**Lab01 - IS355.Q11**

**MSSV:** 22520335

**Họ và tên:** Nguyễn Trung Duy

**Kết quả bài tập tại lớp**

**B. Chữ ký số lên dữ liệu trong blockchain**

1. Bạn thử đóng vai trò của Tèo viết một đoạn chương trình Python để cố gắng sửa thông điệp của Tý thành “Ty hates cat”. Bạn chụp hình lại kết quả chạy.

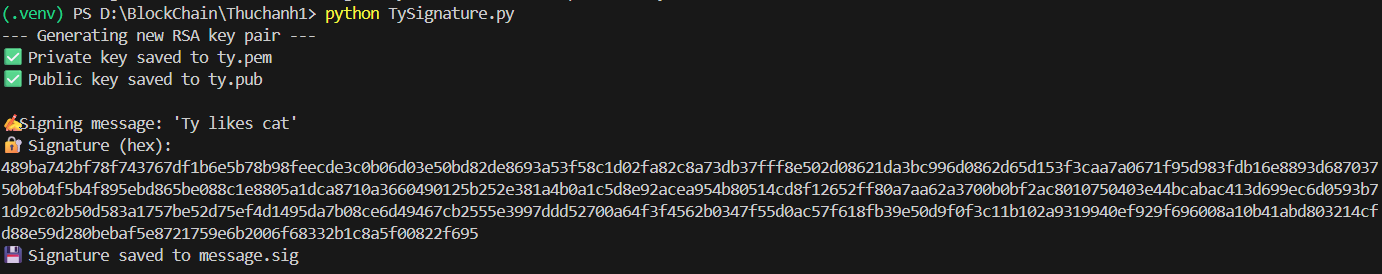
Kết quả:

A black screen with white text

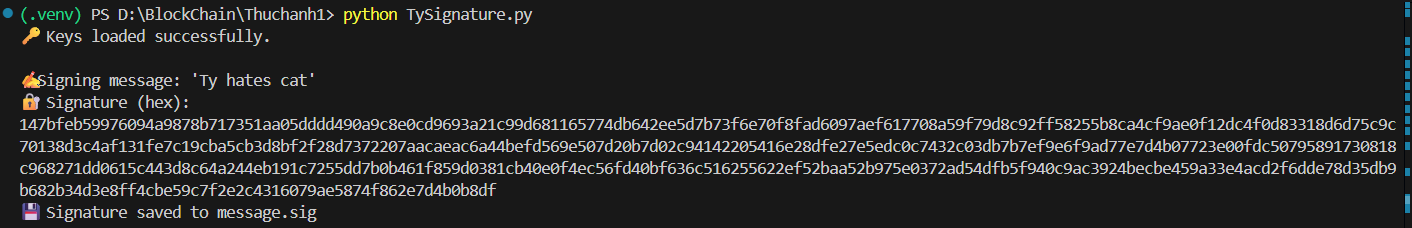
AI-generated content may be incorrect.

2. Bạn chạy TySignature.py, chụp lại kết quả dữ liệu được mã hoá dựa trên thông điệp “Ty likes cat”. Sau đó bạn thay thông điệp thành “Ty hates cat” rồi chạy lại chương trình đồng thời chụp kết quả và so sánh 2 giá trị này.

* Kết quả chạy thông điệp “Ty likes cat”



* Kết quả chạy thông điệp “Ty hates cat”



* Hai giá trị chữ ký số hoàn toàn khác nhau
* Nhận xét: hai giá trị chữ ký số thu được hoàn toàn khác nhau mặc dù chỉ thay đổi một từ trong thông điệp. Điều này chứng tỏ chữ ký số **phụ thuộc chặt chẽ vào nội dung thông điệp**. Chỉ cần một thay đổi nhỏ trong thông điệp cũng dẫn đến sự thay đổi hoàn toàn của chữ ký. Do đó, nếu có ai đó (như Tèo) cố gắng sửa đổi nội dung thông điệp, chữ ký số sẽ **không còn hợp lệ**, và thông điệp sẽ bị phát hiện là **đã bị thay đổi**.

3. \* Bạn viết 1 chương trình để xác thực xem có phải Tý là người đã viết “Ty likes cat” hay không?

- Code:

A screen shot of a computer program

AI-generated content may be incorrect.

* Kết quả

A black background with white text

AI-generated content may be incorrect.

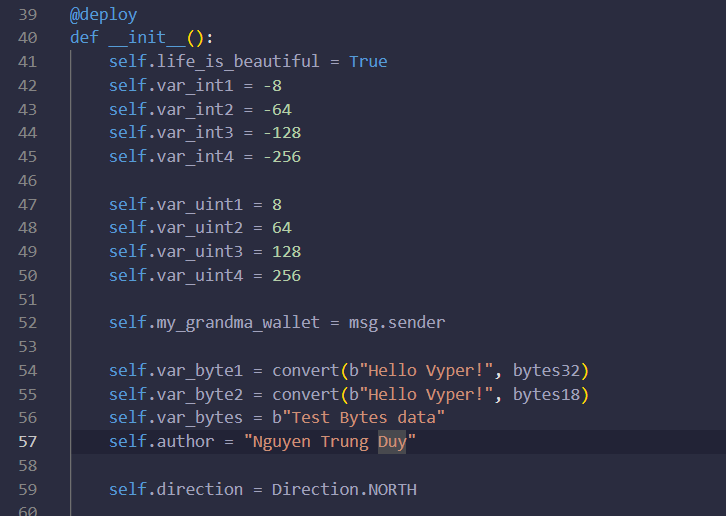
**E. Ngôn ngữ lập trình Vyper**

**i. Kiểu dữ liệu**

Viết một hợp đồng đặt tên DataType.vy để kiểm thử các kiểu dữ liệu như hình 13.

Sau đó bạn biên dịch và chụp kết quả để nộp báo cáo.

* Code:



* Kết quả biên dịch

A screenshot of a computer

AI-generated content may be incorrect.

**iii. Mutability**

* Kết quả biên dịch:

A screenshot of a computer

AI-generated content may be incorrect.

* Kết quả triển khai đoạn hợp đồng thông minh trên nên tảng Ethereum

A screenshot of a computer

AI-generated content may be incorrect.

* Sau khi triển khai lên nền tảng etherum, các hàm hoạt động đúng như mong đợi:
* Hàm add cộng chính xác hai số nguyên.
* Hàm get\_name\_and\_title trả về chuỗi tiêu đề + tên tác giả hiện tại.
* Hàm change\_name thay đổi tên tác giả thành giá trị mới.
* Hàm donate lưu tên người quyên góp và chấp nhận giá trị ETH gửi kèm.

A screenshot of a computer screen

AI-generated content may be incorrect.

**iv. Cấu trúc điều khiển**

Yêu cầu: Biên dịch, sau đó triển khai đoạn hợp đồng thông minh trên nên tảng Ethereum để xem kết quả như thế nào, và ghi nhận vào báo cáo?

* Kết quả biên dịch :

A screenshot of a computer

AI-generated content may be incorrect.

* Kết quả triển khai

A screenshot of a computer program

AI-generated content may be incorrect.

* Sau khi triển khai lên Ethereum, các hàm hoạt động đúng như logic điều khiển được lập trình:
* Hàm sum(): trả về 56.

A screenshot of a phone

AI-generated content may be incorrect.

* Hàm greet(time):
  + Kết quả: Trả về lời chào phù hợp với cấu trúc if/elif/else.
  + Hoạt động:
    - Nếu nhập "morning", trả về "Good morning!".

A screenshot of a computer

AI-generated content may be incorrect.

* + - Nếu nhập "evening", trả về "Good evening!".

A blue square with white text

AI-generated content may be incorrect.

* + - Nếu nhập chuỗi khác, trả về "How are you?". Ví dụ: nhập “hello”:

A screenshot of a computer

AI-generated content may be incorrect.

**v. Biến môi trường**

Yêu cầu: Biên dịch, sau đó triển khai đoạn hợp đồng thông minh trên nên tảng Ethereum để xem kết quả như thế nào, và ghi nhận vào báo cáo?

* Kết quả biên dịch

A screenshot of a computer program

AI-generated content may be incorrect.

* Kết quả triển khai

A screenshot of a computer

AI-generated content may be incorrect.

* **Kết luận:** Hợp đồng đã hoạt động đúng theo thiết kế, chứng minh khả năng truy cập và lưu trữ các biến môi trường quan trọng sau: **msg.sender** (người gửi), **msg.value** (giá trị ETH) và **block.timestamp** (thời gian block)

A screenshot of a computer

AI-generated content may be incorrect.

**vi. Event logging**

Yêu cầu: Biên dịch, sau đó triển khai đoạn hợp đồng thông minh trên nên tảng Ethereum để xem kết quả như thế nào, và ghi nhận vào báo cáo?

* Kết quả biên dịch

A screenshot of a computer

AI-generated content may be incorrect.

* Kết quả triển khai

A computer screen shot of white text

AI-generated content may be incorrect.

* Kết luận:

Hàm donate() đã thực hiện đúng chức năng của mình là phát ra một sự kiện Donation chứa thông tin chi tiết về người quyên góp (msg.sender) và số lượng tiền (msg.value).

A screenshot of a computer

AI-generated content may be incorrect.

**vii. Interface**

Yêu cầu: Biên dịch, sau đó triển khai đoạn hợp đồng thông minh trên nên tảng Ethereum để xem kết quả như thế nào, và ghi nhận vào báo cáo?

* Kết quả biên dịch

A screenshot of a computer

AI-generated content may be incorrect.

* Kết quả triển khai

A screenshot of a computer

AI-generated content may be incorrect.

* Kết luận:

Sau khi triển khai hợp đồng Storage.vy lưu trữ một giá trị số nguyên và triển khai hợp đồng StorageClient.vy với địa chỉ của Storage, việc gọi hàm call\_retrieve() từ StorageClient đã trả về chính xác giá trị mà hàm retrieve() trong Storage.vy lưu trữ.

* Hàm retrieve trong Storage.vy lưu “123”

A computer screen with white text and green text

AI-generated content may be incorrect.

* Khi call\_retrieve() trong StorageClient

A screenshot of a computer

AI-generated content may be incorrect.