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 № 4

з дисципліни «Сучасні технології безпечного програмування»

**«Використання мнемонічних фраз для формування ключів шифрування»**

Виконав:

студент гр. КН-Н922б

Зозуля В.Д.

Перевірив:

доцент кафедри

Бульба С.С.

Харків – 2022

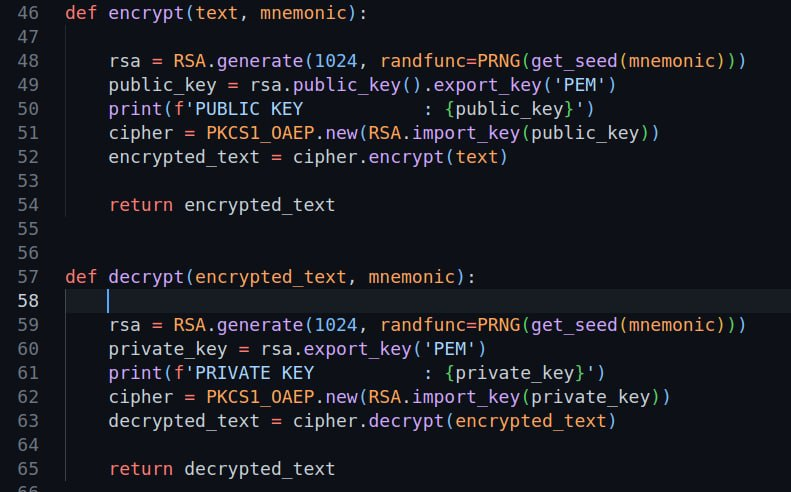
**Мета роботи**: Дослідити і реалізувати використання мнемонічних фраз для формування ключів шифрування за допомогою алгоритму bip39.

**Хід роботи**

1. Bip39 word sets for UA and EN.



1. Encrypt and Decrypt methods.



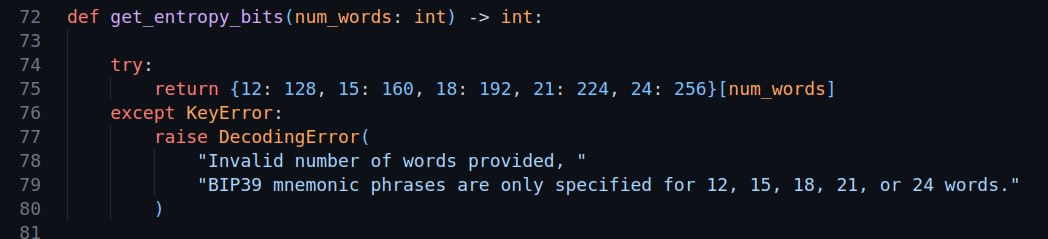
1. Added randfunc parameter to reproduce RSA keys



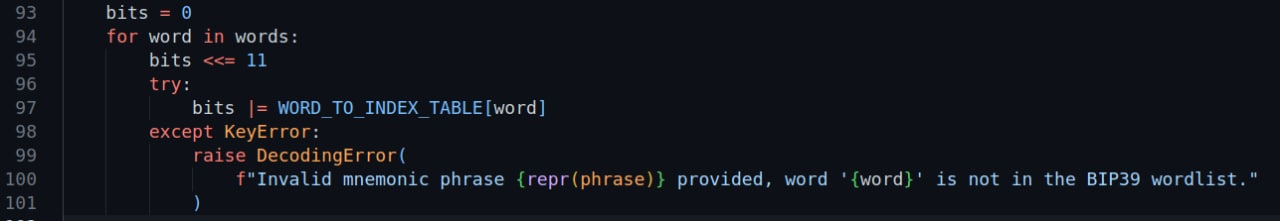
1. Validate letters in mnemonic phrase



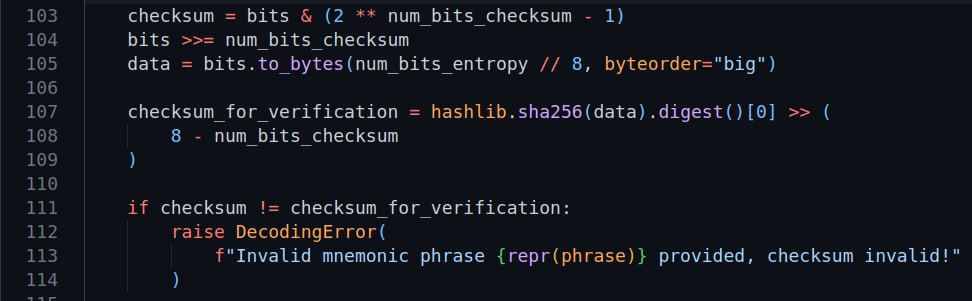
1. Validate words length



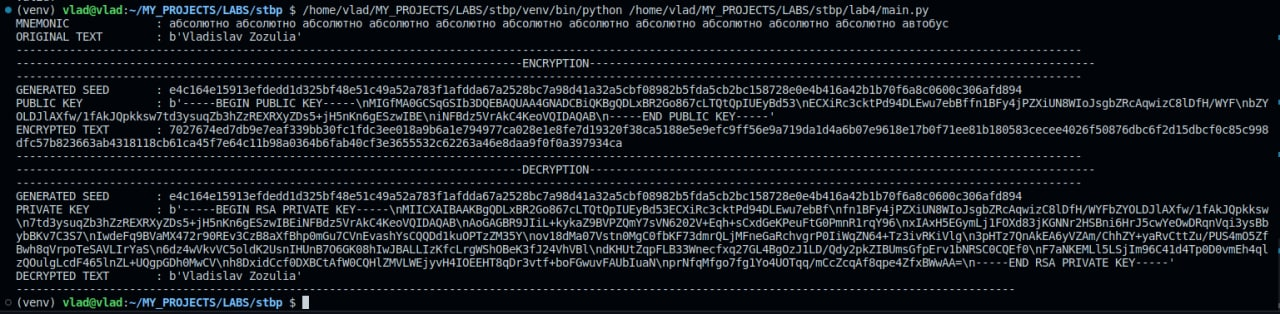
1. Validate words



1. Check checksum



**Результат роботи**

Рисунок 1. Результат роботи

**Висновок**

Дослідив і реалізував використання мнемонічних фраз для формування ключів шифрування за допомогою алгоритму bip39.