

CryptoverseCTF 2022

Sahil Bugade
(<http://snip3r.me>)

Problem Statement:

Crypto/Warmup 1293 solves / 107 points

Baby

Decode the following ciphertext: `cGlwZ3N7cG5yZm5lXzY0X3Nnan0=`.

Remember: **CyberChef** is your friend.

Flag (solved)

SUBMIT

Given cipher text: `cGlwZ3N7cG5yZm5lXzY0X3Nnan0=`

Now after solving a bit of crypto CTFs we were easily able to guess that the given cipher text was encoded in base64. So firstly we decoded it from base64.

Base64 Decode

Base64 online decode function

```
cGlwZ3N7cG5yZm5lXzY0X3Nnan0=
```

Decode

☒ Auto Update

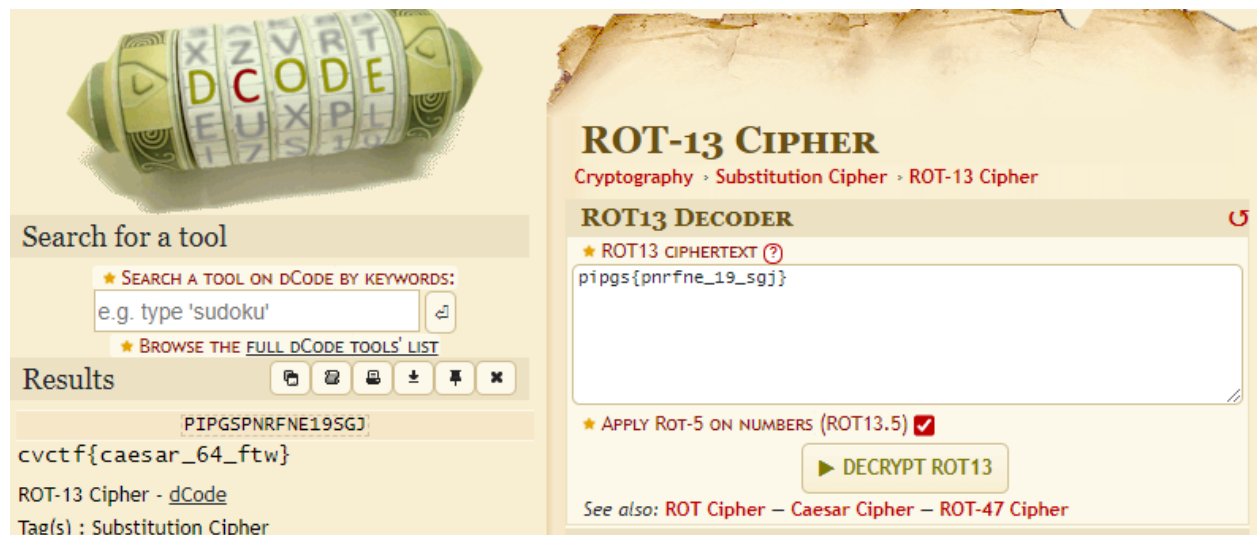
```
pipgs{pnrfne_64_sgj}
```

As you can see the decode text is “pipgs{pnrfne_64_sgj}” which can be identified as a format that a flag would be written in but isn’t the actual flag as the competition had its flag format “cvctf{”.

So hereby, I saw that the output we got had (PiPgS) repeated “P” and the flag format (CvCtf) had “C” repeated. So I calculated how far is the alphabet “C” from “P” and came out to be 13 letters ahead.

So I calculated manually each and every alphabet 13 ahead of the given decoded form and came out with the flag cvctf{caesar_64_ftw}.

Later I came to know that such type of encryption is called ROT-13 encryption and could be found on the site: <https://www.dcode.fr/rot-13-cipher>.



The screenshot shows the dCode website's ROT-13 Cipher Decoder tool. On the left, there's a search bar with the text "Search for a tool" and a search button. Below it, a search result for "PIPSPNRFNE19SGJ" is shown, with the decoded text "cvctf{caesar_64_ftw}" and the tag "ROT-13 Cipher - dCode". On the right, the "ROT-13 CIPHER" section is visible, featuring a "ROT13 DECODER" input field containing "pipgs{pnrfne_19_sgj}" and a "DECRYPT ROT13" button. The interface is designed to look like a piece of old parchment.

Flag: cvctf{caesar_64_ftw}

It was our first international CTF, so overall we enjoyed it and to mention teamwork is always a key to success!