



## RSA Noob-

### RSA Noob

Jul 11th 18   60 points   1801 Solves   Cryptography   Medium   intelagent 



Community Rating: **4.43 / 5**

---

These numbers were scratched out on a prison wall. Can you help me decode them?  
[https://mega.nz/#!al8iDSYB!s5olEDK5zZmYdx1LZU8s4CmYqnynvU\\_aOUvdQojJPJQ](https://mega.nz/#!al8iDSYB!s5olEDK5zZmYdx1LZU8s4CmYqnynvU_aOUvdQojJPJQ)

The file given was-

```
1 e: 1
2 c: 9327565722767258308650643213344542404592011161659991421
3 n: 245841236512478852752909734912575581815967630033049838269083
```

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

I code the program to decode it.

```
1 from Crypto.Util.number import inverse
2
3 n= 245841236512478852752909734912575581815967630033049838269083
4 e= 1
5 c=9327565722767258308650643213344542404592011161659991421
6 p = 416064700201658306196320137931
7 q = 590872612825179551336102196593
8 phi = (p-1)*(q-1)
9
10 d = inverse(e,phi)
11 m = pow(c,d,n)
12
13 print(hex(m)[2:])
14
```

It will give us the hex value and after decoding this hex we will get the flag.

The screenshot shows a web application for decoding data. On the left is a sidebar with a search bar and a list of operations: 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, and Arithmetic / Logic. The main area is divided into three sections: 'Recipe', 'Input', and 'Output'. The 'Recipe' section has a 'From Hex' button and a 'Delimiter' dropdown set to 'Auto'. The 'Input' section contains a text area with the hex string '61626374667b6233747465725f75705f793075725f657d'. The 'Output' section shows the decoded result 'abctf{b3tter\_up\_y0ur\_e}'. At the bottom, there is a 'STEP' button, a green 'BAKE!' button with a chef icon, and an 'Auto Bake' checkbox.

Flag is: abctf{b3tter\_up\_y0ur\_e}