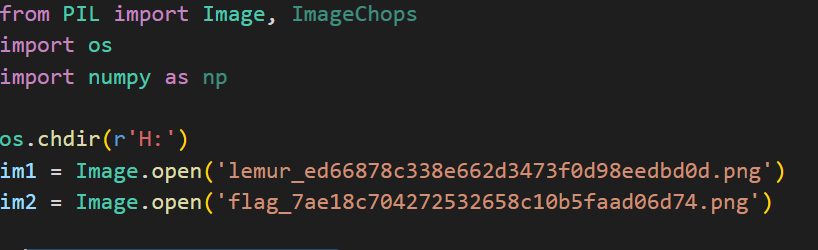
Họ và tên : Phùng Đức Dũng

Báo cáo Write-up Cryptography

Phần 1: Lemur Xor

Xor là 1 mã hoá phổ biến trong thường gặp. Ở dạng bài này người ra đề liên quan đến mã hoá xor với xử lí ảnh . Người ra đề đã gợi ý rằng “Đã giâú đi cùng 1 mật mã trong 2 bức ảnh và bạn sẽ phải xor 2 bức ảnh đấy để tìm ra câu trả lời”.Kết hợp hint 1 từ classroom anh đã cho: xor 2 image . Cùng với đó có 2 tệp đính kèm **lemur.png** và **flag.png**. Vậy chúng ta sẽ phải xử lí 2 ảnh này để tìm ra được đáp án

Mở 2 ảnh:

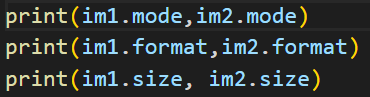


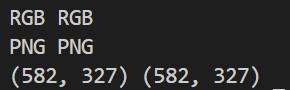
Để xử lí ảnh ta sẽ sử dụng thư viện Pillow của Python, ta tìm hiểu được 1 số vấn đề như sau:

+ 2 hình ảnh có độ dài rộng là (582,327) pixel

+ sử dụng mode hình ảnh RGB

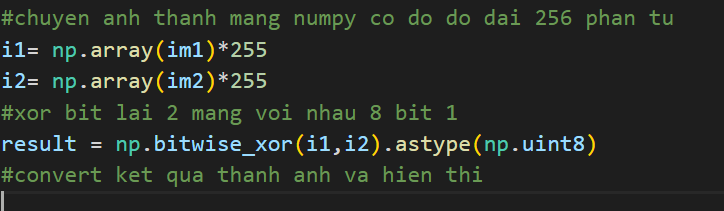
+ format ảnh là png



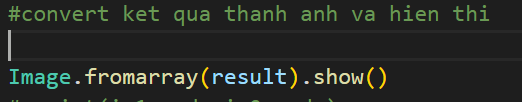


Do có cùng kích thước ảnh ,nên có thể chuyển kích thước ảnh sang mảng numpy kiểu dữ liệu bit để dễ xor với nhau, sử dụng thư viên numpy có cùng kiểu dữ liệu trong 1 mảng có độ dài 256 phần tử

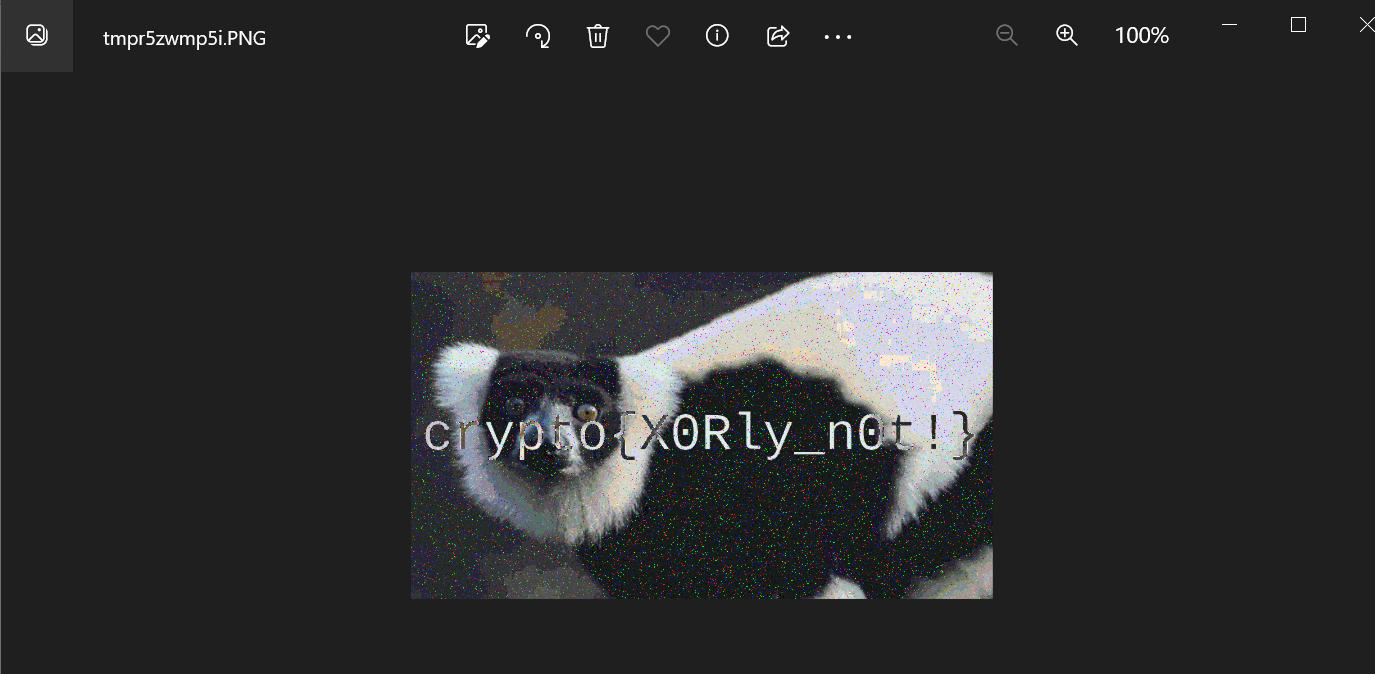
Sau đó sử dụng hàm bitwise\_xor của thư viện numpy với 2 mảng cùng độ dài ,8 bit lần lượt



Sau khi xor thì convert lại thành ảnh rồi hiển thị kết quả sử dụng thư viện PIL

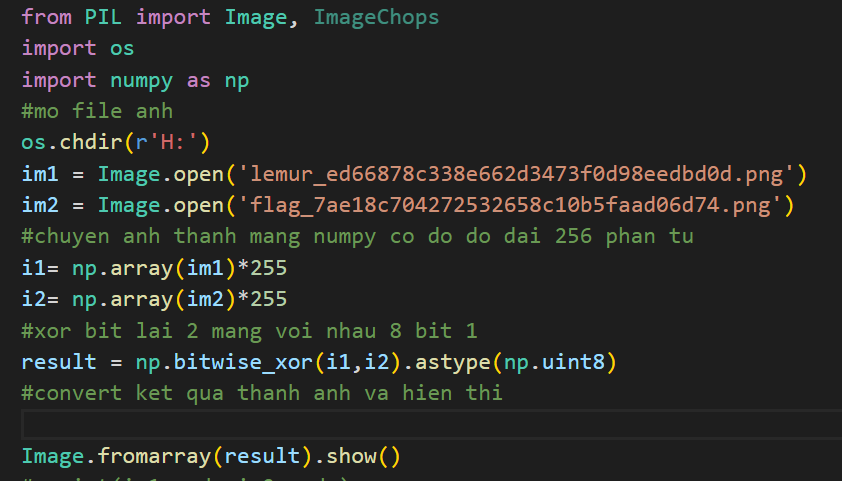


Kết quả:



Đáp án đưa ra : 

Code hoàn chỉnh:

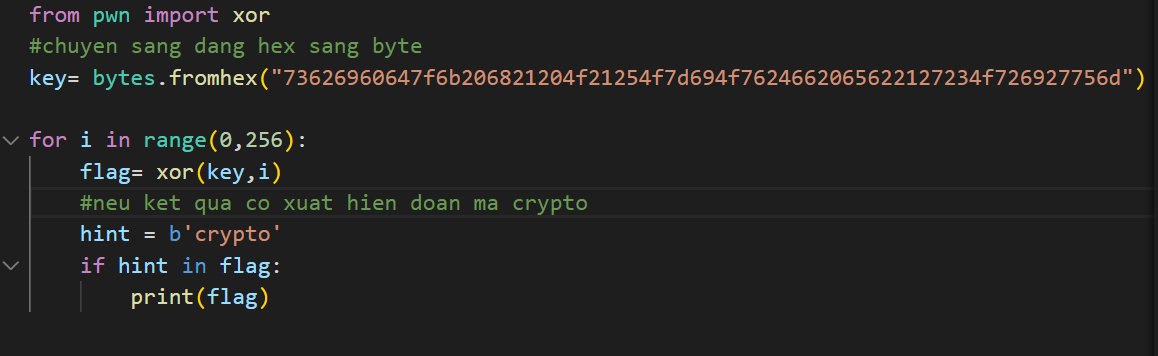


Bài 2: favourite byte

Đề bài cryptohack cho rằng đã xor với 1 vài byte, nhưng không nói rõ là dùng byte nào. Và lưu ý người chơi phải decode sang hex trước

Gợi ý tiếp theo từ anh đưa ra là for loop và tiền tố crypto

Như vậy là đầu tiên ta phải đổi key về dạng hex sang byte. Sau đó sẽ xor từng byte 1, 1 byte =8 bit thì cho chạy vòng lặp là 2^8=256 trường hợp ( vì có thể là byte 0 ,byte 10, byte 25,…). Nếu xuất hiện hint của đáp án chữ cái đầu tiên là crypto thì chắc chắn đó là kết quả. Ta đã sử dụng hết gợi ý từ bài toán đưa ra



Đáp án đưa ra :



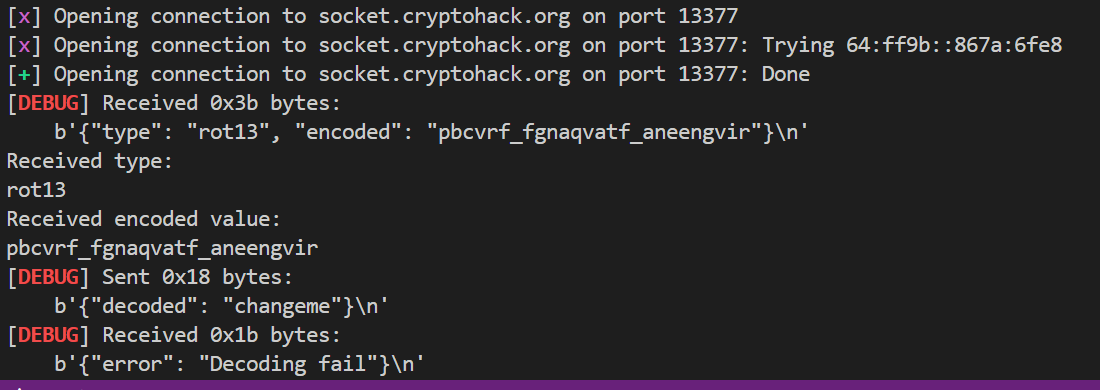
Bài 3 : encoding challenge

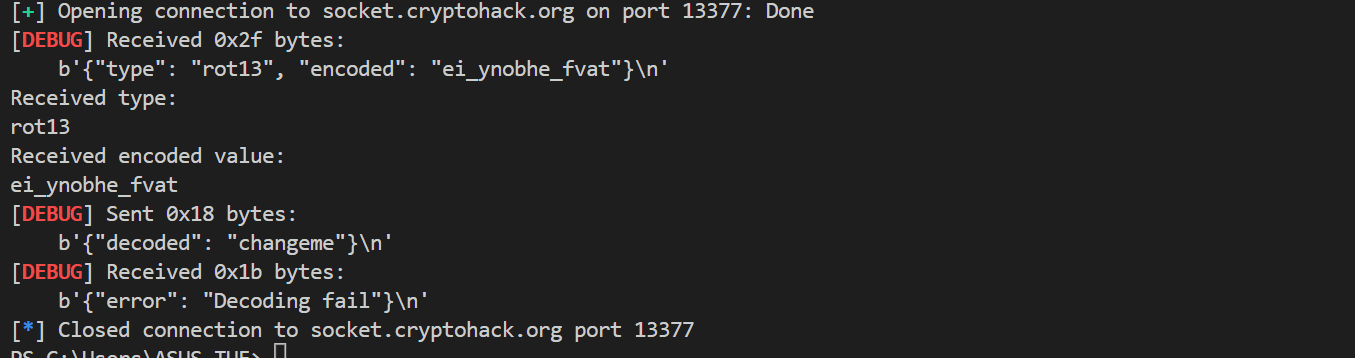
Ý tưởng bài này là tổng hợp các kiến thức về encoding code bằng nhiều cách khác nhau

Quá trình trao đổi dữ liệu bằng hình thức request response dựa trên mô hình client-server

Ta có thể hình dung là nhận encode từ server CrytoHack, sau đó client decode đoạn mã vừa nhận được và hiển thị kết quả

Mỗi khi nhận đoạn mã từ server trong file pwntools\_example.py thì :



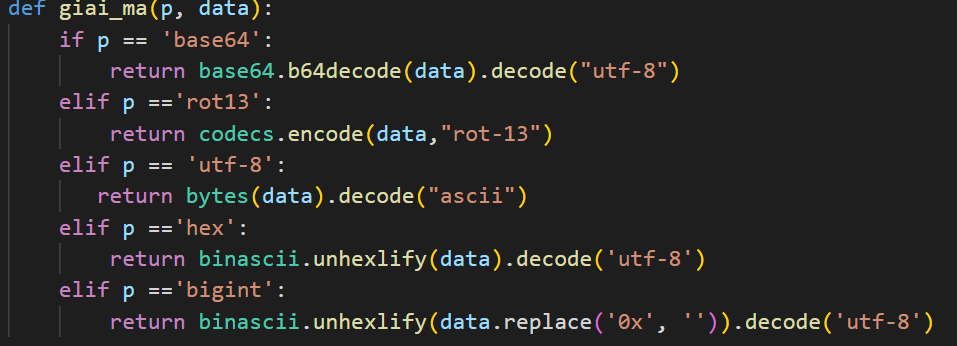


Tuy nhiên mỗi lần nhận kết quả thì sẽ khác nhau và kiểu dữ liệu mã hoá cũng sẽ khác nhau (rot13, bigint, base64, hex,..). Sử dụng Hint1 từ anh đã cho là

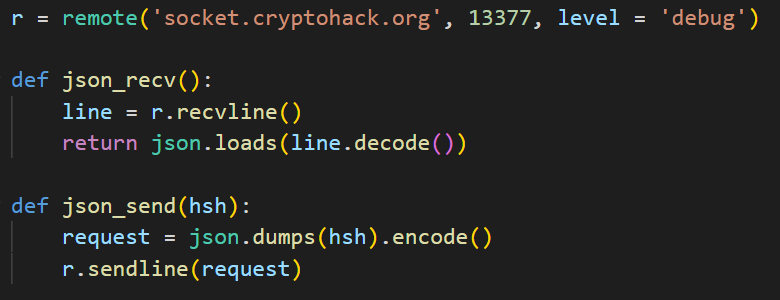


Thì ta phải xử lí hết trường hợp khi receive đoạn encoded từ server và decode sang utf-08

Em viết hàm giai\_ma() để xử lí từng trường hợp :

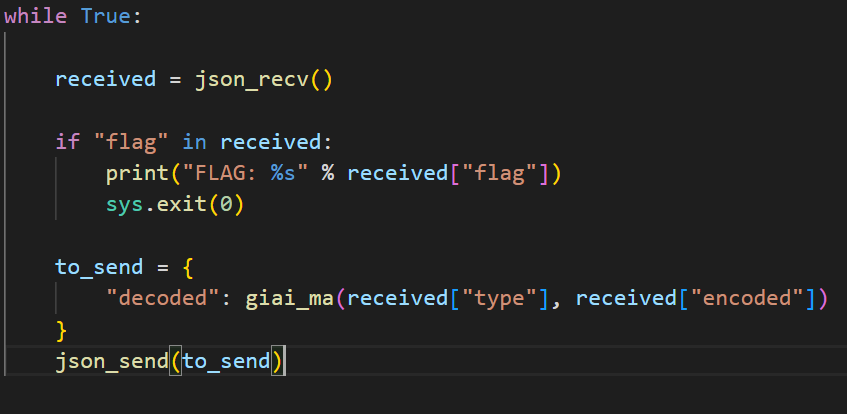


Đoạn code này thể hiện quá trình request respone của 2 máy với nhau

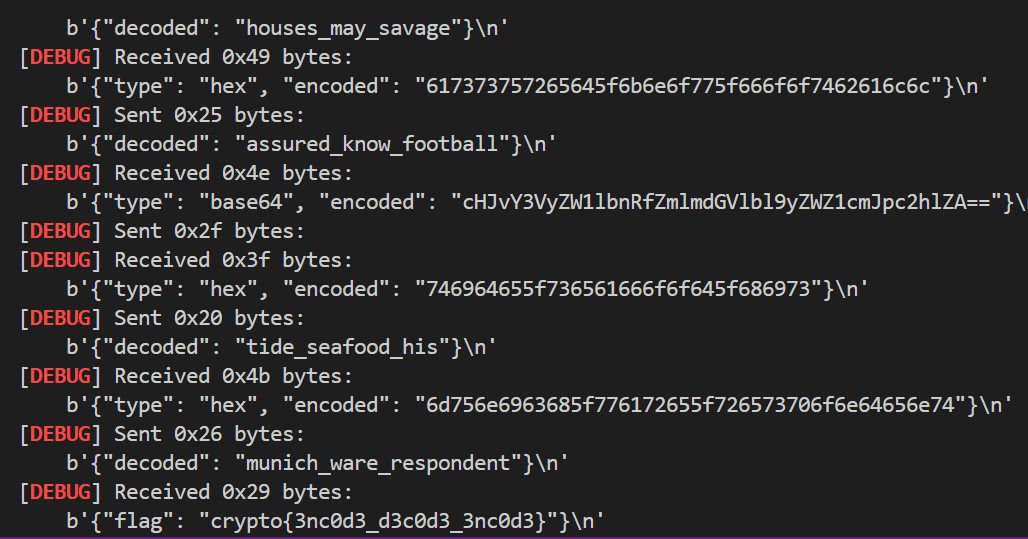


Sau đó ta tiến hành trao đổi dữ liệu liên tục giữa 2 máy chủ trong 1 vòng lặp

Nếu kết quả decoded có xuất hiện “flag” trong đáp án , đó là kết quả cuối cùng của ta và kết thúc vòng lặp, kết thúc phiên làm việc



Kết quả cuối cùng sau 1 lúc đợi thì cho ra như sau:



Đáp án cần tìm:

