

# **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

The screenshot shows a challenge card for 'Mod 26'. At the top, it says 'Mod 26' with a link icon. Below that are three tags: 'Easy', 'Cryptography', and 'picoCTF 2021'. To the right are icons for user profile and close. Underneath, it says 'AUTHOR: PANDU' and 'Description'. The description text reads: 'Cryptography can be easy, do you know what ROT13 is?' followed by a ROT13 encoded string: 'cvpbPGS{arkg\_gvzr\_V'yy\_ge1\_2\_ebhaqf\_bs\_ebg13\_MAZyqFQj}'. A 'Hints' button with a question mark and a count of '1' is shown. Below the description, it says '282,090 users solved' with a progress bar at 93% and a 'Liked' button. At the bottom is a text input field containing 'picoCTF{FLAG}' and a blue 'Submit Flag' button.

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

The screenshot shows the 'ROT13 DECODER' tool from dcode.fr. It has a sidebar with a 'RESULTS' section containing the flag 'picoCTF{next\_time\_I'll\_try\_2\_rounds\_of\_rot13\_ZNMIdSDw}'. The main area is titled 'ROT13 DECODER' and contains a text input field with the ROT13 encoded string 'cvpbPGS{arkg\_gvzr\_V'yy\_ge1\_2\_ebhaqf\_bs\_ebg13\_MAZyqFQj'. Below it is a checkbox for '★ APPLY ROT-5 ON NUMBERS (ROT13.5)' and a large orange '► DECRYPT ROT13' button. A note at the bottom says 'See also: ROT Cipher — Caesar Cipher — ROT-47 Cipher'. To the right, there's a vertical sidebar with some text and a red 'HOT' indicator.

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

# hashcrack

AUTHOR: NANA AMA ATOMBO-SACKY  
Description  
A company stored a secret message on a server which got breached due to the admin using weakly hashed passwords.  
Can you gain access to the secret stored within the server?  
Access the server using nc verbal-sleep.picoctf.net 52059

This challenge launches an instance on demand.  
Its current status is: RUNNING  
Instance Time Remaining: 12:46

Restart Instance

Hints ?  
1 2 3

32,476 users solved  
96% Liked

Submit Flag

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

Results

MD5

password123

MD5 DECODER

★ MD5 HASH: 482C811DA5D5B4BC6D497FFA98491E38

OPTIONS

★ SALT PREFIXED MD5(SALT+WORD)

★ SALT SUFFIXED MD5(WORD+SALT)

DECRYPT

See also: Hash Function — SHA-1 — SHA-256 — Crypt() Hashing Function

MD5 ENCODER

FROM A CHARACTER STRING

MD5 PLAIN TEXT OR PASSWORD

dCode

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

```
(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:
```

Like first time, decode the cipher

The screenshot shows the dCode SHA-1 Decoder interface. In the 'Results' section, the word 'letmein' is entered under the 'SHA1' tab. Below it, the 'SHA-1 DECODER' section displays the identified SHA-1 hash: `b7a875fc1ea228b9061041b7cec4bd3c52ab3ce3`. There are options for 'SALT PREFIXED SHA1(SALT+WORD)' and 'SALT SUFFIXED SHA1(WORD+SALT)'.

This is the second decode, and... yeahhh... paste the password like this.  
Anyway i'm 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.picotf.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{UseStr0nG_h@shEs_&PaSswDs!_5b836723}

[REDACTED]
```

**Flag:** picoCTF{UseStr0nG\_h@shEs\_&PaSswDs!\_5b836723}

# EVEN RSA CAN BE BROKEN???

The screenshot shows a challenge page from picoCTF. The title is "EVEN RSA CAN BE BROKEN???" with a bookmark icon. Below it are tags: "Easy", "Cryptography", "picoCTF 2025", and "browser\_webshell\_solvable". The author is Michael Crotty. The challenge description states: "This service provides you an encrypted flag. Can you decrypt it with just N & e?". It also says: "Connect to the program with netcat: nc verbal-sleep.picoctf.net 63509". A link to the source code is provided. The status is "RUNNING" with 14:31 remaining. A "Restart Instance" button is available. Below the description, it says "16,459 users solved". On the right, there are "Hints" (1, 2, 3), a "95% Liked" rating, and a "Submit Flag" button.

This is RSA chall. You can visit dcode.fr and use RSA decoder. After you paste the netcat command, you will gate many key like this

```
$ nc verbal-sleep.picoctf.net 63509
N: 2168300557518102069924897514236084162847479211235052838703393603098412109996006591810654543127203426174783431909166217336046922586649341668988532411282
e: 65537
ciphertext: 1836428094352010053848398114828082393691510409178798418527943885706912313054998901865650826557555083792153411462260926151949556397474861475722
920647406357
```

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

The screenshot shows the RSA Decoder tool. On the left, there's a terminal window with the command "nc verbal-sleep.picoctf.net 63509" and the resulting ciphertext: "53411462260926151949556397474861475722920647406357". The RSA Decoder interface has fields for "PUBLIC KEY E (USUALLY E=65537)", "PUBLIC KEY VALUE (INTEGER) N=", and "PRIVATE KEY VALUE (INTEGER) D=". To the right, there's a grid of letters and symbols corresponding to the ciphertext digits.

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

# 13

13

Easy Cryptography picoCTF 2019

AUTHOR: ALEX FULTON/DANIEL TUNITIS

Description

Cryptography can be easy, do you know what ROT13 is?  
cvpbPGS{abg\_gbb\_onq\_bs\_n\_ceboyrz}

96,134 users solved

Hints ? 1

88% Liked

picoCTF(FLAG) Submit Flag

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

Results

CVPBPGSABGGB\_YRZ  
picoCTF{not\_too\_bad\_of\_a\_problem}

ROT13 DECODER

\* ROT13 CIPHERTEXT  
cvpbPGS{abg\_gbb\_onq\_bs\_n\_ceboyrz}

\* APPLY ROT-5 ON NUMBERS (ROT13.5)

► DECRYPT ROT13

See also: ROT Cipher – Caesar Cipher – ROT-47 Cipher

ROT13 ENCODER

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

## Interencdec

The screenshot shows a challenge page for 'interencdec'. At the top, there's a title bar with the challenge name and a blue bookmark icon. Below it, a navigation bar includes categories like 'Easy', 'Cryptography', 'picoCTF 2024', 'base64', 'browser\_webshell\_solvable', and 'caesar'. The author is listed as 'NGIRIMANA SCHADRACK'. A 'Hints' button with a question mark and a count of '1' is visible. The challenge description asks for the real meaning from a file, with a download link provided. It also notes that 48,476 users solved the challenge. Below the description is a text input field for the flag ('picoCTF{FLAG}') and a large blue 'Submit Flag' button.

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
YidkM0JxZGtwQ]RYdHFhR3g2YUhsZmF6TnF1VGwzWVRoc1h6ZzVNR3N5TxpjNWZRPT0nCg==

(AnonCapybara@OngCapybara) - [/mnt/d/PicoCtf]
$ echo "YidkM0JxZGtwQ]RYdHFhR3g2YUhsZmF6TnF1VGwzWVRoc1h6ZzVNR3N5TxpjNWZRPT0nCg==" | base64 -d
b'd3BqdkpBTxtqaGx6aH1fazNqeTl3YTNrXzg5MGsyMzc5fQ=='

(AnonCapybara@OngCapybara) - [/mnt/d/PicoCtf]
$ echo "d3BqdkpBTxtqaGx6aH1fazNqeTl3YTNrXzg5MGsyMzc5fQ==" | 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}