Báo cáo demo **cryptography**

**Crypto01:**

\*Các loại mã sử dụng trong bài:

-Base 64

-ROT – 13

Quy trình làm:

Tải file về và mở file document.xml ta sẽ thu được đoạn mã như sau:

**SnV2Z3JVbmd7RTVnX25hcV9POWZyMTlfNmZfT24wdlBfczVlX1BlbGNnNX0=**

-Nhận thấy kiểu mã có nhiều chữ in cộng với **có ký tự đệm là dấu bằng** suy ra đây là kiểu mã Base-64

Sau khi giải mã ta sẽ thu được :

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

Ta thấy có dạng WhiteHat{flag}

W – J cách nhau 13 ký tự trong bảng chữ cái tiếng anh

h – u cách nhanh 13 ký từ trong bảng chữ cái tiếng anh

có thể đây là dạng mã ROT-13 thử giải mã ROT-13 ta thu được

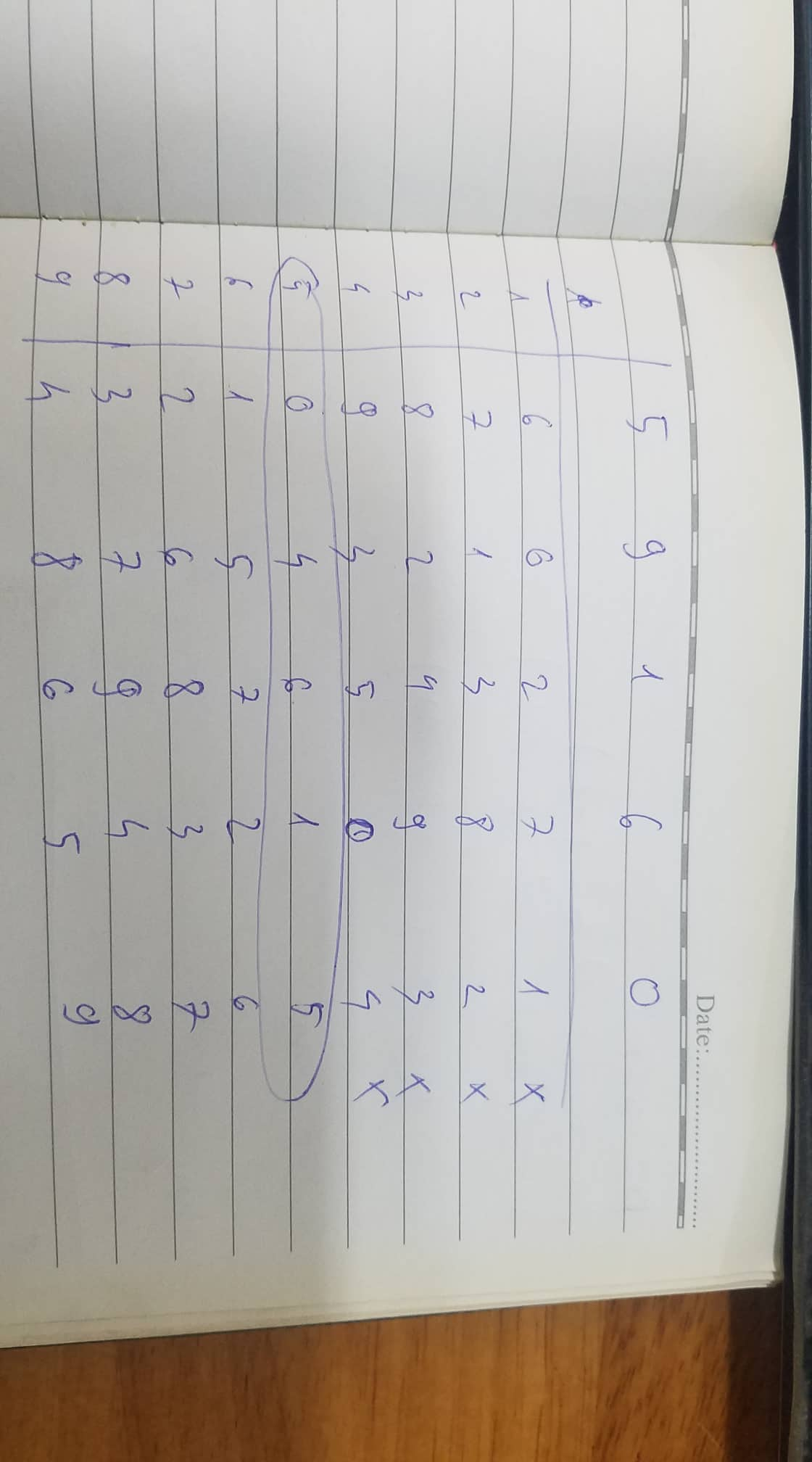
**WhiteHat{R5t\_and\_B9se19\_6s\_Ba0iC\_f5r\_Crypt5}**

Đã ra dạng yêu cầu thử submit thì vẫn chưa được đáp án

Vẫn đề ROT-13 khong dịch mã hóa số lên trắc chắn phần ký tự là đúng còn liên quan đến phần số trong đoạn ký tự

Các chữ số trong đoạn có 5 – 9 – 1 – 6 – 0

Thử tăng lần lượt các số và thử submit ta sẽ thu được kết quả



Thử tăng đến 5 ta có được kết quả cần submit đúng

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

**Crypto03**

\*các loại mã sử dụng:

- RSA

- INT

Sau khi tải file về ta sẽ thấy một file .txt chứ:

* P – số nguyên tố
* N – Modun
* E – Số mũ công khai
* C – Văn bản mã hóa

Vấn đề chính bây giờ để giải ra được văn bản gốc ta có một công thức như sau Cd mod n tất cả các thông số đã đủ chỉ còn thiếu d(Số mũ bí mật)

Tìm d:

Để tìm được D ta phải sử dụng cách nghịc đảo modun nhân thì trong python có thư viện gmpy2

Cú pháp

q = n//p

r=(q-1)\*(p-1)

d=gmpy2.divm(1,e,r)

ta sẽ tìm được d sau khi thực hiện các dòng lệnh này

bây giờ ta chỉ cần sử dụng công thức giả là ra:

ta dùng **pow** trong python

kq = pow(c,d,n)

print(kq)

sau khi chạy tất cả ta sẽ thu được:

**168674572898678246183111547923985547062218148376430**

Chuyển từ mã INT sang ASCII

**simple\_rsa\_decryption**

trong bai gi có dạng SHA thi ta chuyển tiếp sang SHA1

**100be37579e0f27c314efcb68a773b31537b5118 đây là kết**

submid