**Crypto | CTF - 20TH01**

**Sinh viên: Nguyễn Thành Trung**

**\*\*\*\*\***

**War game trên WhiteHat**

**Tài khoản: TrungJea2019**

**---------------------------------------------------------------------------**

**01. Crypto01**

* **Nội dung:**

Lost in my mind

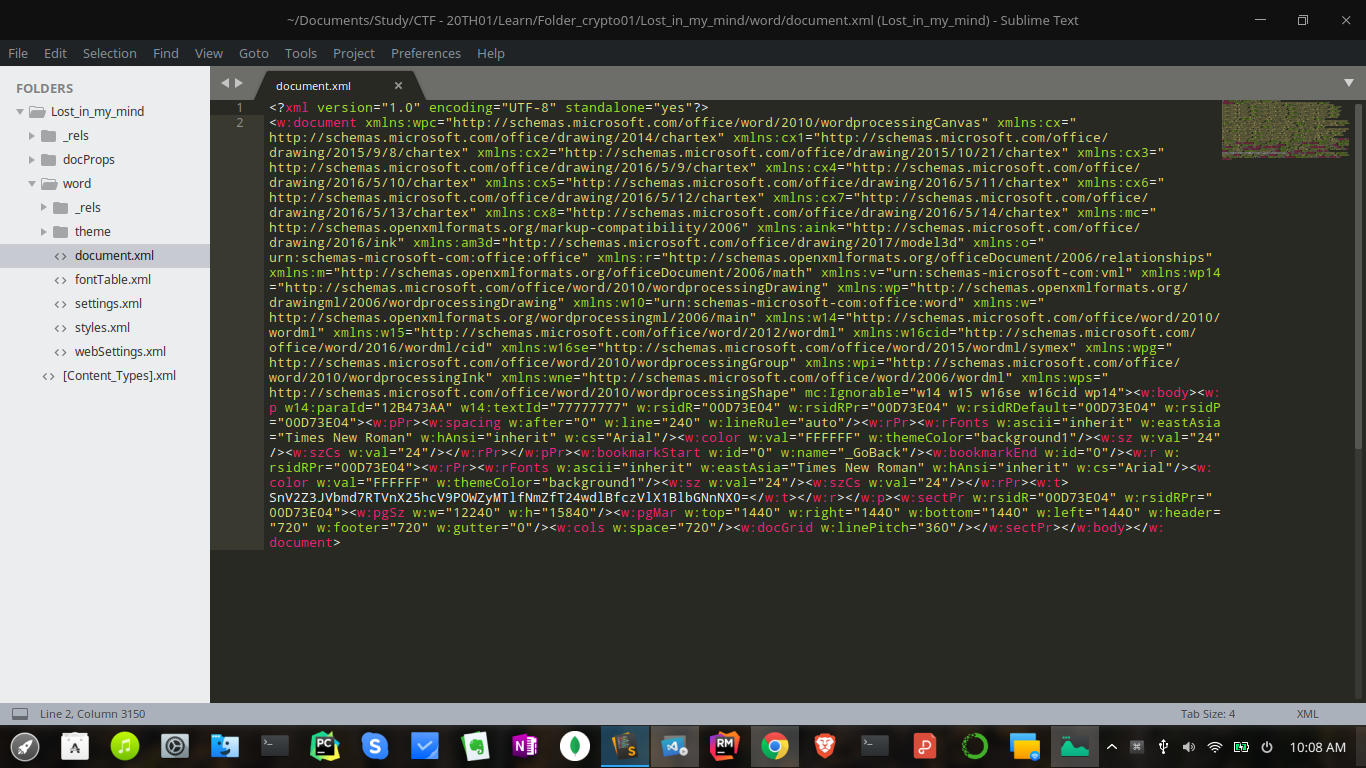
You can submit WhiteHat{flag}

https://drive.google.com/open?id=1lUDrGjKs8puanj6150A8HV-C-YhL9cJv

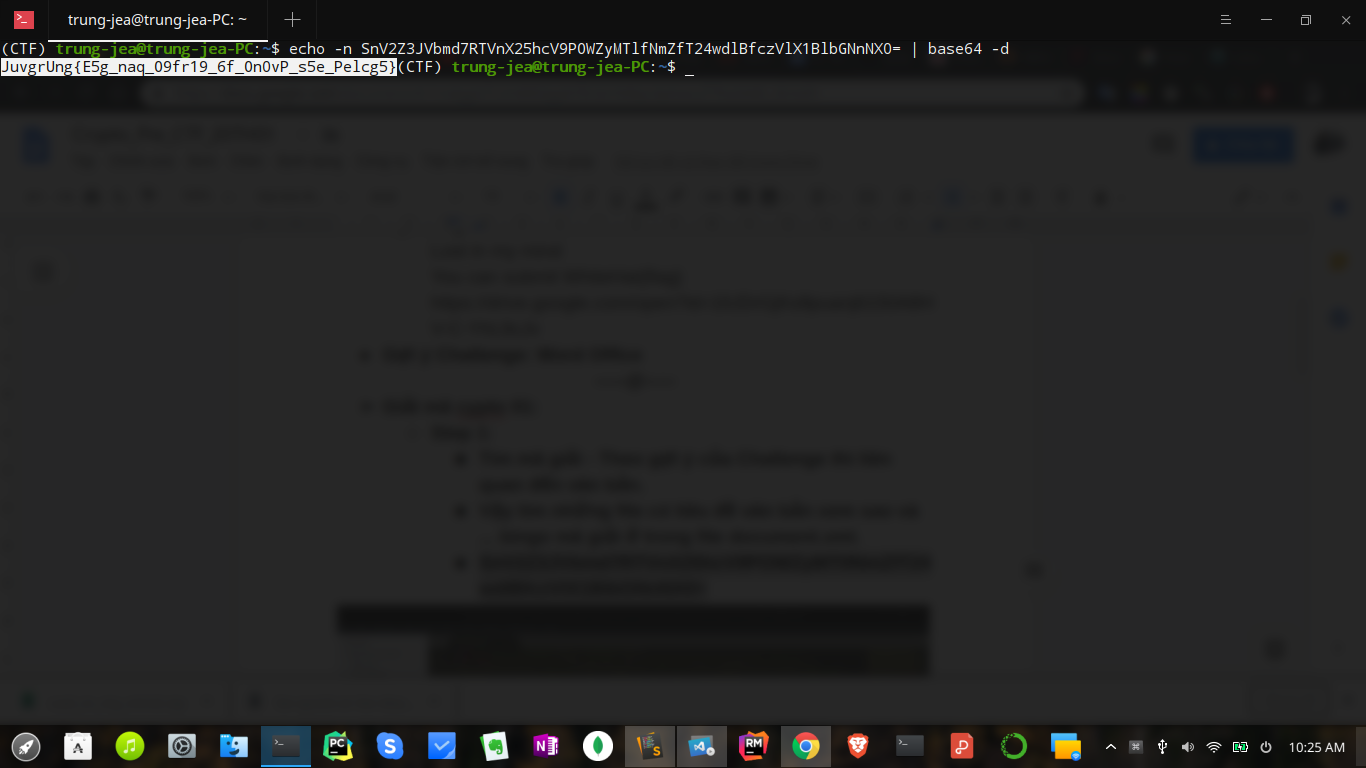
* **Gợi ý Challenge: Word Office**

**-----@-----**

* **Giải mã cypto 01:**
  + **Step 1 - Tìm mã giải:**
    - **Theo gợi ý của Challenge thì liên quan đến văn bản.**
    - **Vậy tìm những file có tiêu đề văn bản xem sao và ... bingo mã giải ở trong file document.xml.**
    - **SnV2Z3JVbmd7RTVnX25hcV9POWZyMTlfNmZfT24wdlBfczVlX1BlbGNnNX0=**

****

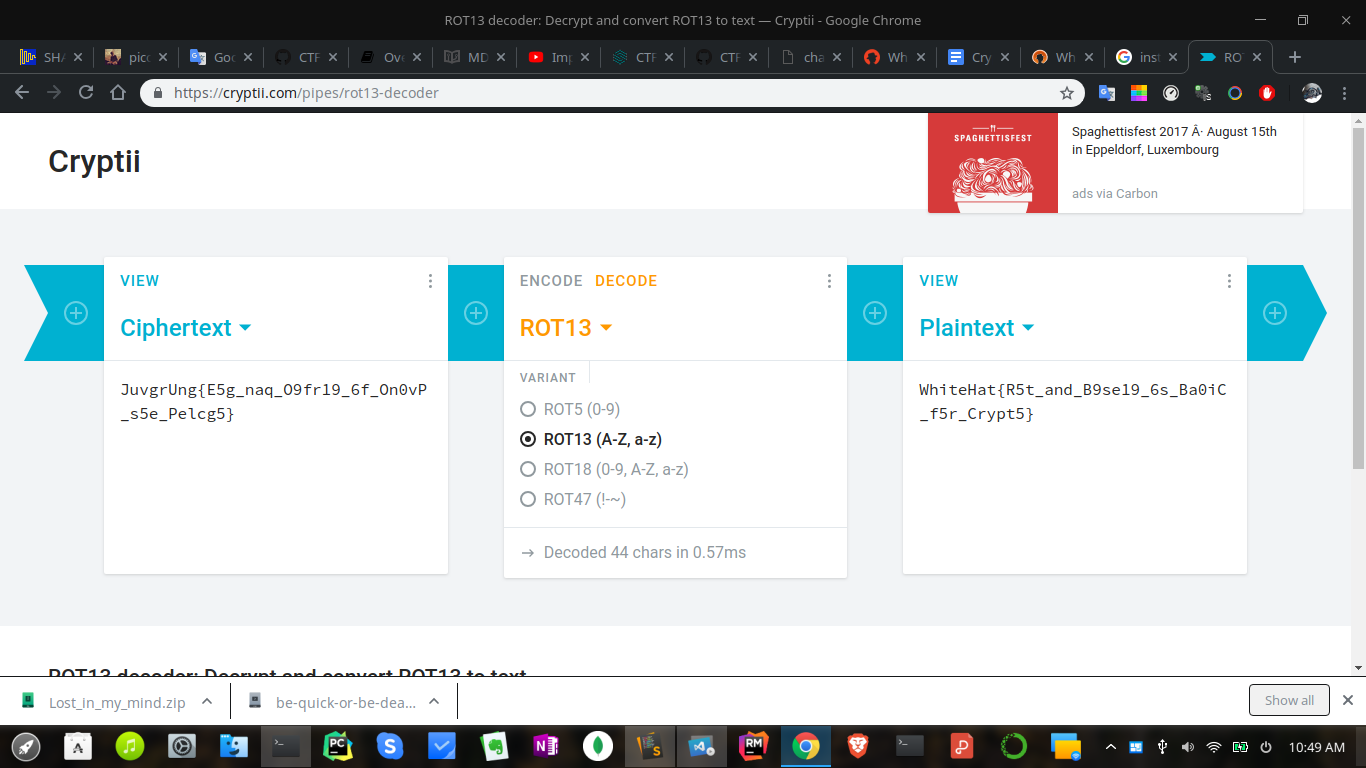
* + **Step 2 - Giải mã Base64:**
    - **Từ những thông tin tìm hiểu được thì đoạn mã trên được mã hoá theo kiểu Base64.**
    - **Vậy thì giải mã nó thôi...**
    - **Mình dùng Command Line để giải mã Base64:**
    - **Cú pháp: echo -n "Đoạn mã giải" | base64 -d**

****

**Kết quả: JuvgrUng{E5g\_naq\_O9fr19\_6f\_On0vP\_s5e\_Pelcg5}**

* + **Step 3 - Giải mã Caesar:**
    - **Từ kết quả trên, nếu ai có chút hiểu biết về mật mã sẽ nhận ra được nó được mã hoá theo kiểu mật mã dịch chuyển - Caesar.**
    - **Nguyên lý nó cơ bản:** 
      * **Dựa trên bản chữ cái Tiếng Anh - Alphabet, mỗi kí tự trong mã sẽ được dịch chuyển đến kí tự khác với khoảng các từ là xác định.**
    - **Xác định khoảng cách:**
      * **Dễ thấy WhiteHat -> JuvgrUng khoảng cách từ trong Alphabet là 13 kí tự - ROT13.**
      * **Vậy để giải mã mình sử dụng:**

[**https://cryptii.com/pipes/rot13-decoder**](https://cryptii.com/pipes/rot13-decoder)

****

**Kết quả: WhiteHat{R5t\_and\_B9se19\_6s\_Ba0iC\_f5r\_Crypt5}**

* + **Step 4 - Giải mã Number:**
    - **Thử submit kết quả trên thấy sai @@ What the ....?**
    - **Sau 1 hồi thì thấy kí tự đã được giải mã còn số thì chưa.**
    - **Thử tìm công cụ để giải mã nhưng chưa tìm thấy.**
    - **Đành phải làm thủ công tăng từng đơn vị cho tất cả các số theo vòng tròn số 0 1 2 3 4 5 6 7 8 9.**

****

* + - **Tăng xong được kết quả liền submit, sai 4 quả đầu tiên --> nản. Cứ nghĩ không xong rồi.**
    - **Và ... cuối cùng đến khi tăng lần 5 đơn vị, tức là:**
      * **5 -> 0 | 9 -> 4 | 1 -> 6 | 6 -> 1 | 0 -> 5**

**Kết quả: WhiteHat{R0t\_and\_B4se64\_1s\_Ba5iC\_f0r\_Crypt0}**

**--> Submit thành công. Yeah !!!**

**-------------------------------------------------------------------------------------------------**

**02. Crypto03**

* **Nội dung:**

Ezcrypto

Please help me solve this homework, my teacher said that it is component of a very popular cryptosystem.

You should submit WhiteHat{sha1(flag)}

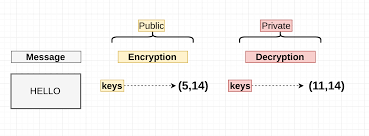
Download file here:

https://drive.google.com/open?id=1zNNxJ7K9ZkNDsHTej7bzj\_XtAU5oLdFI

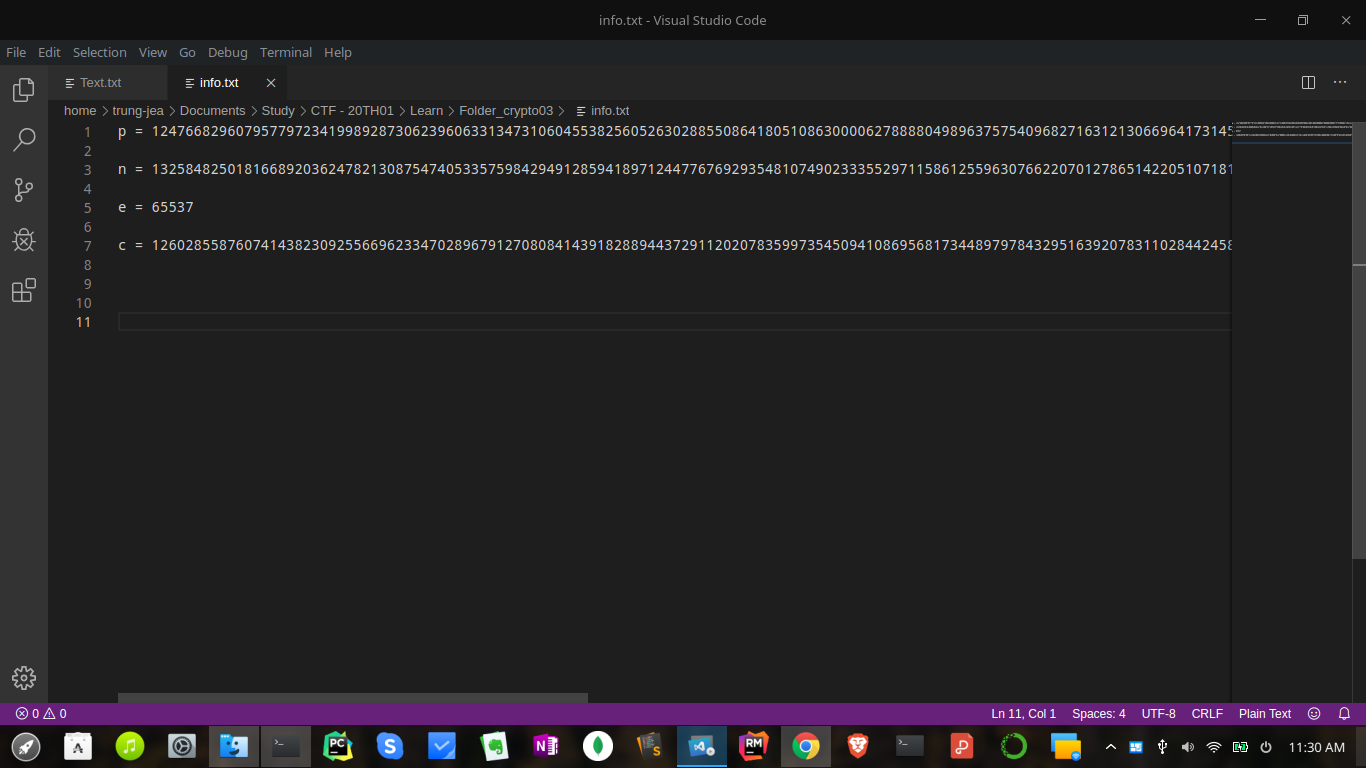
* **Gợi ý Challenge:** *Không có gợi ý nào*

**-----@-----**

* **Giải mã cypto 03:** 
  + **Step 1 - Tìm mã giải:**
    - **Bài này liên quan đến RSA. Đại loại là bạn muốn truyền dữ liệu an toàn thì RSA là hệ thống làm việc đó ^^.**

****

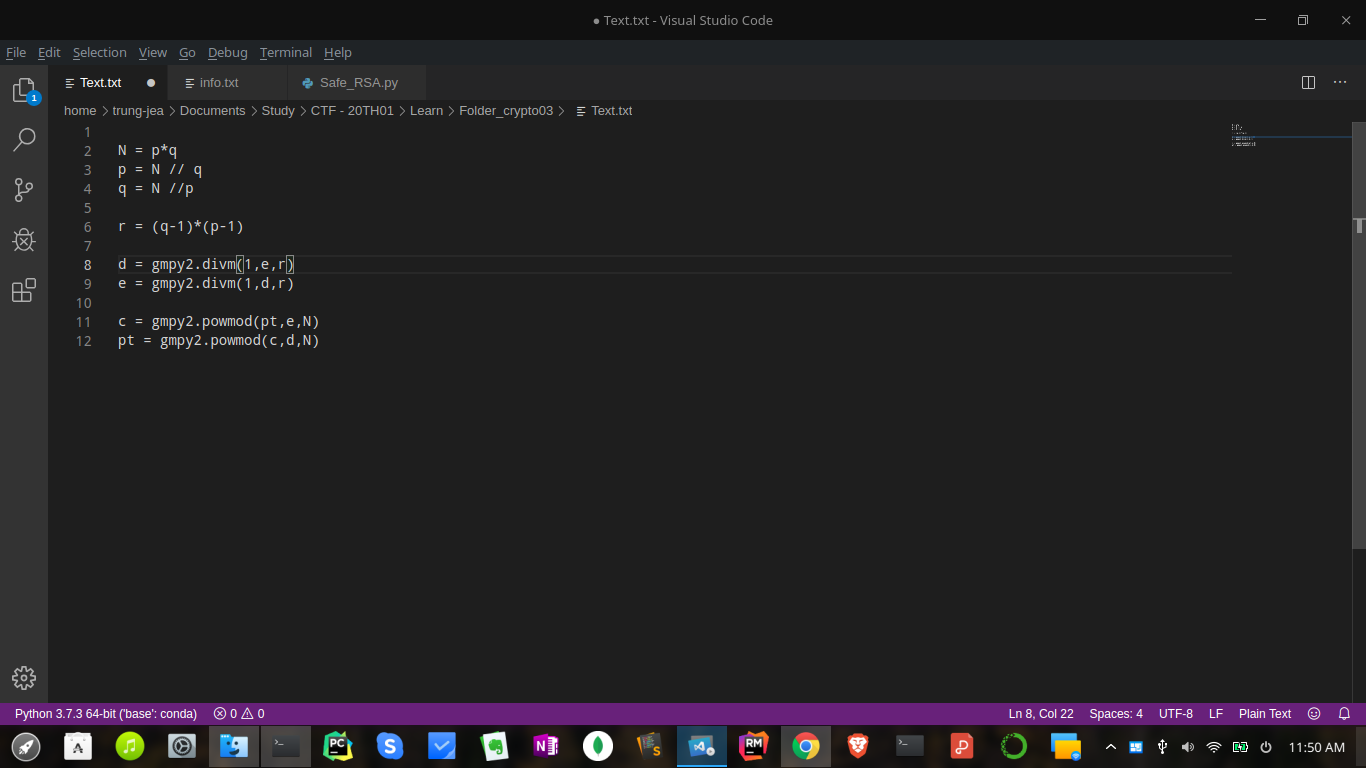
* + - **Đề bài cho ta các thông số như sau.**
    - **Tìm hiểu 1 chút thì ta sẽ thấy được các công thức tính toán các thông số này.**

****

* + **Step 2 - Tính toán RSA:**
    - **Các thành phần cần quan tâm trong khi tính toán RSA:**

|  |  |
| --- | --- |
| **p** | **n** |
| **q** | **d** |
| **e** | **r** |
| **c** | **pt** |

* + - **Tạm thời mình vẫn chưa hiểu biết nhiều về các thông số trên.**
    - **Nhưng mình cần các bạn quan tâm đến pt sẽ tính ra cho ra flag.**
    - **Trong bài này mình chỉ cần dùng công thức tính từng thành phần trên như sau:**

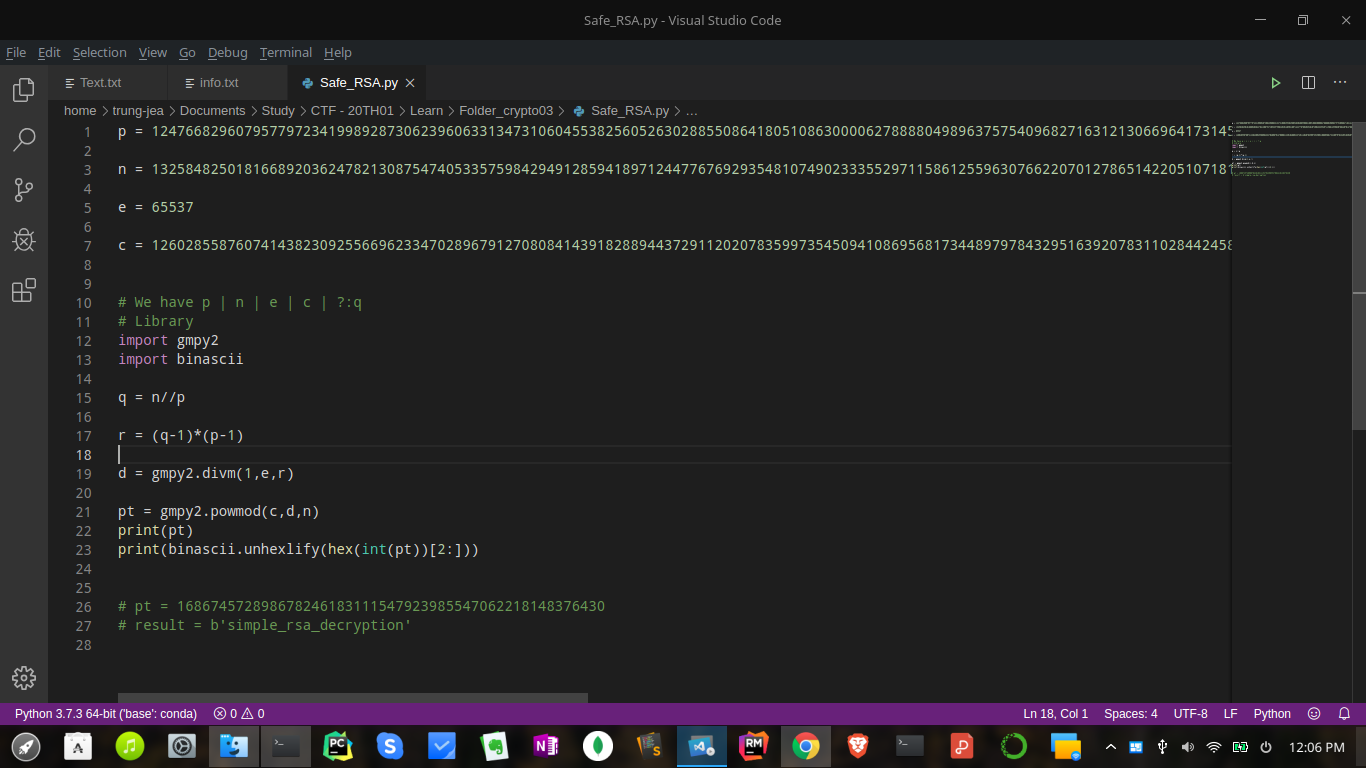
****

* + - **Dựa vào công thức tính toán các thành phần còn thiếu để tìm được pt.**

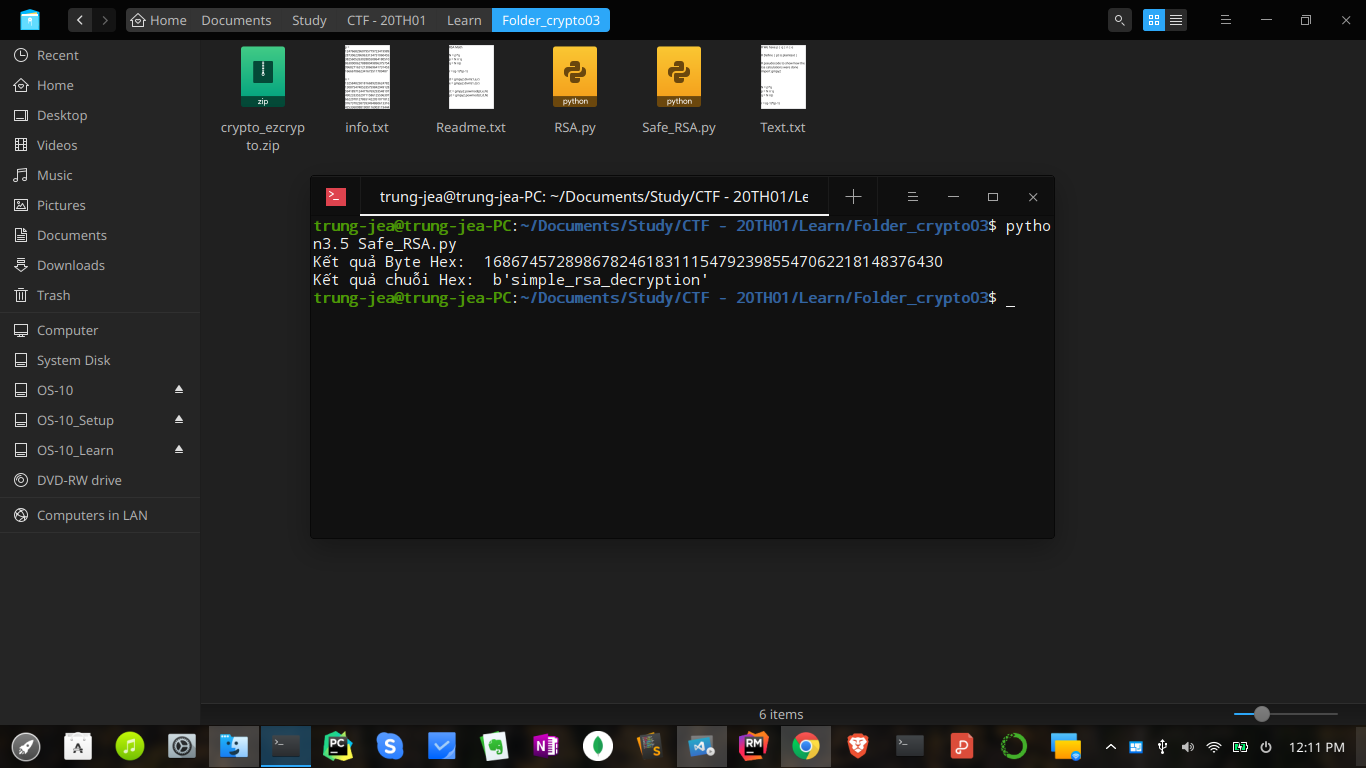
**Kết quả:**

**pt = 168674572898678246183111547923985547062218148376430**

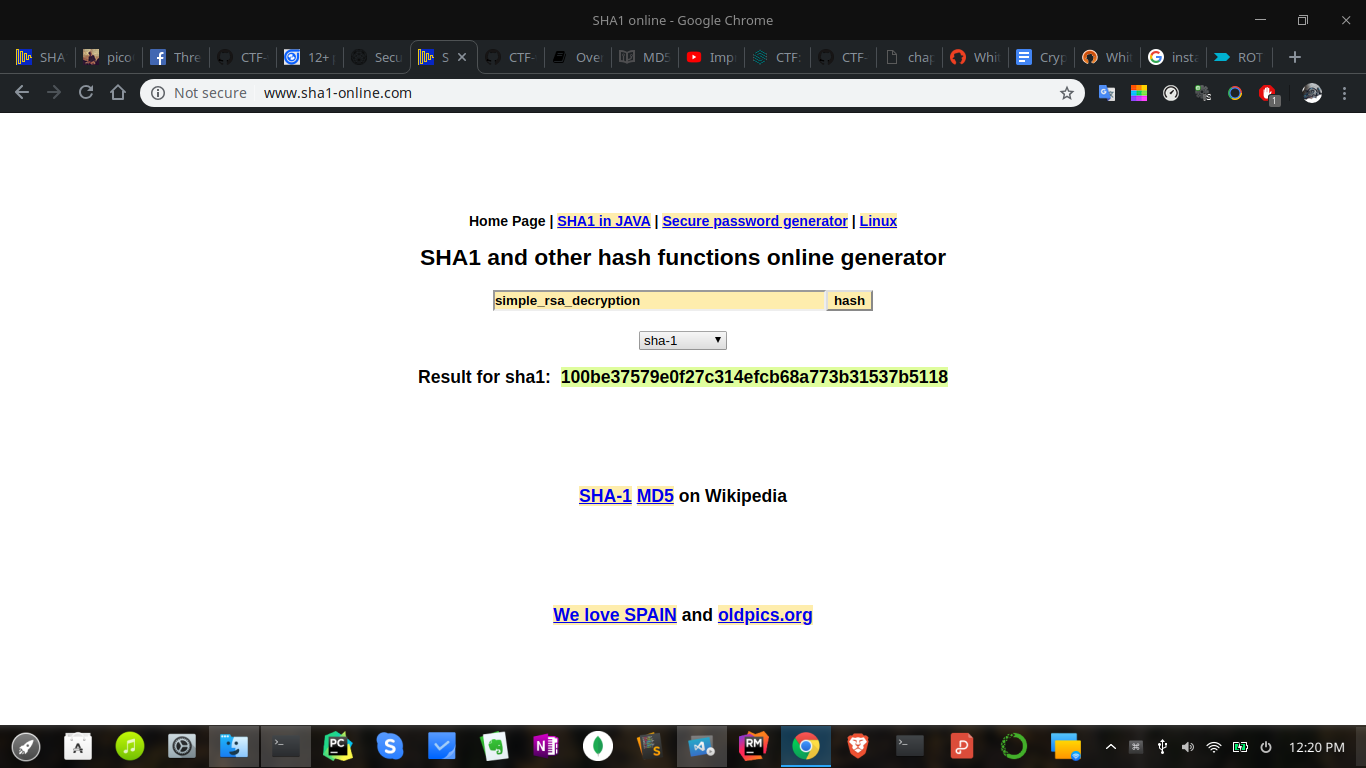
* + **Step 3 - Chuyển hệ Hex:**
    - **Kết quả trên cho ta giá trị chuỗi chứa byte hex.**
    - **Thế nên ta cần chuyển chuỗi chứa byte hex thành chuỗi Hex.**
    - **Mình dùng unhexlify trong thư viện binascii.**

****

**Kết quả: b'simple\_rsa\_decryption' (Đây là flag)**

****

* + **Step 3 - Mã hoá an toàn dữ liệu với sha-1:**
    - **SHA1 (Secure Hash Algorithm):** Là một chuỗi mã bao gồm 40 ký tự
    - **Mục đích mình làm bước này là đề bài yêu cầu submit theo kiểu** WhiteHat{sha1(flag)}.
    - **Tính Sha-1(simple\_rsa\_decryption)**

****

**Kết quả: 100be37579e0f27c314efcb68a773b31537b5118**

**Submit:** WhiteHat{100be37579e0f27c314efcb68a773b31537b5118} thành công

See ya!

tu bi con tì niu