

# WRITEUP PicoCTF

*Cryptography Easy*

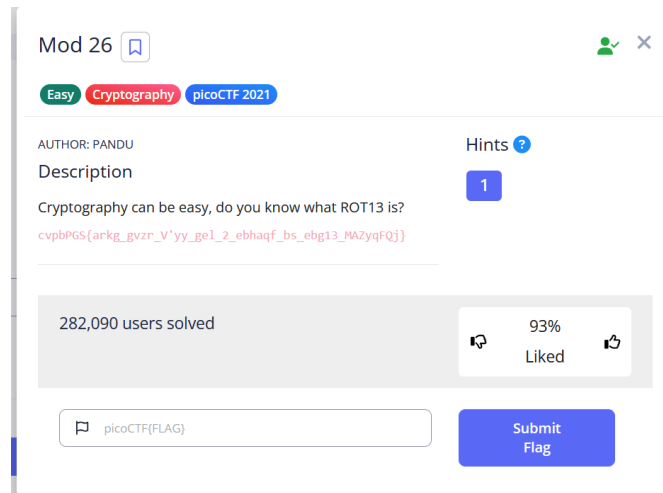


By: OngCapybara

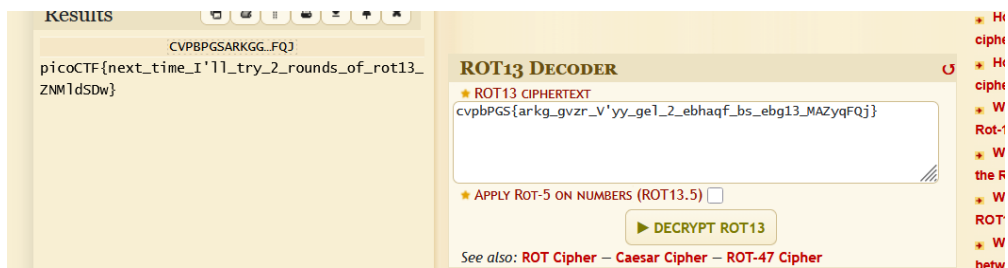
## Table Of Contents

Table Of Contents .....	i
Mod 26 .....	1
hashcrack .....	2
EVEN RSA CAN BE BROKEN???	4
13 .....	5
Interencdec.....	6

## Mod 26

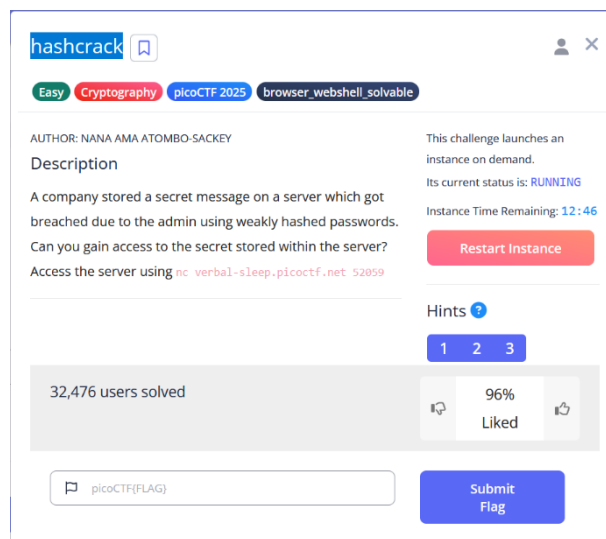


Use ROT13 decoder from dcode.fr and you will get the flag



**Flag:** picoCTF{next\_time\_I'll\_try\_2\_rounds\_of\_rot13\_ZNMldSDw}

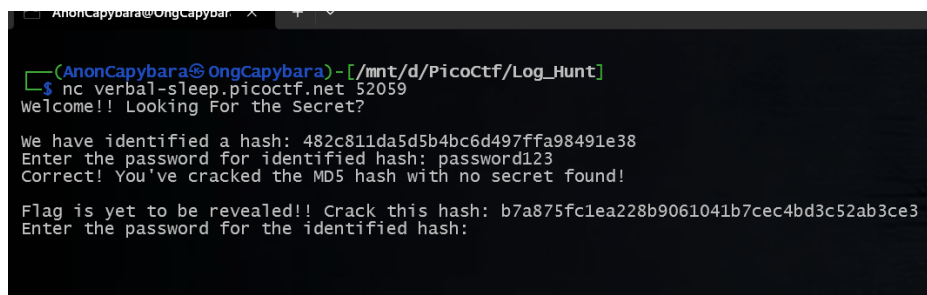
# hashcrack



Paste the netcat command to your terminal and you will get MD5 cipher and you can decode that using MD5 decoder from web above and you will get the first password like this



After that, paste it and you will get SHA-1 cipher text



Like first time, decode the cipher



This is the second decode, and... yeahhh... paste the password like this.  
 Anyway i'am forget to screenshots the third steps (my bad). You can take  
 third password and you will get the flag :D

```

[AnonCapybara@OngCapybara] - [/mnt/d/PicoCtf/Log_Hunt]
$ nc verbal-sleep.picoctf.net 52059
Welcome!! Looking For the Secret?

We have identified a hash: 482c811da5d5b4bc6d497ffa98491e38
Enter the password for identified hash: password123
Correct! You've cracked the MD5 hash with no secret found!

Flag is yet to be revealed!! Crack this hash: b7a875fc1ea228b9061041b7cec4bd3c52ab3ce3
Enter the password for the identified hash: letmein
Correct! You've cracked the SHA-1 hash with no secret found!

Almost there!! Crack this hash: 916e8c4f79b25028c9e467f1eb8eee6d6bbdff965f9928310ad30a8d88697745
Enter the password for the identified hash: qwerty098
Correct! You've cracked the SHA-256 hash with a secret found.
The flag is: picoCTF{UseStrOnG_h@shEs_&PaSswDs!_5b836723}

[AnonCapybara@OngCapybara] - [/mnt/d/PicoCtf/Log_Hunt]
  
```

**Flag:** picoCTF{UseStrOnG\_h@shEs\_&PaSswDs!\_5b836723}

## EVEN RSA CAN BE BROKEN???

### EVEN RSA CAN BE BROKEN???

Easy Cryptography picoCTF 2025 browser\_webshell\_solvable

AUTHOR: MICHAEL CROTTY

#### Description

This service provides you an encrypted flag. Can you decrypt it with just N & e?

Connect to the program with netcat:

```
$ nc verbal-sleep.picoctf.net 63509
```

The program's source code can be downloaded [here](#).

This challenge launches an instance on demand.  
Its current status is: **RUNNING**  
Instance Time Remaining: **14:31**

**Restart Instance**

#### Hints

1 2 3

16,459 users solved

95% Liked

picoCTF{FLAG}

**Submit Flag**

This is RSA chall. You can visit [dcode.fr](https://dcode.fr) and use RSA decoder. After you paste the netcat command, you will get many key like this

```
(AnonCapybara@OngCapybara) - /mnt/d/PicoCtf/Log_Hunt]
$ nc verbal-sleep.picoctf.net 63509
N: 21683005575161020699248975142360884162847479211235052838703393603098412109996006591810654543127203426174783431909166217336046922586649341668988532411282422
e: 65537
cyphertext: 1836428094352010053848398114828082393691510409178798418527938857106912313054998901865650826557555083792153411462260926151949556397474861475722920647406357
(AnonCapybara@OngCapybara) - /mnt/d/PicoCtf/Log_Hunt]
```

After that, you just need to adjust the key like this

#### Results

Warning cyphertext:1...357 = number-s (0-9) → unexpected character-s removed

❌ Wiener's attack: failure

✅ P,Q computed with N ([Self-Limited) Prime Factors Decomposition)

✅ D computed with P,Q,E

✅ Decryption using C,D,N

picoCTF{tw0\_1\$\_pr!m3df98b648}

#### RSA DECODER

Indicate known numbers, leave remaining cells empty.

★ VALUE OF THE CIPHER MESSAGE (INTEGER) C= 53411462260926151949556397474861475722920647406357

★ PUBLIC KEY E (USUALLY E=65537) E= 65537

★ PUBLIC KEY VALUE (INTEGER) N= 83431909166217336046922586649341668988532411282422

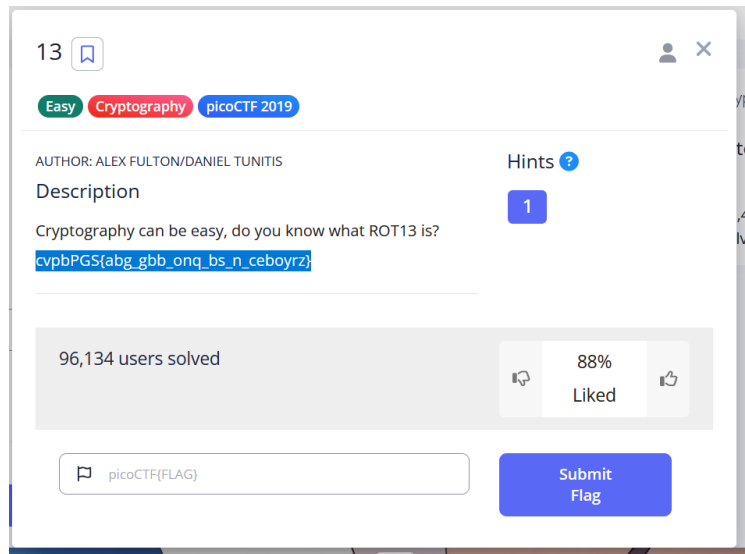
★ PRIVATE KEY VALUE (INTEGER) D=

★ FACTOR 1 (PRIME NUMBER) P=

★ FACTOR 2 (PRIME NUMBER) Q=

**Flag:** picoCTF{tw0\_1\$\_pr!m3df98b648}

## 13

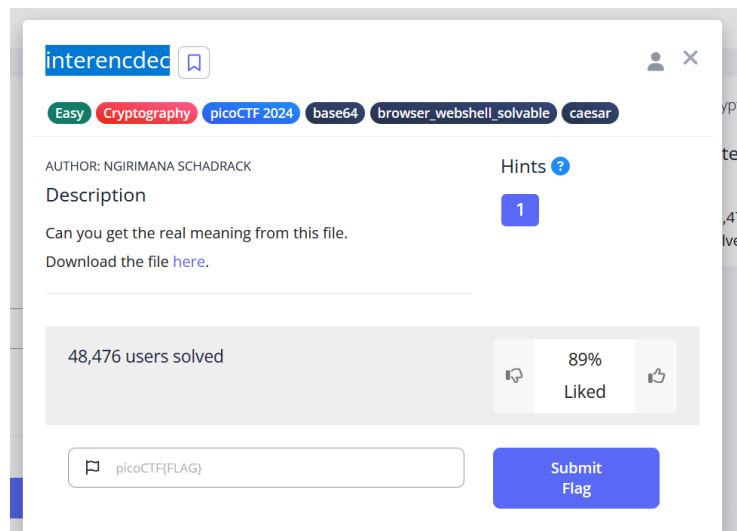


This chall is very easy. You just using ROT13 for decode the cipher and you will get the flag :D



**Flag:** picoCTF{not\_too\_bad\_of\_a\_problem}

# Interencdec



After you download the file, write the file and you will get a base64 cipher text. After that you just following my command and you will get the flag :D

```
(AnonCapybara@OngCapybara) - [/mnt/d/PicoCtf]
$ cat enc_flag
YidkM0JxZGtwQ1RYdHFhR3g2YUhsZmF6TnF1VGwzWVR0c1h6ZzVNR3N5TXpjNWZRPT0nCg==

(AnonCapybara@OngCapybara) - [/mnt/d/PicoCtf]
$ echo "YidkM0JxZGtwQ1RYdHFhR3g2YUhsZmF6TnF1VGwzWVR0c1h6ZzVNR3N5TXpjNWZRPT0nCg==" | base64 -d
b'd3BqdkpBTxtqaGx6aH1fazNqeT13YTnrXzg5MGsyMzc5fQ=='

(AnonCapybara@OngCapybara) - [/mnt/d/PicoCtf]
$ echo "d3BqdkpBTxtqaGx6aH1fazNqeT13YTnrXzg5MGsyMzc5fQ==" | base64 -d
wpjvJAM{jh1zhy_k3jy9wa3k_890k2379}

(AnonCapybara@OngCapybara) - [/mnt/d/PicoCtf]
$ echo 'wpjvJAM{jh1zhy_k3jy9wa3k_890k2379}' | tr 'A-Za-z' 'T-ZA-St-za-s'
picoCTF{caesar_d3cr9pt3d_890d2379}
```

The last command is ROT19 decode

**Flag:** picoCTF{caesar\_d3cr9pt3d\_890d2379}