Міністерство освіти і науки України

Національний технічний університет «ХПІ»

Навчально-науковий інститут комп’ютерних наук та інформаційних технологій

Кафедра комп’ютерної інженерії та програмування

**ЗВІТ**

з лабораторної роботи № 2

з дисципліни «Сучасні технології безпечного програмування»

**«Симетричне шифрування»**

Виконав:

студент гр. КН-Н922б

Зозуля В.Д.

Перевірив:

доцент кафедри

Бульба С.С.

Харків – 2022

**Мета роботи**: Дослідити принципи роботи симетричного шифрування на прикладі алгоритму AES (128).

Як працює алгоритм AES128:

1. Initialization
   1. Add round key
2. N rounds
   1. Sub bytes
   2. Shift rows
   3. Min columns
   4. Add round key
3. Last round
   1. Sub bytes
   2. Shift rows
   3. Add round key

**Хід роботи**

1. Initialization. Перший раунд та кількість раундів.

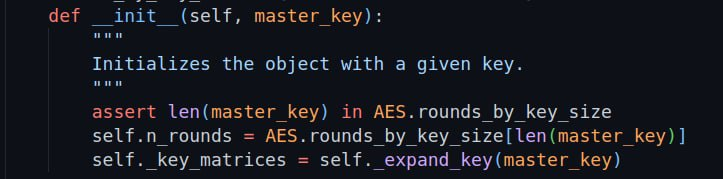


Рисунок 1. Initialization

1. N rounds with last round.

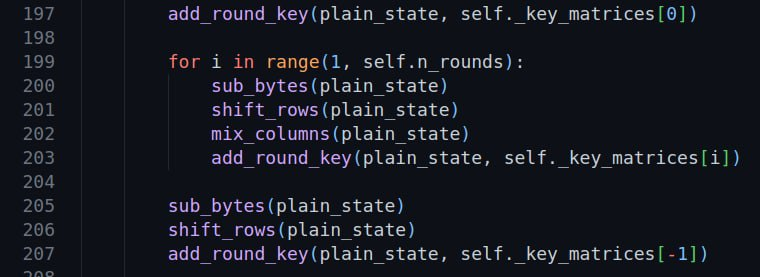


Рисунок 2. Encryption.

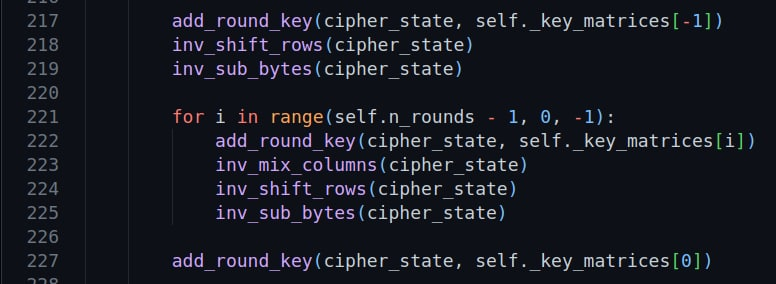


Рисунок 3. Decryption.

**Результат роботи**

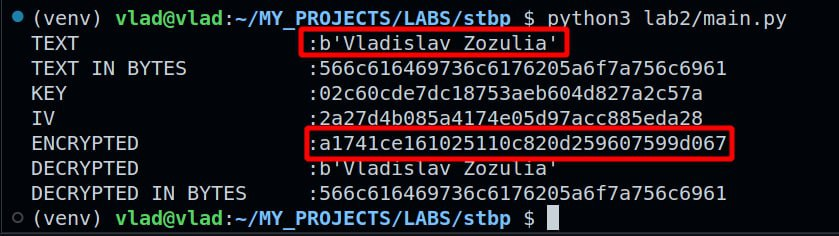


Рисунок 4. Результат роботи програми

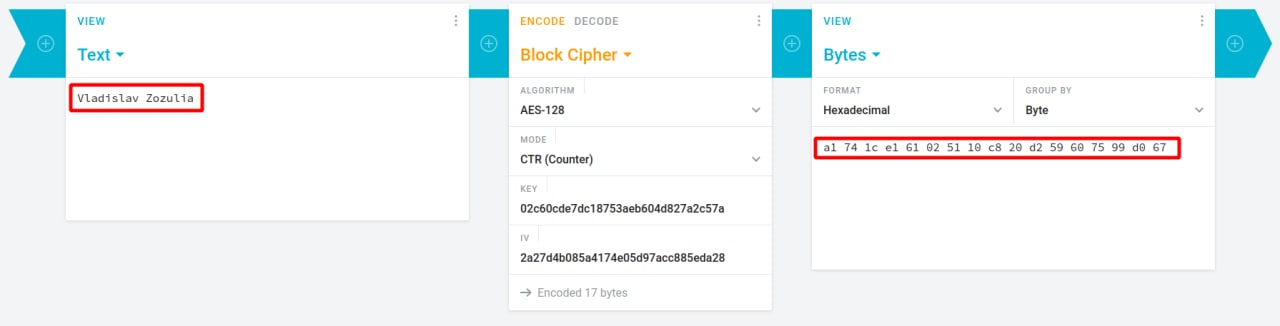


Рисунок 5. Порівняння із сайтом <https://cryptii.com>

**Висновок**

Дослідив принципи роботи симетричного шифрування на прикладі алгоритму AES128.