**Giải thích phần Introduction To CryptoHack**

1. Finding Flags: Giới thiệu cách giải của phần Introduction To CryptoHack

- B1: Giải thử thách bằng cách tìm “flag”.

- B2: Điền câu trả lời bằng định dạng: CRYPTO{flag}

Trong đó “flag” là kết quả cần tìm được.

2. Great Snakes: Chạy file python great\_snakes.py và điền kết quả

3. ASCII: Đổi ord sang char để chuỗi từ dạng mã ascii sang chữ.

4.Hex: Sử dụng bytes.fromhex() để chuyển đổi chuỗi từ dạng hex sang dạng bytes.

5. Base64: Bài toán sử dụng base64 để mã hóa key và hàm base64encode của python chỉ dùng đầu vào là đối tượng kiểu bytes và trả về đầu ra là bytes đã được mã hóa. Do đó, từ đầu vào của bài toán là chuỗi giá trị hex, ta sử dụng bytes.fromhex() để chuyển chuỗi từ dạng hẽ sang dạng bytes, sau đó sử dụng hàm base64encode để mã hóa chuỗi bytes để tìm ra kết quả

6. Bytes and Big Integers: Giải thuật của bài toán chuyển một chuỗi sang một chuỗi số hệ thập phân như sau:

Kí tự (một chữ trong chuỗi) => kí mã ascii => kí tự hệ 16 => kí tự hệ thập phân.

Từ đó, từ đầu vào chuỗi thập phân, dùng bytes\_to\_long() để chuyển chuỗi hệ thập phân sang dạng chuỗi bytes và điền kết quả.

7. XOR Starter: Sử dụng hàm xor() để tính toán của 2 tham số đầu vào để tính ra đầu ra dạng bytes. Vì vậy phải chuyển chuỗi kí tự thành dạng chuỗi bytes rồi dùng hàm xor() tính ra kết quả.

8. XOR Properties: Bài toán cho thông tin về 4 thuộc tính chính khi dùng dấu XOR bao gồm tính giai hoán, kết hợp, đồng nhất và tự nghịch đảo. Do đó, tự đầu vào của bài toán ta sử dụng thuộc tính kết hợp để tính lần lượt KEY2, KEY3 và cuối cùng là FLAG.

9. Favorite byte: vì bài toán có thông tin về việc mã hóa flag sử dụng 1 byte. Và 1 byte có 8 bits, do đó 1 byte có giá trị từ [0, 255]. Do đó, dùng hàm xor() với 2 tham số đầu vào là chuỗi thập lục phân và từng giá trị một của [0, 255] để tìm chuỗi kí tự phù hợp nhất.

10. You either know, XOR you don't: Bài toán có gợi ý về cấu trúc của flag: CRYPTO{flag}và bài toán đã mã hóa xor với key bí mật. Sử dụng thuộc tính kết hợp của XOR để tìm ra key bí mật bằng cách dùng hàm xor() với số lượng từ nhất định để phù hợp với cấu trúc của flag. Sau khi tìm ra key bí mật thì tiếp tục dùng hàm xor() với chuỗi bytes đã được chuyển đổi từ đầu vào với key bí mật để tìm ra kết quả cuối cùng.