



Thứ Năm, 9 tháng 2, 2017

[Alex CTF 2017][Writeup][CR3: What is this encryption?]

# [Alex CTF 2017][Writeup][CR3: What is this encryption?]

*Sloved this problem when contest ended*

Hint

*Fady assumed this time that you will be so noob to tell what encryption he is using  
he send the following note to his friend in plain sight :*  
*p=oxa6055ec186de51800ddd6fcbf0192384ff42d707a55f57af4fcfb0d1dc7bd97055e8275cd4b78ec63c5d592f567c66  
393a061324aa2e6a8d8fc2a910cbee1ed9  
q=oxfa0f9463ea0a93b929c099320d31c277e0b0dbc65b189ed76124f5a1218f5d91fd0102a4c8de11f28be5e4d0ae91  
ab319f4537e97ed74bc663e972a4a9119307  
e=ox6d1fdab4ce3217b3fc32c9ed480a31d067fd57d93a9ab52b472dc393ab7852fbc11abbebfd6aaae8032db1316dc  
22d3f7c3d631e24df13ef23d3b381a1c3e04abcc745d402ee3a031ac2718fae63b240837b4f657f29ca4702da9af22a3  
a019d68904a969ddb01bfc941df70af042f4fae5cbeb9c2151b324f387e525094c41  
c=ox7fe1a4f743675d1987d25d3811fae0f78bbea6852cba5bada47db76d119a3efe24cb04b9449f53becd43b0b46e2  
69826a983f832abb53b7a7e24a43ad15378344ed5c20f51e268186d24c76050c1e73647523bd5f91d9b6ad3e86bbf91  
26588b1dee21e6997372e36c3e74284734748891829665086e0dc523ed23c386bb520*

During contest I know this is **RSA** but I didn't know How to slove it!!! :sad:  
After contest I read about **RSA** and sloved it :cry:

I got **p q e** and **c**  
**c** : Cypher text need decrypt  
**e** : public key in **RSA**  
so I need **d** is a private key to decrypt **c**  
I find **d** step by step below

- 1.  $n = p * q$
- 2.  $\phi(n) = (p - 1) * (q - 1)$
- 3. using Extended Euclid to find **d**
- 4. plain text =  $c^d \% n$

Here is my **python** code

```
p=0xa6055ec186de51800ddd6fcbf0192384ff42d707a55f57af4fcfb0d1dc7bd97055e8275cd4b78ec63c5d592f567c66393a061324aa2e6a8d8fc2a910cbee1ed9
q=0xfa0f9463ea0a93b929c099320d31c277e0b0dbc65b189ed76124f5a1218f5d91fd0102a4c8de11f28be5e4d0ae91ab319f4537e97ed74bc663e972a4a9119307
e=0x6d1fdab4ce3217b3fc32c9ed480a31d067fd57d93a9ab52b472dc393ab7852fbc11abbebfd6aaae8032db1316dcd22d3f7c3d631e24df13ef23d3b381a1c3e04abcc745d402ee3a031ac2718fae63b240837b4f657f29ca4702da9af22a3a019d68904a969ddb01bfc941df70af042f4fae5cbeb9c2151b324f387e525094c41
c=0x7fe1a4f743675d1987d25d3811fae0f78bbea6852cba5bada47db76d119a3efe24cb04b9449f53becd43b0b46e269826a983f832abb53b7a7e24a43ad15378344ed5c20f51e268186d24c76050c1e73647523bd5f91d9b6ad3e86bbf9126588b1dee21e6997372e36c3e74284734748891829665086e0dc523ed23c386bb520

phi = (p - 1) * (q - 1)
y0=0
y1=1
d = 0

#Extened Euclid
while phi > 0:
```

Giới thiệu bản thân

aides le

G+ Theo dõi

Xem hồ ` sơ hoàn c  
tôi

Lưu trữ Blog

2017 (8)

tháng hai (6)

▼ [Alex CTF 2017][W  
[CR3: What is thi

[AlexCTF 2017][Writeup][  
me]

[AlexCTF 2017][Writeup][  
bot]

[AlexCTF 2017][Writeup][  
is awesomed]

[AlexCTF 2017][Writeup][  
Gifted]

[AlexCTF 2017][Writeup][  
Ultracoded]

tháng một (2)


► 2016 (1)

►

```
if (r == 0):  
    break  
t = phi // e  
y = y0 - y1 * t  
phi = e  
e = r  
y0 = y1  
y1 = y  
if (e > 1):  
    print("cannot find d")  
else:  
    d = y  
n = p * q  
plain = pow(c, d, n)  
print str(hex(plain))[2:-1].decode("hex")
```

Flag is ALEXCTF{RS4\_I5\_E55ENT1AL\_T0\_D0\_BY\_H4ND}

Được đăng bởi [aides le](#) vào lúc 05:01

 Đề xuất url này trên Google

Nhãn: [AlexCTF 2017](#), [Cryptography](#)

Không có nhận xét nào:

Đăng nhận xét

Nhận xét với tên: 

Unknown (Google) ▼

Đăng xuất

Xuất bản

Xem trước

☐ Thông báo cho tôi

[Trang chủ](#)

[Bài đăng Cũ hơn](#)

Đăng ký: [Đăng Nhận xét \(Atom\)](#)

Chủ đề Đơn giản. Được tạo bởi [Blogger](#).