




MAY 10, 2017 / CTF

## ENC BRAINHACK WRITEUP

# Enc – Crypto 100pts

---

 Break my encryptionEnc.txt

Berikut isi filenya

$e = 3$

$n = 189137687020123159261852192605885322671854225839439913905089$

$c = 116349429993499036729985853392736442671966425740999199390529$

Ini adalah challenge tentang RSA. RSA adalah salah satu metode penyandian dengan memanfaatkan public dan private key. Seperti namanya, public key adalah suatu kunci yang bersifat publik (semua orang dapat tahu) dan private key hanya yang memiliki yang tahu. Data yang dienkripsi dengan public key milik A, hanya bisa di dekripsi dengan private key A. Jadi konsepnya adalah, ketika akan mengirimkan data, kita harus meminta public key si penerima, lalu mengenkripsi datanya, kemudian mengirimkan data terenkripsi tersebut kepada penerima. Bingung? Mari kita analogikan.

Misalnya ada 2 orang bernama Alvin dan Feby. Alvin ingin mengirimkan surat cinta ke Feby dan ingin memastikan hanya Feby yang bisa membacanya. Oleh karena itu, Alvin mengirimkan surat tersebut dengan memasukkannya kedalam kotak peti kecil. Kemudian Feby membeli sebuah gembok, dan mengirimkan gembok tersebut kepada Alvin. Lalu kotak tersebut di gembok dengan gembok milik Feby. Karena hanya Feby

yang memiliki kunci gemboknya, maka bisa dipastikan yang dapat membuka gemboknya adalah Feby.

Dari analogi tersebut, data yang akan dikirim bisa diumpamakan sebagai surat cinta, gembok diumpamakan sebagai public key, dan kunci gemboknya adalah private key

Oke lalu bagaimana penerapannya dalam RSA? Click this great [explanation](#). Kita langsung saja ke challenge nya ya, hehe

- Cari nilai p dan q pake [ini](#)
- $p = 362736035870515331128527330659$  ;  $q = 521419622856657689423872613771$
- $t = (p-1) * (q-1)$   
 $= 189137687020123159261852192605001167013127052818887513960660$
- $e = 3$

```
import gmpy
from Crypto.PublicKey import RSA

n = 189137687020123159261852192605885322671854225839439913905089
c = 116349429993499036729985853392736442671966425740999199390529
e = long(3)
p = 521419622856657689423872613771
q = 362736035870515331128527330659

d = long(gmpy.invert(e, (p-1)*(q-1)))
key = RSA.construct((n,e,d))

print key.decrypt(c)
print hex(key.decrypt(c))
print hex(key.decrypt(c))[2:-1].decode('hex')
```

**FLAG: noob{cool3r\_th4n\_RSA}**

## PREVIOUS POST

BRAINHACK CTF WRITEUP 1.0

## NEXT POST

QUADRATHLON 2017 WRITEUP – PART 2

## CATEGORIES

CTF

**BE FIRST TO COMMENT**

## Leave a Reply

Your email address will not be published. Required fields are marked \*

Enter Your Comment...

Your Name\*

Your Email\*

Your URL

Post Comment

# CLAYDAY BLOG

## ARCHIVES

JUNE 2017

MAY 2017

LIFE

