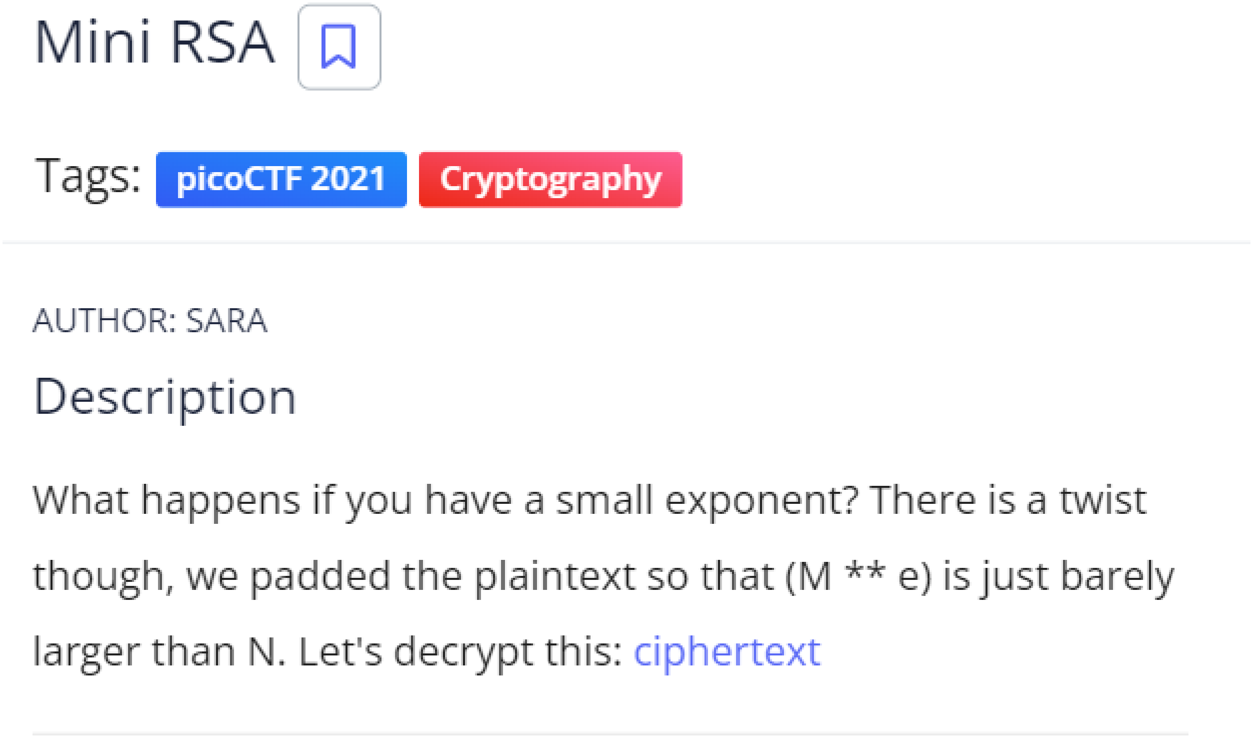
Mini RSA



Mini RSA

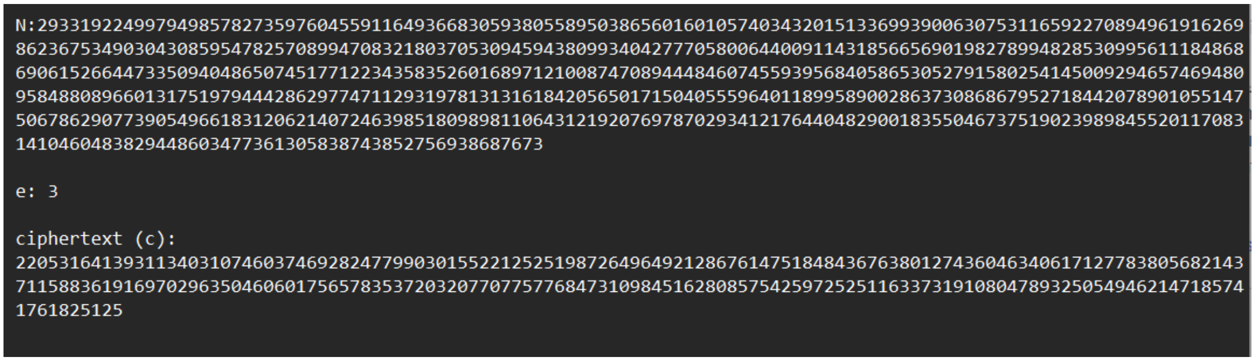
Tags: picoCTF 2021 Cryptography

AUTHOR: SARA

Description

What happens if you have a small exponent? There is a twist though, we padded the plaintext so that (M ** e) is just barely larger than N. Let's decrypt this: ciphertext

The attached file contained the following :

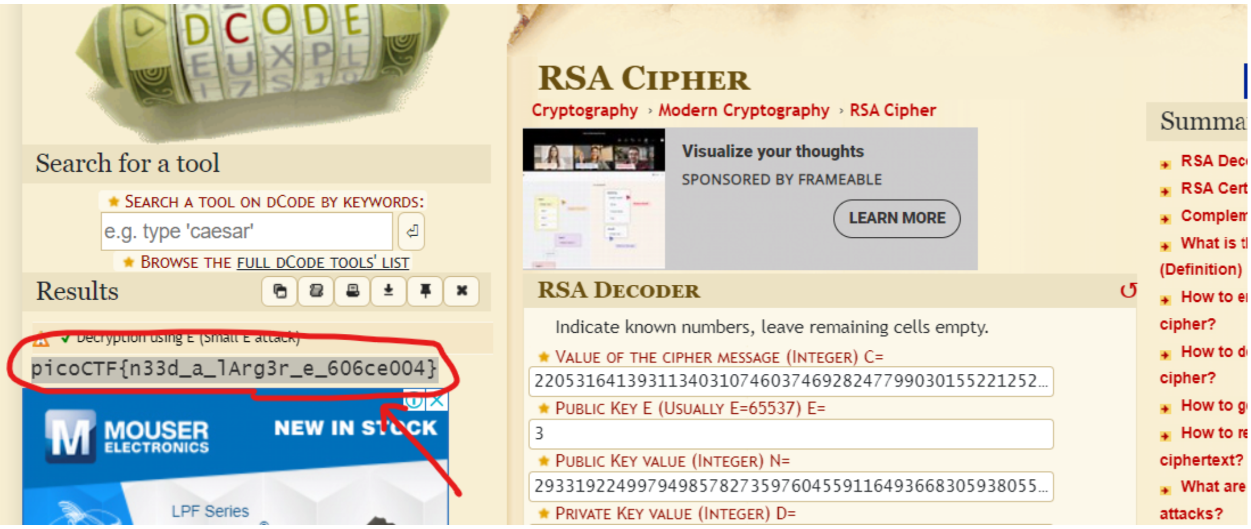


```
N:29331922499794985782735976045591164936683059380558950386560160105740343201513369939006307531165922708949619162 69
86236753490304308595478257089947083218037053094594380993404277705800644009114318566569019827899482853099561118 4868
69061526644733509404865074517712234358352601689712100874708944484607455939568405865305279158025414500929465746 9480
95848808966013175197944428629774711293197813131618420565017150405559640118995890028637308686795271844207890105 5147
50678629077390549661831206214072463985180989811064312192076978702934121764404829001835504673751902398984552011 7083
1410460483829448603477361305838743852756938687673

e: 3

ciphertext (c):
22053164139311340310746037469282477990301552212525198726496492128676147518484367638012743604634061712778380568 2143
71158836191697029635046060175657835372032077077577684731098451628085754259725251163373191080478932505494621471 8574
1761825125
```

After some research on how rsa encryption works, found out it can basically be represented in a formula :

c = (m^e) % N

Where, m is the message to encrypt, c is the encrypted ciphertext and e and N are large prime numbers.
I searched online for some RSA cipher decoders and reached this site.
And sure enough :



DCODE
Search for a tool
★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'caesar'
★ BROWSE THE FULL DCODE TOOLS' LIST
Results

Decryption using E (Small E attack)

```
picoCTF{n33d_a_lArg3r_e_606ce004}
```

RSA Cipher

Cryptography › Modern Cryptography › RSA Cipher

RSA Decoder

Indicate known numbers, leave remaining cells empty.

★ VALUE OF THE CIPHER MESSAGE (INTEGER) C=
2205316413931134031074603746928247799030155221252…

★ PUBLIC KEY E (USUALLY E=65537) E=
3

★ PUBLIC KEY VALUE (INTEGER) N=
2933192249979498578273597604559116493668305938055…

★ PRIVATE KEY VALUE (INTEGER) D=