PICOCTF 2023

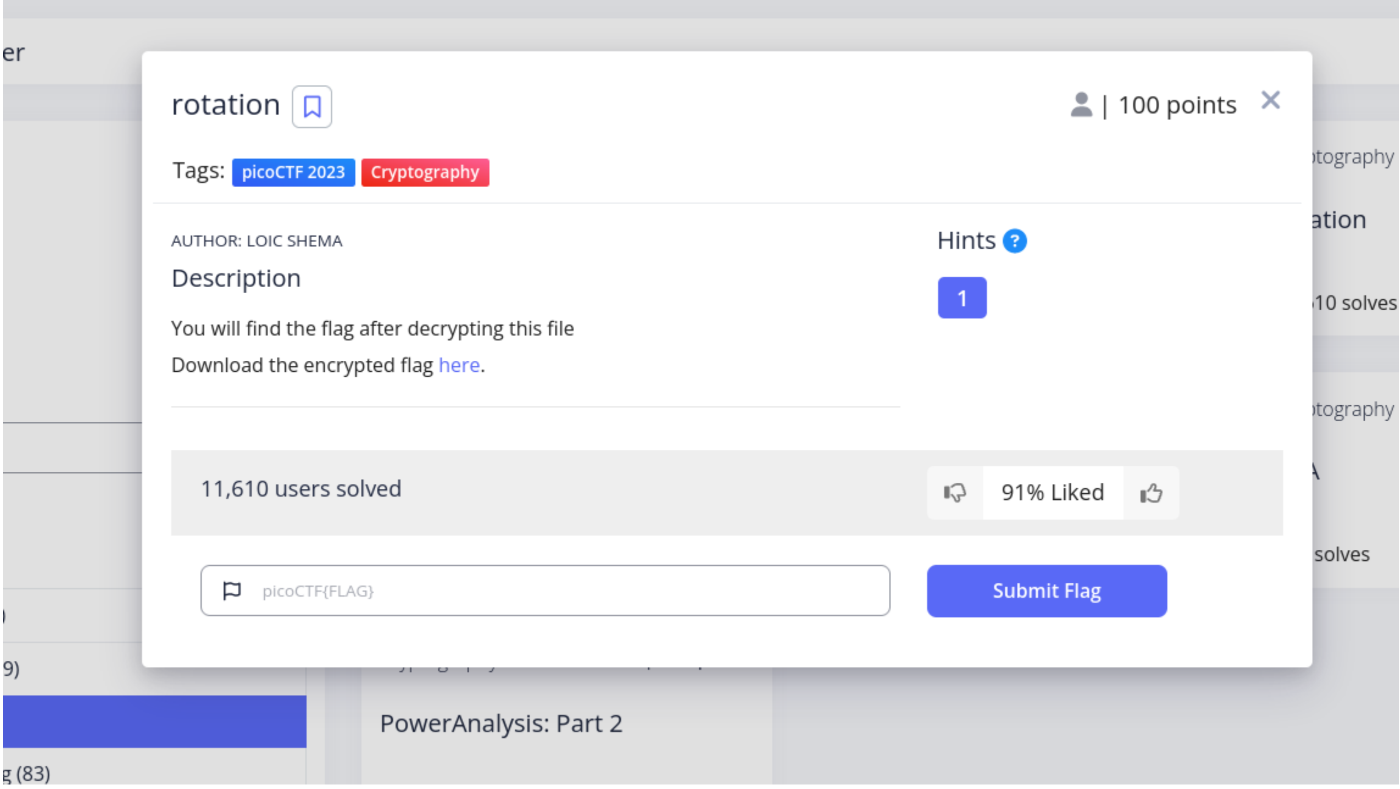
CATEGORY : Cryptography

CHALLENGE : rotation

POINTS : 100

WRITEUP

First I copy the link of the file by doing a right click on “here” and clicking on “copy link”



rotation | 100 points

Tags: picoCTF 2023 Cryptography

AUTHOR: LOIC SHEMA

Description

You will find the flag after decrypting this file

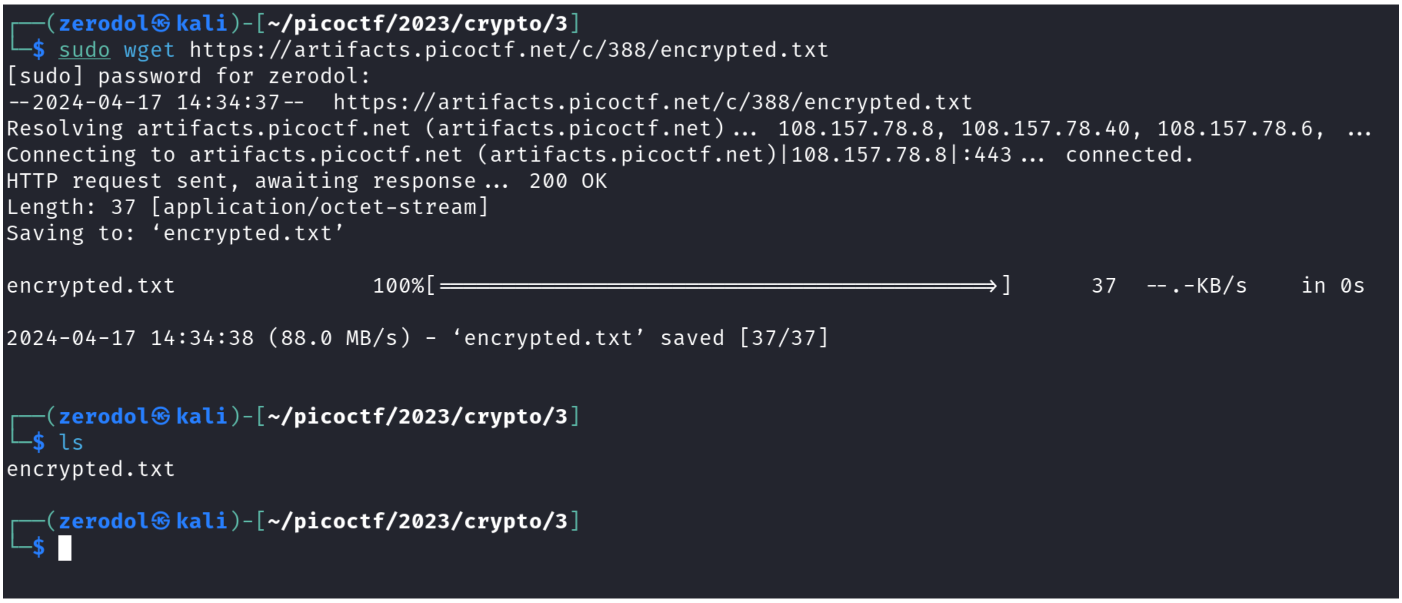
Download the encrypted flag here.

Hints 1

11,610 users solved

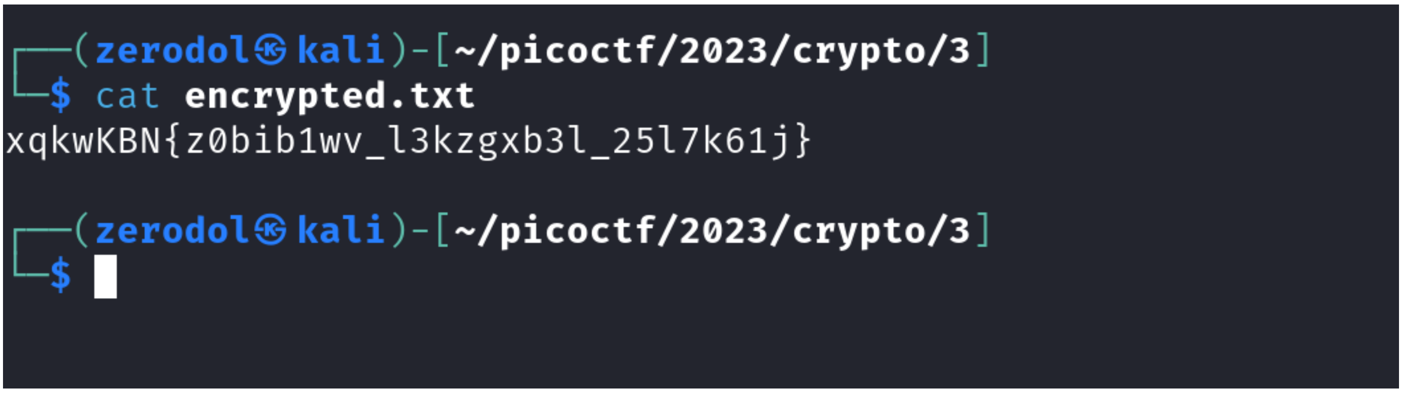
91% Liked

Next I download the file with the **“wget”** command. We have a file name **encrypted.txt**



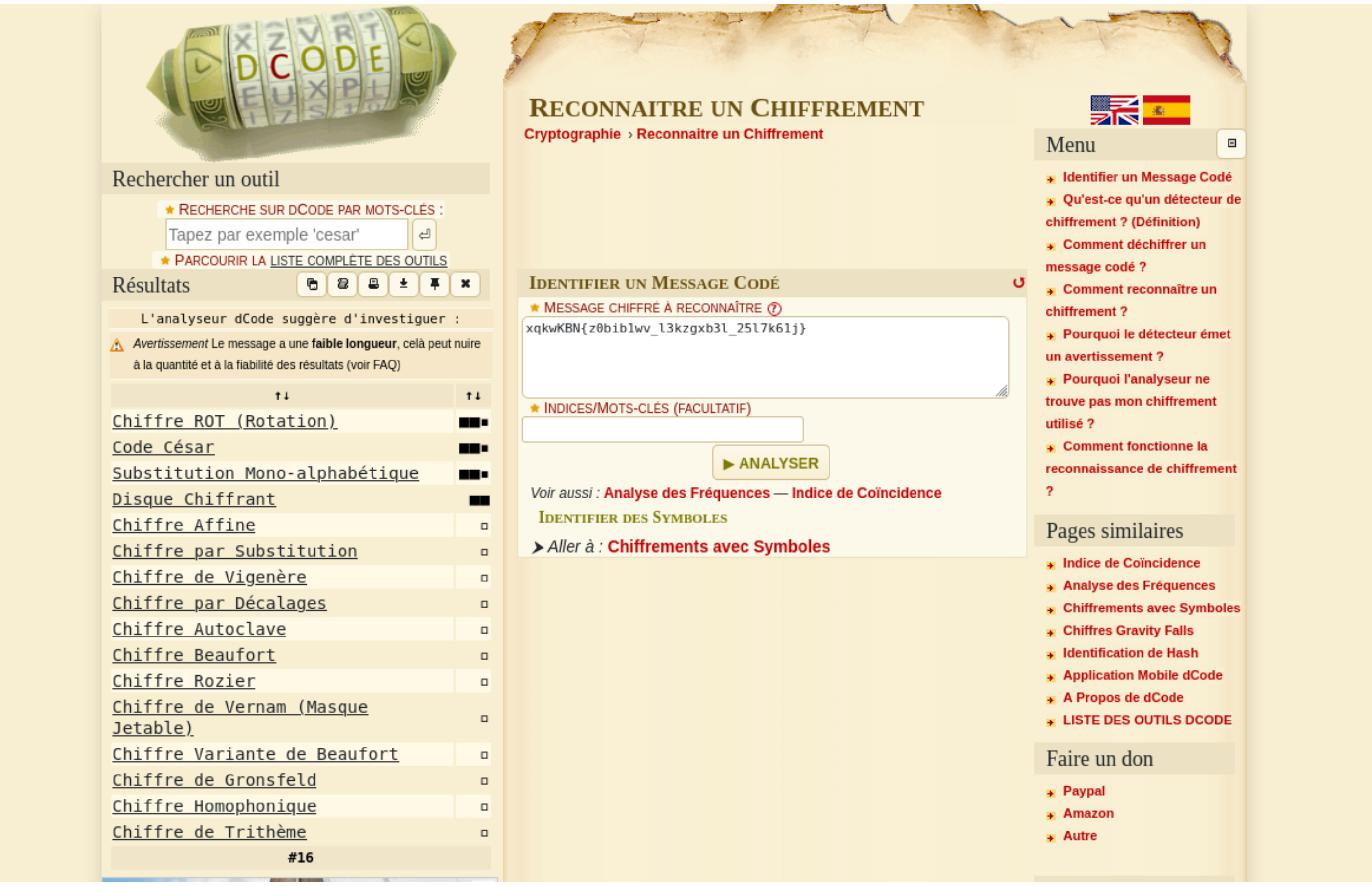
```
┌──(zerodol㉿kali)-[~/picoctf/2023/crypto/3]
└─$ sudo wget https://artifacts.picoctf.net/c/388/encrypted.txt
[sudo] password for zerodol:
--2024-04-17 14:34:37--  https://artifacts.picoctf.net/c/388/encrypted.txt
Resolving artifacts.picoctf.net (artifacts.picoctf.net)... 108.157.78.8, 108.157.78.40, 108.157.78.6, ...
Connecting to artifacts.picoctf.net (artifacts.picoctf.net)|108.157.78.8|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 37 [application/octet-stream]
Saving to: ‘encrypted.txt’

encrypted.txt             100%[===========================================>]      37  --.-KB/s    in 0s

2024-04-17 14:34:38 (88.0 MB/s) - ‘encrypted.txt’ saved [37/37]


┌──(zerodol㉿kali)-[~/picoctf/2023/crypto/3]
└─$ ls
encrypted.txt

┌──(zerodol㉿kali)-[~/picoctf/2023/crypto/3]
└─$ 
```

I display the content of the file and we can see that the content is encrypted but we don't know the algorithm. It's time to use **"dcode"**



```
┌──(zerodol㉿kali)-[~/picoctf/2023/crypto/3]
└─$ cat encrypted.txt
xqkwKBN{z0bib1wv_l3kzgxb3l_25l7k61j}

┌──(zerodol㉿kali)-[~/picoctf/2023/crypto/3]
└─$ █
```

We go on "**dcode.fr/cipher-identifier**" and we paste the content to determine the cipher. It appears to be a "Chiffre ROT (Rotation) cipher". We can click on it and it will lead us to the page where we can decipher it.



DCODE
Rechercher un outil
★ RECHERCHE SUR DCODE PAR MOTS-CLÉS :
Tapez par exemple 'cesar'
★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS
Résultats

L'analyseur dCode suggère d'investiguer :

⚠ *Avertissement* Le message a une **faible longueur**, celà peut nuire à la quantité et à la fiabilité des résultats (voir FAQ)

↑↓	↑↓
Chiffre ROT (Rotation)	■■▪
Code César	■■▪
Substitution Mono-alphabétique	■■▪
Disque Chiffrant	■■
Chiffre Affine	▫
Chiffre par Substitution	▫
Chiffre de Vigenère	▫
Chiffre par Décalages	▫
Chiffre Autoclave	▫
Chiffre Beaufort	▫
Chiffre Rozier	▫
Chiffre de Vernam (Masque Jetable)	▫
Chiffre Variante de Beaufort	▫
Chiffre de Gronsfeld	▫
Chiffre Homophonique	▫
Chiffre de Trithème	▫
#16	

RECONNAITRE UN CHIFFREMENT

Cryptographie › Reconnaitre un Chiffrement

IDENTIFIER UN MESSAGE CODÉ

★ MESSAGE CHIFFRÉ À RECONNAÎTRE ⓘ

```
xqkwKBN{z0bib1wv_l3kzgxb3l_25l7k61j}
```

★ INDICES/MOTS-CLÉS (FACULTATIF)

▶ ANALYSER

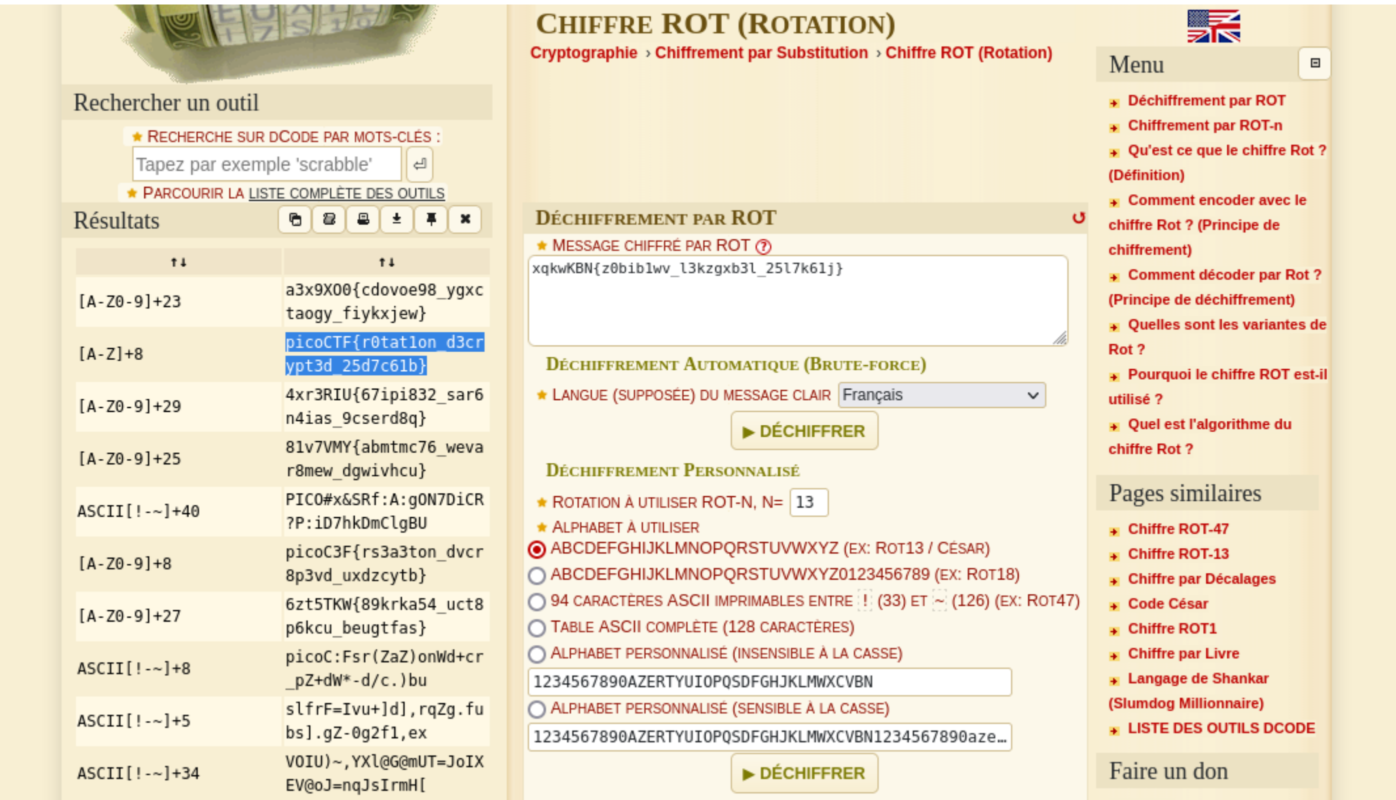
Voir aussi : Analyse des Fréquences — Indice de Coïncidence

IDENTIFIER DES SYMBOLES

➤ Aller à : Chiffrements avec Symboles

Menu
Identifier un Message Codé
Qu'est-ce qu'un détecteur de chiffrement ? (Définition)
Comment déchiffrer un message codé ?
Comment reconnaître un chiffrement ?
Pourquoi le détecteur émet un avertissement ?
Pourquoi l'analyseur ne trouve pas mon chiffrement utilisé ?
Comment fonctionne la reconnaissance de chiffrement ?
Pages similaires
Indice de Coïncidence
Analyse des Fréquences
Chiffrements avec Symboles
Chiffres Gravity Falls
Identification de Hash
Application Mobile dCode
A Propos de dCode
LISTE DES OUTILS DCODE
Faire un don
Paypal
Amazon
Autre

We put the encrypted content and we have multiple responses due to multiple attempts. But we can see that there is something that appears to have the pattern of the flags on picoctf



Rechercher un outil

★ RECHERCHE SUR DCODE PAR MOTS-CLÉS :

Tapez par exemple 'scrabble'

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

↑↓	↑↓
[A-Z0-9]+23	a3x9XO0{cdovoe98_ygxctaogy_fiykxjew}
[A-Z]+8	picoCTF{r0tat1on_d3crypt3d_25d7c61b}
[A-Z0-9]+29	4xr3RIU{67ipi832_sar6n4ias_9cserd8q}
[A-Z0-9]+25	81v7VMY{abmtmc76_wevar8mew_dgwivhcu}
ASCII[!-~]+40	PICO#x&SRf:A:gON7DiCR?P:iD7hkDmClgBU
[A-Z0-9]+8	picoC3F{rs3a3ton_dvcr8p3vd_uxdzcytb}
[A-Z0-9]+27	6zt5TKW{89krka54_uct8p6kcu_beugtfas}
ASCII[!-~]+8	picoC:Fsr(ZaZ)onWd+cr_pZ+dW*-d/c.)bu
ASCII[!-~]+5	slfrF=Ivu+]d],rqZg.fubs].gZ-0g2f1,ex
ASCII[!-~]+34	VOIU)~,YXl@G@mUT=JoIXEV@oJ=nqJsIrmH[

CHIFFRE ROT (ROTATION)

Cryptographie › Chiffrement par Substitution › Chiffre ROT (Rotation)

DÉCHIFFREMENT PAR ROT

★ MESSAGE CHIFFRÉ PAR ROT

```
xqkwKBN{z0bib1wv_l3kzgxb3l_25l7k61j}
```

DÉCHIFFREMENT AUTOMATIQUE (BRUTE-FORCE)

★ LANGUE (SUPPOSÉE) DU MESSAGE CLAIR: Français

▶ DÉCHIFFRER

DÉCHIFFREMENT PERSONNALISÉ

★ ROTATION À UTILISER ROT-N, N= 13

★ ALPHABET À UTILISER

● ABCDEFGHIJKLMNOPQRSTUVWXYZ (EX: ROT13 / CÉSAR)

○ ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 (EX: ROT18)

○ 94 CARACTÈRES ASCII IMPRIMABLES ENTRE ! (33) ET ~ (126) (EX: ROT47)

○ TABLE ASCII COMPLÈTE (128 CARACTÈRES)

○ ALPHABET PERSONNALISÉ (INSENSIBLE À LA CASSE)

1234567890AZERTYUIOPQSDFGHJKLMWXCVBN

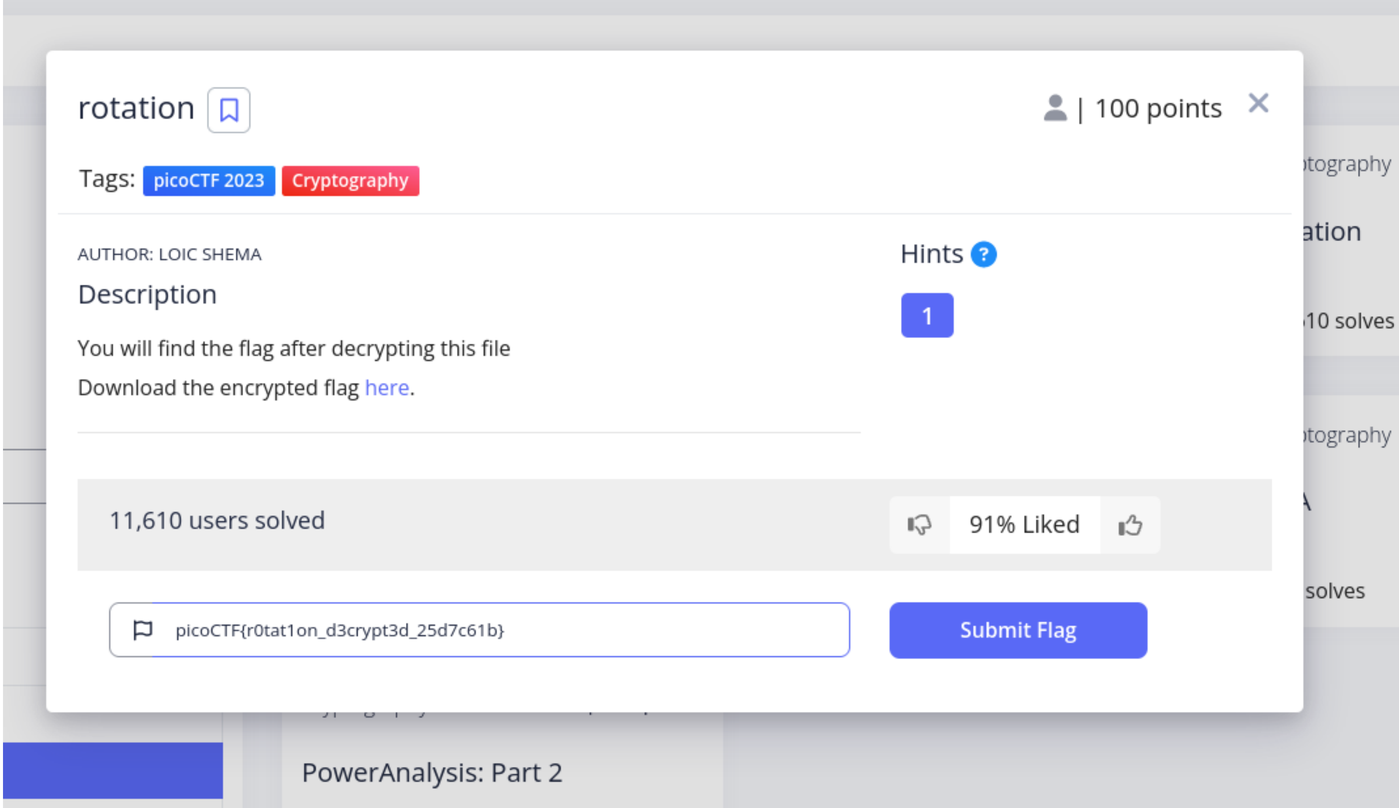
○ ALPHABET PERSONNALISÉ (SENSIBLE À LA CASSE)

1234567890AZERTYUIOPQSDFGHJKLMWXCVBN1234567890aze…

▶ DÉCHIFFRER

Menu
Déchiffrement par ROT
Chiffrement par ROT-n
Qu'est ce que le chiffre Rot ? (Définition)
Comment encoder avec le chiffre Rot ? (Principe de chiffrement)
Comment décoder par Rot ? (Principe de déchiffrement)
Quelles sont les variantes de Rot ?
Pourquoi le chiffre ROT est-il utilisé ?
Quel est l'algorithme du chiffre Rot ?
Pages similaires
Chiffre ROT-47
Chiffre ROT-13
Chiffre par Décalages
Code César
Chiffre ROT1
Chiffre par Livre
Langage de Shankar (Slumdog Millionnaire)
LISTE DES OUTILS DCODE
Faire un don

We have our flag : **picoCFT{r0tat1on_d3cryp3d_25d7c61b}**



rotation

Tags: picoCTF 2023 Cryptography

| 100 points

AUTHOR: LOIC SHEMA

Description

You will find the flag after decrypting this file

Download the encrypted flag here.

Hints ?

1

11,610 users solved

91% Liked

picoCTF{r0tat1on_d3crypt3d_25d7c61b}

Submit Flag