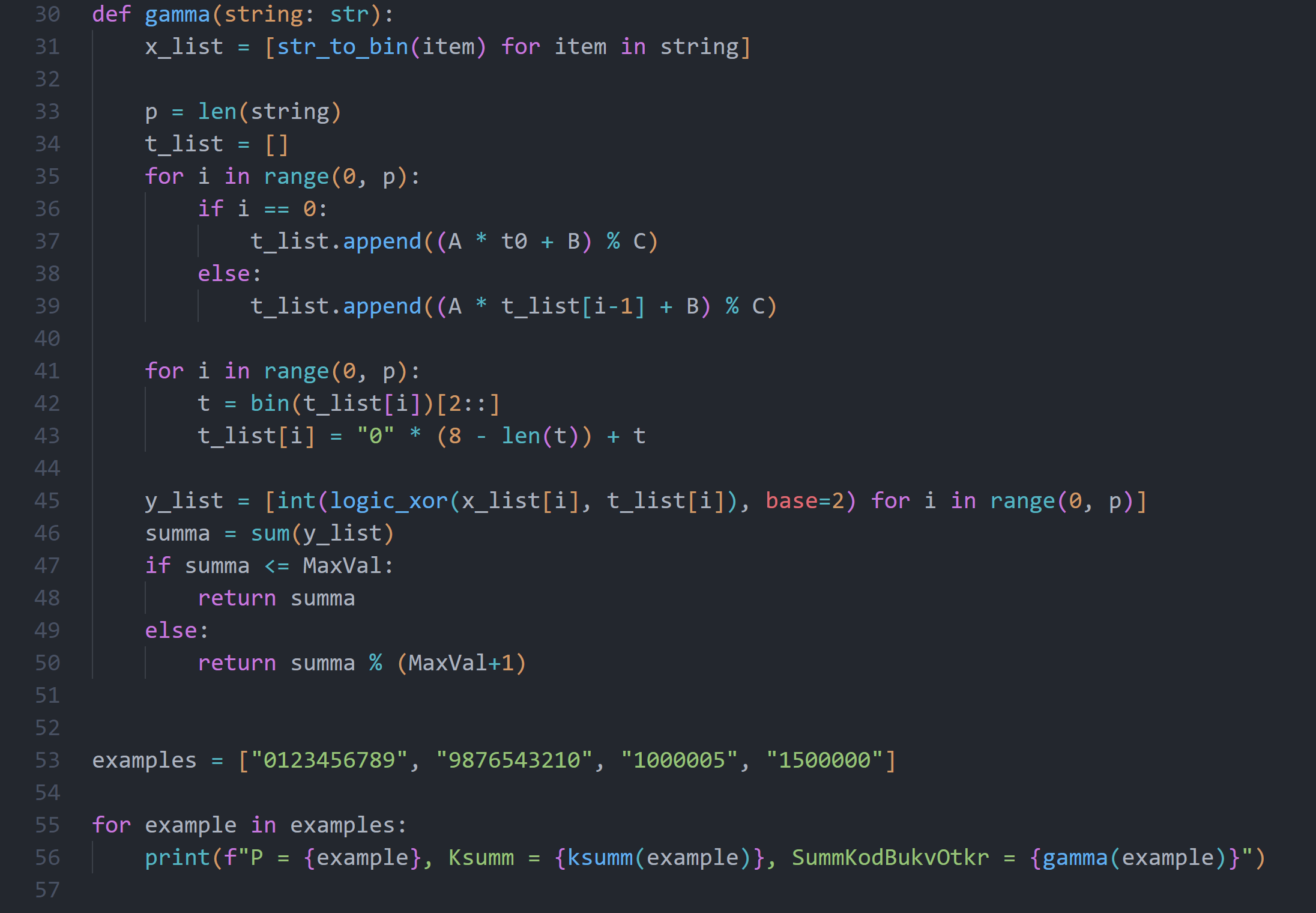
Вариант № 1

A = 17, B = 11, C= МахVal + 1 = 256, t0 = 172.

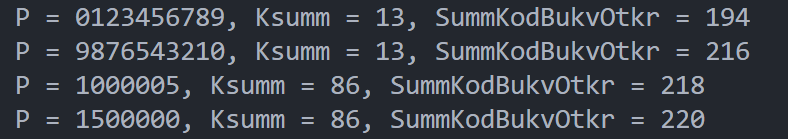
Объявление переменных из условия и создание функции для вычисления контрольной суммы.



Создание функции для вычисления контрольной суммы методом хеширования с применением гаммирования.



Проверка работы программы:



Контрольные вопросы:

1. Назвать три функции ЭЦП

 1) Функция авторизации подписавшегося; 2) Гарантия того, что подписавшийся не откажется от подписанного документа; 3) Подтверждение подлинности документа.

1. Перечислить этапы формирования ЭЦП

 1) Отправитель X по специальному алгоритму обрабатывает документ, предназначенный для адресата Y. Вырабатывается некий параметр, характеризующий документ в целом; 2) X с помощью своего секретного ключа шифрует полученный параметр - итоговый шифр и является ЭЦП отправителя X; 3) X отправляет Y документ и свою ЭЦП 4) Y реализует на полученном документе тот же алгоритм, которым пользовался X; 5) Y дешифрует ЭЦП X, пользуясь открытым (публичным) ключом X; 6) Y сравнивает значение параметра, полученного в пункте 4, с расшифрованным значением ЭЦП. Значения должны совпадать, если документ и/или ЭЦП не были изменены.

1. Что шифруется при применении ЭЦП?

 Хэш-сумма файла.

1. Что называется хэш-значением документа?

 Значение интегрального параметра документа.

1. Что называется хэш-функцией?

 Хэш-функция преобразует исходные данные в некоторый меньший массив данных; результат выполнения хэш-функции с двумя случайными наборами входных данных с высокой вероятностью должен быть различным. Сложность алгоритма такой функции должна обеспечить невозможность изменения осмысленного исходных данных с сохранением того же результата. Также алгоритм функции реализуется так, что по результату невозможно однозначно восстановить исходные данные.

1. Что называется сворачиванием (хэшированием) документа?

 Вычислением результата используемой хэш-функции для данных, содержащихся в документе.

1. В чём заключается метод контрольных сумм?

Складываются все коды символов в документе. Если значение какого-либо кода превышает максимальное допустимое значение, то берётся значение K mod (MaxVal + 1).

1. Перечислить этапы метода хэширования с применением гаммирования

1) Каждый символ представляется в виде восьмибитного двоичного слова; 2) По рекуррентной формуле создаётся последовательность псевдослучайных чисел; 3) Значение каждого символа складывается по модулю 2 с соответствующим значением в последовательности псевдослучайных чисел; 4) Полученные числа переводятся в десятичную систему счисления; 5) Полученная последовательность суммируется по модулю MaxVal + 1.

1. Недостаток метода контрольных сумм

 Можно произвольным образом изменить порядок следования символов в файле, и при этом контрольная сумма останется прежней.

Вывод:

Проделав данную работу, мы научились хешировать данные методом контрольных сумм и методом гаммирования.