

Forum:[Hack Forums](#)

Thread: [generating public key having public modulus and exponent](#)

someguy8 - September 29, 2015, 3:47 am

hi !

im having this trouble for weeks and can't find a solution

i have the public modulus and exponent and want to generate the public key to encrypt files using it

i can't find anything neither on the web nor on the openssl man pages (im using linux)

do some body have an idea or a tool to do this ?!

crazyycast13 - September 29, 2015, 9:13 pm

<http://crypto.stackexchange.com/questions/29471/generate-rsa-public-key-having-public-modulus-and-exponent>

So I assume this is you?

someguy8 - September 30, 2015, 10:32 am

so any help u can give ? PS: revisit the link again

How bout using your brain - October 1, 2015, 3:41 am

Why would you wanna encrypt files with RSA? You do know that you can only encrypt data that is smaller than your modulus? So you would have to split up your files in blocks and encrypt them block by block and whatnot.

The way to do it, is to create an AES key. Use that key to symmetrically encrypt your files and then use RSA to encrypt your AES key.

Now I don't know how you can import it into openssl, but really you can just do your math yourself: All you need to do is to raise your AES key to the power of your public exponent e and then reduce by your modulus.

Code $key^e \bmod N$

someguy8 - October 1, 2015, 7:19 am

actually i don't want to encrypt files, i just want to encrypt a list of words one by one, and i have to encrypt them with the public key that much the modulus i have, but i don't have the public key that's the problem

i know this looks weird, why i am doing this in the first place. i have some reasons and i only need some help :)

How bout using your brain - October 1, 2015, 7:30 am

You do realize that the public exponent e and your modulus is your public key?

If you want to encrypt words you simply do the following in python:

PHP Code

```
<?php  
e = 0x10001  
N = 0x1234214....
```

```
words = open("words.txt").read().split()
```

```
for w in words:  
    ww = int(w.encode("hex"), 16)  
    print pow(ww, e, N)
```

someguy8 - *October 1, 2015, 7:55 am*

thanks, actually that would work :)

i just downloaded a bunch of python books, i should learn it !