RSA Beginner-

RSA Beginner

Jul 11th 18   90 points   1140 Solves   Cryptography   Hard   intelagent

Community Rating: **4.53 / 5**

I found this scribbled on a piece of paper. Can you make sense of it?
https://mega.nz/#!zD4wDYiC!iLB3pMJElgWZy6Bv97FF8SJz1KEk9lWsgBSw62mtxQg

We are provided with n,e,c and have to decrypt RSA encryption.

I made a program to decode RSA

```
from Crypto.Util.number import inverse

e= 3
c=2198788492188036287524967340373018438014878893445086 11639028
n= 245841236512478852752909734912575581815967630033049 838269083
p = 41606470020165830619632 0137931
q = 59087261282517955133610 2196593
phi = (p-1)*(q-1)

d = inverse(e,phi)

m = pow(c,d,n)

print(hex(m)[2:])
```

We get the hex and after decoding hex we will get the flag.

61626374667b7273345f69735f61773373306d337d

Operations	Recipe	Input

Operations

Search...

Favourites ⭐

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Recipe

From Hex

Delimiter
Auto

STEP BAKE! ☑ Auto Bake

Input length: 43 lines: 2

61626374667b7273345f69735f61773373306d337d

Output time: 1ms length: 21 lines: 1

abctf{rs4_is_aw3s0m3}

Flag is: abctf{rs4_is_aw3s0m3}